SZTAFETA ENIGMY

Odnaleziony raport polskich kryptologów

Warszawa 2019

Redakcja, opracowanie i tłumaczenie tekstów
Marek Grajek

Skład
Agnieszka Dębska, Izabela Laskus

Projekt okładki i opracowanie graficzne
Bernard Wałek

© Copyright by Agencja Bezpieczeństwa Wewnętrznego
Centralny Ośrodek Szkolenia i Edukacji
im. gen. dyw. Stefana Roweckiego „Grota" w Emowie
Emów 2019

ISBN: 978-83-953038-0-7

Wydanie II uzupełnione

Agencja Bezpieczeństwa Wewnętrznego
Centralny Ośrodek Szkolenia i Edukacji
im. gen. dyw. Stefana Roweckiego „Grota" w Emowie
05-462 Wiązowna, ul. Nadwiślańczyków 2

Druk i oprawa:
WIP-Druk Sp. z o.o.
05-077 Warszawa, ul. Jana Pawła II 7
tel. (+48) 22 815 20 14
e-mail: wipdruk@wipdruk.pl
www.wipdruk.pl

SPIS TREŚCI

Podziękowania
5

Przedmowa
7

Preface
25

Przedmowa do drugiego wydania
43

Preface to the second edition
45

Raport – fotokopia oryginału
47

Raport – fotokopia przekładu na język francuski
111

Transkrypt oryginału w języku niemieckim
143

Przekład oryginału na język polski
177

Przekład oryginału na język angielski
211

Transkrypt wersji francuskojęzycznej
243

Podziękowania

Pragnę złożyć serdeczne podziękowania Szefowi Agencji Bezpieczeństwa Wewnętrznego Panu prof. dr. hab. Piotrowi Pogonowskiemu za umożliwienie opublikowania niniejszej książki pod auspicjami instytucji, na której czele Pan Profesor stoi. Dziękuję za okazanie wrażliwości na to, co jest świadectwem naszej historii, dowodem ludzkich dokonań i możliwości. Za wspólną chęć propagowania sukcesu polskich kryptologów, który istotnie wpłynął na działalność alianckich służb specjalnych, a co za tym idzie – także na losy drugiej wojny światowej.

Gorące podziękowania kieruję także do osób, bez których pomocy tekst nigdy by nie powstał. Philippe Guillot udzielił w poszukiwaniach pomocy, która przyspieszyła dotarcie do celu. Jerry McCarthy pochylił się nad angielskim tłumaczeniem tekstu, wnosząc do niego istotne korekty. Zbiegiem okoliczności w pracach nad publikacją uczestniczyli przedstawiciele tych samych krajów, które były zaangażowane we wczesny etap międzyalianckiej współpracy kryptologicznej, opisany w prezentowanym dokumencie.

Marek Grajek, Warszawa 2019

Przedmowa

Konferencja, która odbyła się w Pyrach w dniach 24–27 lipca 1939 r., stanowiła efektywny początek współpracy kryptologicznej aliantów. Z czasem miała ona wpłynąć na losy II wojny światowej. Spotkanie kryptologów z Polski, Francji i Wielkiej Brytanii było nacechowane dużym ładunkiem emocji, łatwych do odczytania we wspomnieniach uczestników. Raporty przez nich złożone w większym stopniu dotyczą prawdziwych lub prawdopodobnych motywacji stron spotkania, zwrotów akcji w jego trakcie i finalnych ustaleń niż jego istotnej treści, tj. zakresu informacji przekazanych przez polskich kryptologów, określających skalę ich sukcesu w zmaganiach z szyframi niemieckiej Enigmy. Polacy znali granice swojej wiedzy na temat tej maszyny i nie musieli eksponować swych sukcesów. Zagraniczni uczestnicy konferencji zostali zwolnieni z obowiązku szczegółowego relacjonowania polskich metod ataku na szyfr; otrzymali obszerne kompendium wiedzy na temat Enigmy sporządzone w języku niemieckim – jedynym, którym posługiwali się wszyscy uczestnicy konferencji. To kompendium stanowiło właściwy kapitał założycielski kryptologicznej współpracy aliantów, która w ostatecznym wyniku okazała się jednym z czynników decydujących o losach II wojny światowej. Dlatego jest okolicznością nieco niefortunną, że niemal 80 lat po zakończeniu konfliktu, kiedy zdecydowana większość dokumentów opisujących wojenne osiągnięcia alianckich kryptologów została udostępniona historykom, dokument o tak fundamentalnym znaczeniu pozostaje niedostępny.

Raport kryptologów Biura Szyfrów z oczywistych powodów nie zachował się w polskich archiwach. Chciałoby się powiedzieć – na szczęście. Część archiwum przedwojennego polskiego wywiadu wskutek tragicznego błędu wpadła w ręce Niemców tuż po zakończeniu kampanii wrześniowej. Wielu agentów polskiego wywiadu przypłaciło to zaniedbanie życiem. W zdobytym archiwum Niemcy znaleźli jedynie trzy depesze zaszyfrowane pierwotnie z wykorzystaniem Enigmy i uznali to znalezisko za przypadkowe. Wyszli z założenia, że systematyczny dekryptaż musiałby pozostawić więcej śladów. Właściwe archiwum polskiego Biura Szyfrów zostało zniszczone w trakcie ewakuacji w stronę rumuńskiej granicy. W miarę jak kończyło się paliwo dla samochodów kolumny ewakuacyjnej, personel, sprzęt i dokumenty były upychane w coraz mniejszej liczbie pojazdów. Wreszcie pod Łuckiem trzeba było spalić skrzynie z dokumentacją i zakopać sprzęt, aby ratować najważniejsze aktywa Biura – jego personel. Kiedy w październiku 1939 r. zespół Biura Szyfrów zebrał się w Paryżu, dysponował dwoma egzemplarzami Enigmy. Mógł liczyć także na pamięć i doświadczenie kryptologów.

W tym momencie zaczęła przynosić efekty decyzja o podzieleniu się sekretem Enigmy z kryptologami z Francji i Wielkiej Brytanii. Dokumenty i egzemplarze maszyny przekazane aliantom w rezultacie lipcowego spotkania w Pyrach były bezpieczne i pozwalały Polakom skupić się na wznowieniu dekryptażu, zamiast na praco- i czasochłonnym odtwarzaniu stanu wiedzy sprzed września 1939 r. W tym samym czasie brytyjscy kryptolodzy uważnie studiowali materiały otrzymane z Polski. Świadczą o tym raporty spisane przez szefów poszczególnych sekcji już

po zakończeniu działań wojennych. Conel H.O'D. Alexander zapisał w swej *Kryptograficznej historii prac nad Enigmą Kriegsmarine*, że:

> (…) prawie wszystkie wczesne prace nad Enigmą zostały wykonane przez polskich kryptologów, którzy tuż przed rozpoczęciem wojny przekazali szczegółowy opis swych bardzo wartościowych wyników. (…) Spoglądając wstecz na pracę Polaków i uwzględniając, jak niewiele wiedziano wtedy na temat szyfrów maszynowych oraz jak skromnym wyposażeniem mechanicznym dysponowali, przepełnia nas poczucie podziwu dla osiągniętych przez nich rezultatów. (…) Nasze późniejsze sukcesy zawdzięczały wiele ich wczesnym wysiłkom.

A.P. Mahon podziela opinię Alexandra. W oficjalnej *Historii Baraku 8* pisze: *Prawie cała wczesna praca nad Enigmą Kriegsmarine została wykonana przez Polaków, którzy przekazali szczegóły swych znaczących osiągnięć tuż przed wybuchem wojny*. Uwaga zawarta w raporcie Mahona potwierdza, że *Polacy opracowali nową metodę, która zasługuje na znaczące zainteresowanie. Ich opis tej metody, sporządzony w nieco napuszonym języku niemieckim, istnieje do dzisiaj i stanowi interesującą lekturę dla wszystkich, którzy mieli styczność z maszyną*. Mahon objął kierownictwo Hut 8 dopiero w końcowej fazie wojny, toteż znał wczesny okres pracy nad szyfrem jedynie z relacji (głównie Alana Turinga) oraz zachowanych dokumentów. Jego komentarz potwierdza, że kompendium przygotowane przez kryptologów polskiego Biura Szyfrów dla uczestników spotkania w Pyrach było dostępne w Bletchley Park w okresie bezpośrednio po zakończeniu II wojny światowej. Z drugiej strony wzmianka Mahona jest ostatnim śladem tego memorandum, który przekazały dostępne źródła; od tamtej pory aż do dzisiaj nikomu nie udało się go odnaleźć w archiwach, choć zgodnie z logiką systemu winno się w nich znajdować i zostać odtajnione wraz z pozostałymi dokumentami obrazującymi wczesny okres zmagań z niemieckim szyfrem.

Dostępność memorandum w alianckich archiwach stanowi istotny element dyskusji nad rolą i wkładem polskich kryptologów nie tyle w złamanie szyfru Enigmy, ile w zainicjowanie rewolucji w kryptologii, która umożliwiła wczesny sukces, a w dalszej perspektywie – przeobraziła oblicze tej dyscypliny. Brak rzetelnych, pochodzących z pierwszej ręki, informacji na temat wkładu poszczególnych państw w zwycięstwo nad Enigmą sprawił, że jeszcze w czasie II wojny światowej zaczęła się pojawiać narracja prezentująca osiągnięcia polskich kryptologów w krzywym zwierciadle. Ówczesny szef brytyjskich kryptologów zapisał po powrocie z Warszawy, że jeszcze na miejscu:

> (…) kiedy wsiedliśmy do samochodu [Knox] nagle otworzył się i zakładając, że żadna z osób towarzyszących nie zna angielskiego pieklił się, że [Polacy] kłamią tak samo, jak robili w Paryżu. [Cały ich sukces] był oparty na kradzieży. Nigdy tego nie rozpracowali, musieli to ukraść przed laty, a następnie obserwowali rozwój, jak każdy by potrafił, jednak na początku musieli to ukraść lub kupić.

W raporcie przedstawionym po powrocie do Londynu, datowanym na 30 lipca, Knox zmienił nieco spojrzenie. Pisał:

> Spójrzmy na sprawę wprost. Polacy czytali maszynę do 15 września 1938 r. dzięki szczęściu. (…) Jeśli chcemy tego [dekryptażu Enigmy] spróbować, musimy prze-

analizować ich system i statystyki (jeśli je mamy) ze znacznym sceptycyzmem. (…) Jestem przekonany, że Schessky [Ciężki] niewiele wie o maszynie i zapewne próbuje ukrywać przed nami fakty. Młodzi ludzie [trójka kryptologów] wydają się zdolni i uczciwi.

Jeżeli Knox, który uczestniczył w spotkaniu w Pyrach, przedstawił na tyle nierzetelny obraz wydarzeń, to inni kronikarze, którzy nie byli bezpośrednio zaangażowani we wczesny etap współpracy kryptologów, byli skazani na spekulacje i powtarzanie tez wynikających z niewiedzy lub uprzedzenia. Tymczasem okoliczności ułożyły się tak, że wśród kronikarzy dokumentujących prace i osiągnięcia komórek ośrodka w Bletchley Park bezpośrednio po zakończeniu II wojny światowej nie znalazł się nikt, kto byłby czynnie zaangażowany we wczesny etap współpracy. Sam Dilly Knox odszedł w lutym 1943 r., pokonany przez chorobę, z którą walczył jeszcze przed wizytą w Pyrach. Alastair Denniston został w lutym 1942 r. odsunięty ze stanowiska szefa ośrodka Bletchley Park i przeniesiony na stanowisko szefa części G.C.&C.S. zajmującej się łamaniem kodów i szyfrów dyplomatycznych. Nie uczestniczył tym samym w redagowaniu powojennych raportów dotyczących roli ośrodka, którego pracami kierował przez około połowę wojny. Wreszcie Alan Turing, który co prawda nie uczestniczył w konferencji w Pyrach, ale znał jej rezultaty bezpośrednio od Knoxa i Dennistona, także został skłoniony na przełomie 1942 i 1943 r. do porzucenia Bletchley Park, w związku z czym nie wniósł wkładu w sprawozdania redagowane po wojnie. Ich opracowanie spoczęło w rękach ludzi, którzy interesujące nas wydarzenia znali z drugich lub trzecich ust. W tej sytuacji jest zrozumiałe, że nawet w raportach spisywanych przez osoby tak rzetelne i systematyczne, jak Stuart Milner-Barry, pojawiły się nuty stanowiące dysonans w stosunku do wydarzeń historycznych. W redagowanej przez siebie części raportu *Historia Baraku 6* Milner-Barry pisze:

Nie jest historycznie pewne, w jaki sposób Polacy otrzymali połączenia wirników i nie jest to kwestia, co do której byli oni szczególnie komunikatywni. Z pewnością w znacznym stopniu wykorzystywali pracę tajnych agentów i jest najbardziej prawdopodobne, że otrzymali fotografie kluczy i depesz z odpowiadającym tekstem jawnym. Przyznali, że kluczowy element, połączenia walca wejściowego otrzymali od agenta, choć utrzymywali, bez wątpienia słusznie, że mogli byli zrekonstruować je także matematycznie.

Wątek kradzieży i tajnych agentów miał z czasem zrobić prawdziwą karierę. Historia złamania szyfru Enigmy nie została ujawniona planowo, lecz przyszła na świat jako wcześniak, przynajmniej w opinii brytyjskich i amerykańskich sukcesorów ośrodka Bletchley Park. Kilka niepublikowanych wypowiedzi oraz szczątkowych wzmianek we wczesnych publikacjach świadczy o tym, że zarys prawdy był znany w środowisku brytyjskich historyków już w połowie lat 60. XX w. Znał go, jak się wydaje, co najmniej kontrowersyjny brytyjski historyk David Irving. Zapewne świadomy swojej reputacji w środowisku historyków, musiał uznać, że bezpiecznie będzie włożyć najważniejsze kwestie w cudze usta. Wybrał do tego renomowanego historyka z London School of Economics, Donalda Camerona Watta. Ten, w przedmowie do opublikowanej w 1968 r. książki Irvinga *Breach of Security* napisał, że (...) *Wielka Brytania otrzymała od polskiego wywiadu klucze oraz wyposażenie umożliwiające odczytywanie niemieckich depesz wojskowych i dyplomatycznych*.

Ani niedyskrecja Watta, ani o rok wcześniejszy sygnał z Polski (jednozdaniowa wzmianka o łamaniu niemieckich szyfrów przez przedwojenny polski wywiad, zawarta w książce Władysława Kozaczuka *Bitwa o tajemnice*) nie zwróciły uwagi historyków ani weteranów kryptologii. Dopiero opublikowanie w 1973 r. książki francuskiego emerytowanego generała Gustave'a Bertranda *Enigma ou la plus grande énigme de la guerre 1939–1945* rozpętało burzę. Wydaje się zresztą, że stało się tak w mniejszym stopniu ze względu na sensacyjne ujawnienie złamania Enigmy, a w większym – na skutek zawartego w książce ładunku historycznych przeinaczeń oraz tradycyjnych francuskich uszczypliwości pod adresem perfidnych Anglików. Sprawiły one, że publikacji francuskiego generała nie można było po prostu przemilczeć, ale jednocześnie w żadnym wypadku nie wolno było potwierdzić prezentowanej przezeń wersji historii nawet w tych przypadkach, w których Bertrand uczciwie relacjonował wydarzenia, i to nie tylko z uwagi na wrażliwość brytyjskiego sumienia. Była pierwsza połowa lat 70. XX w., Europa była podzielona żelazną kurtyną, w najlepsze trwała cicha konfrontacja pomiędzy Zachodem i światem komunizmu. Kryptolodzy obu obozów nadal polegali na maszynach szyfrujących, których konstrukcja wywodziła się od Enigmy. Przyznanie, że Enigma była łamana już w czasie II wojny światowej stanowiłoby oczywiste, skierowane do przeciwnika ostrzeżenie dotyczące bezpieczeństwa jego obecnych szyfrów.

Służby specjalne Wielkiej Brytanii i USA najwyraźniej uznały, że rewelacje Bertranda są przedwczesne. Ponieważ dekryptaż Enigmy został ujawniony i nie można było tej sprawy z powrotem zamieść pod dywan, trzeba było posłużyć się starym jak świat sposobem – dezinformacją. Do jej rozpowszechniania Brytyjczycy namówili weterana wywiadu z okresu II wojny światowej, Frederica Winterbothama. Winterbotham był swego czasu jednym z twórców systemu dystrybucji informacji pochodzących z dekryptażu do najważniejszych agend rządowych i sztabów, jednak w tej roli nie miał żadnego kontaktu z kryptologicznym warsztatem. W opublikowanej w 1974 r. książce *The Ultra Secret* zawarł wiele ciekawostek dotyczących m.in. tzw. brązowej bogini – maszyny służącej do łamania szyfru. Z punktu widzenia jego mocodawców najważniejszy okazał się zapewne fragment relacjonujący historię udziału Polaków w zwycięstwie nad Enigmą:

> W 1938 roku w fabryce we wschodnich Niemczech, która (…) produkowała pewien rodzaj sprzętu łącznościowego, był zatrudniony polski mechanik. (…) We właściwym czasie młody Polak został (…) sekretnie przeszmuglowany pod fałszywym paszportem (…), zainstalowany w Paryżu, gdzie dostał do swej dyspozycji warsztat. Tam pod opieką przydzielonego stolarza zaczął pracować nad drewnianą makietą urządzenia, w którego produkcji uczestniczył w Niemczech.

Rok później inny Brytyjczyk, Anthony Cave Brown, opublikował książkę *Bodyguard of Lies*, w której zawarł podobną historię:

> Gibson [szef stacji MI6 w Pradze] (…) spotkał polskiego Żyda [zatrudnionego wcześniej przy produkcji maszyny], który zaoferował MI6 sprzedaż za 10.000 funtów swej wiedzy na temat Enigmy. (…) Po sprawdzeniu jego wiarygodności, jak głosi historia, MI6 zainstalowało go w apartamencie w Paryżu, gdzie Lewiński odtwarzał z pamięci dane Enigmy.

Wreszcie w 1976 r. William Stevenson opublikował biografię Sir Williama Stephensona, w czasie wojny szefa komórki brytyjskiego wywiadu w USA, pt. *A Man Called Intrepid*, w której przedstawił nieco odmienną wersję zdobycia przez Polaków sekretu Enigmy: *Polska zdobyła Enigmę w początku 1939 roku, gdy jej agenci uprowadzili wojskową ciężarówkę dostarczającą maszyny Enigma w rejon przygraniczny*. Wersje przedstawiane kolejno przez brytyjskich pisarzy różniły się wzajemnie. Zawierały jednak punkt wspólny, który stanowił ich najważniejszy element, a zarazem element spójny ze spekulacjami Knoxa i jego następców z Bletchley Park: sukces Polaków w zmaganiach z Enigmą był oparty na kradzieży lub zdobyciu w inny sposób egzemplarza maszyny. Był w nim zawarty czytelny komunikat dla kryptologicznego adwersarza: tak długo, jak długo jesteście w stanie chronić fizyczne bezpieczeństwo waszych maszyn szyfrujących, wasze szyfry są także bezpieczne.

Jeżeli rewelacje brytyjskich historyków były, jak zakładamy, świadomą dezinformacją, jej poziom budził zakłopotanie i zapewne nie był w stanie wprowadzić w błąd funkcjonariuszy tajnych służb. Ale przyniósł nieoczekiwany efekt uboczny, którego skutki do dnia dzisiejszego stawiają barierę na drodze poznania historycznej prawdy o złamaniu Enigmy. W połowie lat 80. XX w. Brytyjczycy musieli uznać, że maszyny bazujące na Enigmie powoli wychodzą z użycia, a zatem prawda o tej maszynie nikomu już nie może zaszkodzić, i rozpoczęli stopniowe ujawnianie dokumentów źródłowych dotyczących jej historii. Od końca lat 80. każdy, kto pragnie poznać dzieje złamania Enigmy, bez większych trudności może zapoznać się z podstawowymi dokumentami źródłowymi i podsumowaniami opracowanymi z udziałem weteranów alianckich ośrodków kryptologicznych. Mimo to współcześni historycy mają tendencję do powtarzania z upodobaniem dawnych dezinformacji. Norman Davies w opublikowanej w 2006 r. książce *Europa walczy 1939–1945. Nie takie proste zwycięstwo* rolę Polaków w złamaniu Enigmy opisał następująco: *Przedwojenny polski wywiad dowiedział się, że niemiecka armia rozwija* (…) *kod bazujący na komercyjnej maszynie zwanej 'Enigma'. Polscy agenci przedostali się do fabryki, w której była produkowana zaawansowana wersja maszyny i zdobyli jej projekty*. W 2010 r. Richard Aldrich przedstawił w swej książce *GCHQ. The Uncensored Story of Britain's most secret intelligence agency* jeszcze jedną wersję polskiej zdobyczy: *Zanim polski wywiad musiał uciekać z Warszawy, jego agenci osiągnęli znakomity sukces, kradnąc kilka egzemplarzy wojskowej Enigmy z niemieckiej fabryki, w której maszyna była produkowana*.

W tym kontekście zrozumiałe stają się wieloletnie starania polskich historyków o odnalezienie w alianckich archiwach oraz ujawnienie kopii memorandum przekazanego przez Polaków w Pyrach. To memorandum, jeżeli się zachowało, stanowi najbardziej autorytatywne potwierdzenie i podsumowanie wkładu Polaków w złamanie szyfru Enigmy. Można argumentować, że tę rolę mogą odegrać także inne dokumenty opracowane przez polskich kryptologów w różnych okresach ich działalności. Mowa tu przede wszystkim o tzw. Dokumencie L stanowiącym załącznik do raportu płk. Gwidona Langera dotyczącego przedwojennej działalności polskiego Biura Szyfrów. Dokument, opracowany zapewne w pierwszej połowie 1940 r., został zlokalizowany w zbiorach Instytutu Polskiego i Muzeum im. gen. Sikorskiego w Londynie. Jego skrótowy charakter pozwala się domyślać, że stanowi próbę rekonstrukcji z pamięci źródeł utraconych w trakcie ewakuacji z Polski i w konsekwencji nie oddaje w pełni zakresu informacji przekazanych aliantom w lipcu 1939 r. Dwie części powojennych wspomnień Mariana Rejewskiego zostały utrwalone odpowiednio w 1967 i 1974 r.; dystans czasowy wobec opisywanych wydarzeń oraz brak dostępu do choćby szczątkowych dokumentów

źródłowych także ograniczają ich użyteczność jako punktu odniesienia do analizy polskiego wkładu w złamanie szyfru. Co więcej, oba dokumenty zachowały się wyłącznie w polskich archiwach, co w pewnej mierze ogranicza potencjał ich wykorzystania w dyskusji nad rolą kryptologów kilku krajów w triumfie nad Enigmą.

Dotychczasowe starania o odnalezienie w wojennych archiwach aliantów Polski kopii raportu z Pyr pozostają bezskuteczne. Jednak w 2016 r. autor trafił w archiwum francuskich sił zbrojnych na dokument, który zapewne jest skróconą wersją poszukiwanego raportu, bazującą na pełnym tekście, do którego autorzy musieli mieć dostęp i który uzupełnili opisem wydarzeń pomiędzy lipcem 1939 i czerwcem 1940 r. W konsekwencji dokument stanowi najpełniejsze znane obecnie podsumowanie wkładu Polaków w złamanie Enigmy, pochodzące z zasobów archiwalnych aliantów. Jest on częścią zespołu akt odtajnionych 2 grudnia 2015 r. decyzją Direction Générale de la Sécurité Extérieure i przeniesionych do archiwum Service Historique de la Defense w Vincennes[1]. Skład zespołu akt jednoznacznie wskazuje na to, że stanowią one część prywatnego archiwum emerytowanego generała armii francuskiej, Gustave'a Bertranda, wojennego zwierzchnika polskich kryptologów. Skądinąd wiadomo, że w ramach likwidacji półkonspiracyjnego ośrodka kryptologicznego, który działał od listopada 1940 do listopada 1942 r. w pobliżu Uzés w nieokupowanej części Francji, Bertrand ukrył archiwum – zamurował je w domu swojej matki w Grasse. Po wyzwoleniu południa Francji w 1944 r. dokumenty odzyskał, jednak bezpośrednio po jego śmierci 23 maja 1976 r. posiadłość w Théoule-sur-Mer (w którym pełnił funkcję mera) została przeszukana przez przedstawicieli armii, którzy skonfiskowali znaczną ich część. Sądząc z przekazanych przez wdowę po generale informacji dotyczących objętości zajętych akt, zespół ujawniony w 2015 r. stanowi jedynie skromną część archiwum Bertranda.

Niedatowany i niepodpisany maszynopis został oznaczony w wykazie akt jako notatka techniczna w języku niemieckim (*Notice technique en allemande*); towarzyszy mu rękopiśmienne tłumaczenie na język francuski. Zbieg zdarzeń sprawił, że znamy okoliczności i powody powstania dokumentu. Powojenny raport płk. Langera z działalności Ekspozytury 300 oraz ewakuacji ośrodka z Francji[2] zawiera informację, że:

> (…) w Fuzach (nasze m.p.) prosił Bolek o napisanie elaboratu, w którym w sposób obiektywny przedstawiono, w jakiej mierze każdy z trzech partnerów przyczynił się do rozwiązania zagadnienia maszyny Enigmy. Elaborat opracowali por. Rejewski i Zygalski. Gdy Bolek go przestudiował, powiedział on, że całą pracę musi przerobić, bo czytając go w obecnej formie odnosi się wrażenie, jakoby Francuzi prawie nic nie zrobili.

Kwestia autorstwa memorandum jest nieco złożona. Langer wskazuje, że opracowali je Marian Rejewski i Henryk Zygalski, co może wskazywać na jego powstanie w okresie po śmierci Jerzego Różyckiego lub co najmniej w czasie jego pobytu w Afryce Północnej w 1941 r. Z drugiej strony chronologia wydarzeń opisanych w dokumencie obejmuje okres do drugiej połowy czerwca 1940 r. Ze wspomnień Bertranda oraz raportów Langera wiadomo, że kryptolodzy kontynuowali dekryptaż Enigmy co najmniej w ciągu 1941 r. Można przypuszczać, że memorandum opracowane w tymże roku albo później zawierałoby choć szczątkowe odniesienia do tych

[1] Service Historique de la Defense, SHD DE2016 ZB25.
[2] IJP 709/133/5, s. 39.

prac. Ich brak wskazuje na drugą połowę 1940 r. jako najbardziej prawdopodobny okres powstania dokumentu. We wspomnieniach Mariana Rejewskiego widnieje informacja, że we wczesnej fazie pracy w ośrodku P.C. Cadix Francuzi mieli problemy z dostarczeniem kryptologom szyfrogramów. Aby czymkolwiek zająć zespół, którego morale szwankowało w wyniku narzuconej przeprowadzki do Francji, Bertrand dostarczył kryptologom pakiet szwajcarskich depesz szyfrowanych za pomocą komercyjnej Enigmy, które Polacy szybko złamali. Opracowanie podsumowań i sprawozdań należy do klasyki działania każdej biurokracji, jest więc prawdopodobne, że analizowany dokument powstał w drugiej połowie 1940 r., gdy francuscy zwierzchnicy usiłowali zająć kryptologów jakąkolwiek pracą. Jeśli jednak ten domysł jest poprawny, to memorandum jest najprawdopodobniej zbiorowym dziełem całej trójki: Rejewskiego, Różyckiego i Zygalskiego. Pominięcie Różyckiego przez Langera w raporcie składanym już po zakończeniu wojny może być podyktowane psychologicznym wyparciem postaci kryptologa po jego przedwczesnej śmierci. Skądinąd wiadomo, że w trakcie przesłuchania na zamku Eisenberg w marcu 1944 r. Langer powoływał się na prace dwóch matematyków, najwyraźniej dostosowując swoje wspomnienia (lub co najmniej zeznania) do rzeczywistości po śmierci Różyckiego. W powojennym raporcie mógł zadziałać identyczny mechanizm.

Dokument nosi tytuł *ENIGMA. Kurzgefasste Darstellung der Auflösungsmethoden* (pol. *Enigma. Zarys metod rozwiązania*). Odwołanie do skrótu użyte w tytule sugeruje istnienie pełnej wersji tego samego tekstu. Jedynym dokumentem, który mógł pełnić taką rolę, mógł być raport przygotowany dla uczestników spotkania w Pyrach. Wskazuje na to kilka elementów. Po pierwsze wiadomo, że raport z Pyr został opracowany w języku niemieckim, jedynym, w jakim mogli się komunikować wszyscy uczestnicy spotkania. Zważywszy na okoliczności opracowania analizowanego tekstu, nie istniały żadne powody, aby w dalszym ciągu sięgać po pomoc języka przeciwnika. Opracowanie dokumentu w języku niemieckim wskazuje na to, że stanowił on, zgodnie z tytułem, skrót tekstu źródłowego opracowanego właśnie w tym języku. Drugą okolicznością wskazującą na to, że autorzy mieli dostęp do swojego pierwotnego raportu jest jego szczegółowość, zwłaszcza w zestawieniu z wcześniejszym o co najmniej pół roku „Dokumentem L". Ten ostatni ma objętość odpowiadającą około połowie analizowanego tekstu i pomija kilka interesujących, zawartych w nim wątków. Dotyczy to szczególnie kilku sekcji poświęconych analizie szyfrów Kriegsmarine. Powojenne komentarze brytyjskich kryptologów jednoznacznie potwierdzają, że Polacy podzielili się z nimi wynikami swoich prac dotyczących wykorzystania Enigmy przez niemiecką marynarkę. Dalej wskażemy także, że Brytyjczycy nigdy nie zdołali wyjść poza i ponad rezultaty osiągnięte przez Polaków wyłącznie na gruncie kryptologicznej teorii. Rozpoznanie brakujących elementów szyfru oraz finalne złamanie szyfru Enigmy Kriegsmarine zawdzięczali dokumentom znalezionym na pokładzie zdobytych okrętów przeciwnika. Tymczasem w znanych dotąd polskich źródłach („Dokument L" oraz *Wspomnienia* Mariana Rejewskiego) dekryptaż Enigmy Kriegsmarine został jedynie zasygnalizowany, bez podawania szczegółów. Zestawienie brytyjskich raportów z treścią polskich dokumentów jednoznacznie wskazuje, że Brytyjczycy odwoływali się do innego dostarczonego przez Polaków dokumentu niż teksty znane do tej pory. Obszerne informacje na temat historii dekryptażu szyfrów Kriegsmarine przez polskie Biuro Szyfrów pojawiają się po raz pierwszy właśnie w analizowanym dokumencie.

Różnice pomiędzy domniemanym oryginałem i ujawnionym dokumentem nie ograniczają się do skrótów. Raport przygotowany w związku z konferencją w Pyrach siłą rzeczy nie mógł objąć jej samej ani wydarzeń, które nastąpiły po niej. Omawiany dokument doprowadza narrację do punktu bezpośrednio poprzedzającego domniemany czas jego redakcji. Dzięki temu mamy możliwość poznania wydarzeń obserwowanych z polskiego punktu widzenia aż do kapitulacji Francji. Raport obejmuje konferencję w Pyrach oraz wczesny okres alianckiej, trójstronnej współpracy kryptologicznej. Autorzy dostarczają informacje o najwcześniejszych sukcesach brytyjskich kryptologów: od metody ataku opracowanej przez Dilly'ego Knoxa, aż po zmianę procedury szyfrowania poprzedzającą kampanię francuską i jej pokonanie dzięki zastosowaniu metody Herivela. Ostatni rozdział potwierdza okoliczności powstania raportu przekazane przez Gwidona Langera: zawiera wyliczenie elementów wkładu uczestników kryptologicznego aliansu w złamanie szyfrów Enigmy. Można zrozumieć podenerwowanie Gustave'a Bertranda po lekturze dokumentu – na tle dorobku polskich i brytyjskich kryptologów wkład Francuzów w postaci dwóch dokumentów rysuje się nader skromnie.

Znaczna część informacji prezentowanych w raporcie powiela zagadnienia znane z innych, wcześniej dostępnych dokumentów. Jego wyjątkowy charakter sprowadza się do dwóch wartości. Jest on jedynym znanym obecnie dokumentem podsumowującym wkład Polaków w złamanie Enigmy oraz wczesny etap alianckiej współpracy kryptologicznej, pochodzącym z archiwów alianckich. Jednocześnie stanowi najszersze ujawnione do tej pory podsumowanie tego okresu zawarte w źródłach innych niż anglosaskie. Zgodnie z literą rozkazu Bertranda, za którego przyczyną opracowanie powstało, choć zapewne niezupełnie zgodnie z jego intencjami, zakres memorandum pozwala poszerzyć analizę wkładu kryptologów trzech krajów w złamanie Enigmy w stosunku do dotychczasowego stanu wiedzy. Rozpocznijmy zatem przegląd dokumentu od elementów stanowiących istotne nowości.

W rozdziale 2, poświęconym początkom polskich zmagań z Enigmą, Rejewski potwierdza jednoznacznie, że polski wywiad zdobył istotne informacje na temat maszyny na długo przed tym, jak Gustave Bertrand jesienią 1931 r. przekazał Polakom dwa dokumenty pochodzące od Hansa-Thilo Schmidta. Można się było tego domyśleć na podstawie wspomnień Rejewskiego; opisując najwcześniejszy etap ataku na szyfr Enigmy, posługiwał się on nomenklaturą odnoszącą się raczej do Enigmy G niż modelu I, którego dotyczyły rewelacje Bertranda. Większość historyków sugeruje, że dopiero informacje pochodzące od „Asche" pozwoliły kryptologowi zbudować matematyczny model maszyny. Opisany przez Rejewskiego zakres wiedzy Polaków na temat Enigmy oraz posługiwanie się terminologią odnoszącą się do Enigmy G wskazują, że rozpoczął on pracę nad matematycznym modelem maszyny na podstawie danych zdobytych samodzielnie przez polski wywiad. Dokumenty dostarczone przez Bertranda jedynie potwierdziły i uszczegółowiły przyjęte założenia.

Rozdział 4 stanowi kompromis pomiędzy zobowiązaniami wobec zleceniodawcy pracy i własną dumą zawodową. Z informacji uzyskanych od Langera wiadomo, że raport powstał na zlecenie majora Bertranda i miał zaprezentować wkład trzech krajów w załamanie Enigmy. Znając z innych źródeł charakter Bertranda, możemy założyć, że oczekiwał on potwierdzenia znaczącej, jeśli nie najważniejszej, roli Francji oraz własnej w tym sukcesie. Jego przekonanie o decydującej roli w przedsięwzięciu umacniały chociażby pochlebstwa zawarte w korespondencji z brytyjskim partnerem. Dnia 3 sierpnia, wkrótce po powrocie z Polski, szef brytyjskich

kryptologów Alastair Denniston pisał do Bertranda: (…) *pragnę podkreślić, że zawdzięczamy wszystko wyłącznie Panu, liczę na przyszłą współpracę naszego trio, w której Pan musi zająć wiodącą pozycję*. W tych okolicznościach kryptolodzy musieli wskazać na jakąkolwiek okoliczność pozwalającą docenić rolę Francji i Francuzów. Znaleźli ją w dokumentach dostarczonych Polakom jesienią 1932 r. Odnotowali, że (…) *posiadanie dokumentów, a w szczególności klucza dziennego, w rozstrzygający sposób wpłynęło na postęp prac. Bez nich rozwiązanie szyfru Enigmy opóźniłoby się co najmniej o lata*. Pierwsze zdanie stanowi dodatkowe potwierdzenie wniosku sformułowanego powyżej. Autorzy raportu podnoszą znaczenie wyłącznie znajomości klucza dziennego, dając tym samym do zrozumienia, że dostarczona instrukcja obsługi Enigmy nie była dokumentem decydującym o wyniku ich prac. Oznacza to najprawdopodobniej, że Rejewski był w stanie zbudować matematyczny model maszyny na podstawie informacji zdobytych przez polski wywiad wcześniej i samodzielnie. Polacy podkreślają rozstrzygające znaczenie znajomości kluczy dziennych wyłącznie po to, aby natychmiast zrelatywizować to twierdzenie; bez niego rozwiązanie szyfru Enigmy zapewne także okazałoby się możliwe, choć (…) *opóźniłoby się co najmniej o lata*. Temat rozwiązania Enigmy bez dokumentów dostarczonych przez Francuzów powraca nieco później, gdy w rozdziale 7 autorzy szkicują zarys metody, która ich zdaniem pozwoliłaby złamać szyfr także bez pomocy z zewnątrz. Współcześni kryptolodzy potwierdzili, że zarysowana metoda rzeczywiście prowadzi do złamania szyfru, pod warunkiem zrealizowania pewnych założeń. Brak depesz archiwalnych z tego okresu nie pozwala potwierdzić, że te założenia rzeczywiście zostały spełnione. Musimy zatem przyjąć zapewnienie autorów, że wkład Francuzów okazał się decydujący dla sukcesu w zmaganiach z Enigmą, choć to twierdzenie odnosi się wyłącznie do praktyki dekryptażu. Dostarczone dokumenty przyspieszyły złamanie szyfru co najmniej o rok. Jednak po potwierdzeniu tego, Rejewski i jego koledzy natychmiast osłabili siłę własnego argumentu i wykazali, że na gruncie teorii kryptologicznej poradziliby sobie także bez dostarczonych kluczy, łamiąc Enigmę metodami czysto matematycznymi.

Redagując rozdział 6, autorzy nie zdawali sobie sprawy, że tym samym toczą zdalną polemikę z kryptologami brytyjskimi. W rozdziale 5 kryptolodzy opisali, w jaki sposób odtworzyli połączenia walca wejściowego:

> (…) problem sprowadzał się do nieznajomości podstawienia E. Wydaje się, że właśnie na nim załamały się wysiłki kryptologów brytyjskich. Późniejsze badania polskiego Biura Szyfrów dowiodły, że podstawienie E może zostać wyznaczone analitycznie (pod warunkiem znajomości podstawienia S), w rzeczywistości jednak znaleziono je metodą prób i błędów.

Takie określenie niezupełnie oddaje istotę sukcesu Mariana Rejewskiego. Dla rekonstrukcji podstawienia E posłużył się on nie tyle metodą prób i błędów, ile swoją intuicją i znajomością tajników niemieckiej duszy. Wiedząc, że w handlowym modelu maszyny połączenia walca wejściowego odpowiadają układowi klawiszy maszyny założył, że w modelu wojskowym systematyczni Niemcy także sięgnęli po jakąś formę porządku. Najprostszą możliwością był układ alfabetyczny i to właśnie on okazał się poprawnym rozwiązaniem. Sukces osiągnięty na skróty nie usatysfakcjonował jednak Rejewskiego i z czasem opracował on również czysto analityczną metodę rekonstrukcji połączeń walca, którą opisano w rozdziale 6 raportu. Autorzy nie byli świadomi, że w brytyjskich raportach z Warszawy i w późniejszych

opracowaniach brytyjskich kryptologów rekonstrukcja walca wejściowego stała się jednym z kluczowych zagadnień. Dilly Knox już w pierwszym raporcie z Warszawy[3] zauważył, że (…) *Polacy czytali maszynę do 15 września 1938 r. dzięki szczęściu*. Odnosił się do odnalezienia przez Rejewskiego połączeń walca wejściowego, przypisując większą rolę szczęściu niż psychologicznej intuicji kryptologa. W trakcie spotkania w Pyrach Rejewski najwyraźniej usiłował przekonać rozmówcę, że niezależnie od rozwiązania opartego na intuicji opracował także matematyczną metodę rekonstrukcji połączeń walca. Ten fragment rozmowy musiał toczyć się w języku francuskim, Brytyjczyk zanotował bowiem deklarację Polaków w wersji (…) *nous l'aurion pu trouver aussi par mathematique*[4], po czym udał słabą znajomość tego języka i dodał, że deklaracja zapewne odnosiła się do daty znalezienia rozwiązania. W raporcie powojennym, w 1945 r., Milner-Barry zapisał[5], że (…) *kluczowy element, połączenia walca wejściowego, otrzymali od agenta, choć utrzymywali, bez wątpienia słusznie, że mogli byli zrekonstruować je także matematycznie*. Narracja zainicjowana przez Knoxa, zgodnie z którą łut szczęścia miał być decydującym czynnikiem sukcesu Polaków, wkrótce po zakończeniu wojny rozwinęła się w wersję pokutującą następnie przez dziesięciolecia: w złamaniu Enigmy kryptologów wyręczyli agenci. Ta narracja utrzymywała się mimo tego, że w alianckich archiwach były dostępne dokumenty jednoznacznie potwierdzające intelektualną uczciwość Polaków.

Treść rozdziału 13 w zasadzie jest znana także z innych dokumentów, w których opisano polskie metody łamania szyfru, mimo to zasługuje na krótki komentarz. Opisano w niej metodę identyfikacji prawego wirnika z wykorzystaniem metody zaproponowanej przez Jerzego Różyckiego i znanej w gronie polskich kryptologów jako „metoda zegara". Metoda, o której mowa, wykorzystuje właściwość szyfru opisaną pierwotnie w 1922 r. przez ojca współczesnej kryptologii amerykańskiej, Williama Friedmana, i określaną współcześnie mianem indeksu koincydencji. Od dawna zainteresowanie badaczy budziło to, że opis metody stosowanej przez Polaków w najmniejszym stopniu nie odwoływał się do terminologii zaproponowanej przez jej pierwotnego odkrywcę. Oryginalna praca Williama Friedmana zawierająca opis indeksu koincydencji została utajniona niezwłocznie po publikacji i doczekała się odtajnienia dopiero w latach 70. XX w. Krótki okres jej dostępności sprawił, że jej podstawowe ustalenia były znane w wybranych kręgach kryptologów, zwłaszcza w USA i we Francji (w której wydano reprint pracy Friedmana). Nasuwa się pytanie, czy Jerzy Różycki lub którykolwiek z jego kolegów poznał koncepcję indeksu koincydencji w trakcie szkolenia, czy też opracował ją samodzielnie, odkrywając jedno z najważniejszych narzędzi współczesnej kryptologii niezależnie od Friedmana? Marian Rejewski zapisał, że już we Francji odkrył, iż program kursu kryptologicznego realizowanego w Poznaniu w 1929 r. był ściśle oparty na książce jednego z największych kryptologów francuskich – Marcela Givierge'a, zatytułowanej *Cours de cryptographie*. W dostępnym współcześnie angielskim tłumaczeniu tej książki nazwisko Friedmana i wzmianka o indeksie koincydencji występują wyłącznie w jednozdaniowym przypisie odsyłającym do publikacji niedostępnej w okresie pracy Polaków nad szyfrem. W tej sytuacji znaczenia nabiera treść oryginalnego, francuskojęzycznego wydania książki. Być może indeks koincydencji został w nim omówiony szerzej? Poszukiwania autora prowadzone wspólnie z Philippem Guillotem

[3] Por. cytat na s. 2.
[4] (…) *mogliśmy* [je] *znaleźć także* [metodami] *matematycznymi*.
[5] Por. cytat na s. 3.

pozwoliły dotrzeć do oryginalnego wydania publikacji. Wzmianka o indeksie koincydencji ma w nim strukturę identyczną, jak w tłumaczeniu angielskim; Polacy nie mogli zeń poznać natury narzędzia. To spostrzeżenie nie rozstrzyga samo przez się o możliwości niezależnego odkrycia indeksu koincydencji przez Jerzego Różyckiego, choć zwiększa prawdopodobieństwo takiego biegu wydarzeń.

W literaturze zwykło się przyjmować, że zmiana sposobu użycia Enigmy wprowadzona 15 września 1938 r. pokonała metody dekryptażu wykorzystywane przez Polaków, uzależniając dalsze czytanie szyfrogramów sporządzanych przy pomocy tej maszyny od dwóch nowych metod – bomby oraz płacht Zygalskiego. Treść rozdziału 21 potwierdza nieskuteczność większości opracowanych wcześniej metod ataku, przeczy jednak twierdzeniu o oparciu dekryptażu wyłącznie na bombach i płachtach. W tym okresie polscy kryptolodzy mieli już tak głęboką znajomość subtelności szyfru Enigmy, że w wielu wypadkach potrafili sobie radzić, wychwytując zależności znaków klucza depeszy całkowicie nieczytelne dla innych osób. Być może właśnie metody opisane w rozdziale tłumaczą, w jaki sposób Polacy byli zdolni czytać szyfr w pierwszej połowie 1939 r., gdy bomby utraciły skuteczność, a płachty Zygalskiego nie były jeszcze gotowe. Wbrew twierdzeniom kryptologów brytyjskich (por. fragment: (…) *Polacy czytali maszynę do 15 września 1938 r. dzięki szczęściu* w raporcie Knoxa powyżej) Biuro Szyfrów czytało wybrane niemieckie depesze do ostatnich dni przed wybuchem wojny. W rozdziale 27 autorzy raportu podkreślają, że (…) [m]*iesiąc później wybuchła wojna niemiecko-polska. Udało się jeszcze złamać depesze z 25 sierpnia 1939, dnia powszechnej mobilizacji w Niemczech*. W tym czasie bomby były już bezużyteczne, a Polacy posiadali komplety płacht Zygalskiego wyłącznie dla dwóch spośród 60 możliwych kolejności wirników. Skądinąd wiadomo, że w tym okresie klucze do szyfru używane przez niemieckie siły zbrojne obligatoryjnie wykorzystywały co najmniej jeden z nowych wirników wprowadzonych do użytku w grudniu 1938 r., toteż płachty w dyspozycji Biura Szyfrów nie gwarantowały rozwiązania. Polscy kryptolodzy musieli incydentalnie łamać szyfr innymi metodami, zapewne zbliżonymi do zarysowanych w rozdziale 21.

Rozdziały od 27 opisują wydarzenia po wybuchu wojny. W tym okresie Polacy odnoszą się do własnej pracy z dozą cichej rezygnacji:

> (…) polscy kryptolodzy siedzieli bez przerwy nad Enigmami stukając depesze i manipulując płachtami, by nie pozwolić się całkowicie zdystansować Anglikom. Była to całkowicie mechaniczna praca, którą mógł wykonać personel pomocniczy. W tej sytuacji było zrozumiałe, że polscy kryptolodzy nie osiągnęli już istotnych rezultatów kryptologicznych, a punkt ciężkości prac teoretycznych przesunął się do Londynu.

W raporcie Polaków zaczynają się przewijać odniesienia do sukcesów brytyjskich kolegów. Niektóre z nich opierały się zresztą na przedwojennych pracach teoretycznych polskiego Biura Szyfrów: (…) *brytyjscy kryptolodzy urzeczywistnili jeszcze jedną metodę zaproponowaną wcześniej przez Polaków*. Pomysł sprowadzał się do sporządzenia katalogu określającego nie tylko lokalizację przypadków żeńskich, lecz także określenie znaków, których dany przypadek dotyczył. Posiadanie takiego katalogu ułatwiało weryfikację możliwych rozwiązań zidentyfikowanych z wykorzystaniem płacht Zygalskiego. Polacy nie zdołali zrealizować pomysłu samodzielnie, ponieważ ogrom pracy potrzebnej do sporządzenia katalogu wymagał jej automatyzacji. Brytyjczycy, którzy skonstruowali niezbędne urządzenie do wykonania płacht, wykorzystali je obecnie także do realizacji polskiego pomysłu towarzyszącego

płachtom katalogu. (…) [d]*zięki swoim możliwościom finansowym i organizacyjnym* [Brytyjczycy] *wprowadzili w życie nasze plany, które w innym przypadku nie ujrzałyby światła dziennego*. W raportach z wojennej działalności Bletchley Park brak jednak komentarzy wskazujących na polskie pochodzenie idei, która legła u podstaw nowej metody łamania szyfru.

Rozdział 28 został poświęcony w całości spostrzeżeniu Knoxa, które pozwalało łamać bez większego wysiłku depesze wieloczęściowe. W rozdziale 30 opisano metodę Herivela, która w czasie kampanii francuskiej pozwoliła przełamać impas wywołany kolejną zmianą sposobu użycia Enigmy. W tym przypadku Polacy odnotowali choć skromną satysfakcję: do sukcesu młodego brytyjskiego kryptologa dołączyli korekty dotyczące punktów przeskoku nowych wirników: (…) *korekty zostały znalezione i natychmiast zakomunikowane Anglikom. Dopiero po nich metoda Herivela mogła zostać efektywnie zastosowana*. Nie znalazło to jednak odzwierciedlenia w źródłach brytyjskich.

W rozdziale 31 opisano zmiany wprowadzone przez przeciwnika w przededniu kampanii francuskiej. Rezygnacja z dwukrotnego szyfrowania klucza depeszy stanowiła ciężki cios dla Polaków, którzy opierali na nim większość, jeśli nie wszystkie, używane metody dekryptażu. Ale to właśnie Polacy wykryli przygotowywaną zmianę i rozpracowali strukturę nowego systemu. Niektórzy niemieccy szyfranci zastosowali ją przedwcześnie, w przeddzień oficjalnego wprowadzenia. Ponieważ Polacy w tym okresie dysponowali wyprodukowanymi przez Brytyjczyków kompletami płacht Zygalskiego, regularnie łamali klucze niemieckich depesz. Dysponując kluczami do szyfru na dzień 30 kwietnia, zidentyfikowali depesze oparte na procedurze, która miała wejść do powszechnego użytku w dniu następnym. Bez trudu rozpracowali naturę nowego systemu i przekazali jego charakterystykę do Londynu.

Łamanie przez Polaków depesz wymienianych w odrębnej sieci łączności S.D. jest znane z innych źródeł. Analizowany raport zawiera jednak wiele nieznanych dotąd szczegółów. Dane w rozdziale 32 stanowią dodatkowe potwierdzenie łamania przez Polaków depesz Enigmy jeszcze w przededniu wybuchu II wojny światowej: (…) [o]*statnim złamanym dniem był 31 lipiec 1939 r.*

Począwszy od rozdziału 33 mamy do czynienia z informacjami znanymi do tej pory jedynie w zarysie. O samym łamaniu przez Polaków depesz Kriegsmarine było wiadomo z wcześniej dostępnych materiałów, ale jego szczegóły i przede wszystkim zakres pozostawały niedostępne. Wskutek braku danych na temat wkładu Polaków ugruntowało się przekonanie, że główny ciężar zmagań z Enigmą Kriegsmarine wzięli na swe barki kryptolodzy brytyjscy, a największy wkład w późniejszy sukces wniósł Alan Turing. Informacje zawarte w rozdziałach 33–35 zmuszają do ponownej analizy przyjętej wersji historii.

Zmagania z szyframi Kriegsmarine musiały stanowić odrębny obszar zainteresowania polskich kryptologów, pozostający nieco w cieniu wobec innych dziedzin. Do takiego wniosku skłania choćby pozycja rozdziałów poświęconych temu zagadnieniu w całości raportu. Zasadnicza część opracowania ma (z istotnym wyjątkiem, który zostanie skomentowany poniżej) strukturę chronologiczną; rozdziały poświęcone szyfrom Kriegsmarine zostały dorzucone poza chronologią, jakby stanowiły posłowie niezależne wobec całości. Kilka komentarzy rozproszonych w raporcie potwierdza, że z przyczyn czysto praktycznych łączność niemieckiej marynarki nie mieściła się w centrum zainteresowań polskiego Biura Szyfrów. W rozdziale 2 znajdujemy informację, że (…) [j]*eszcze w wiele lat po utworzeniu polskiego Biura Szyfrów*

brak kadr nie pozwalał poświęcać uwagi materiałowi szyfrowemu napływającemu z niemieckiej marynarki. W rozdziale 34 kryptolodzy uskarżają się na trudności w atakach na Enigmę Kriegsmarine wynikające z (…) *niewystarczającego materiału szyfrowego*. Uwzględniając to, że Polska nie była potęgą morską, drugoplanowy charakter prac nad tym właśnie typem Enigmy jest całkowicie zrozumiały. Mimo to Biuro Szyfrów osiągnęło imponujące rezultaty w atakach na szyfry niemieckiej marynarki.

Opis kodów wykorzystywanych przez Kriegsmarine przed wdrożeniem Enigmy (rozdział 33) nie mieści się w zakresie niniejszej analizy. Przygoda Polaków z Enigmą Kriegsmarine rozpoczęła się w sensie formalnym dopiero po wdrożeniu w marynarce z początkiem 1926 r. modelu Enigma C, a w sensie praktycznym – dopiero w roku 1933, gdy kryptolodzy postanowili zastosować wobec archiwalnych depesz metody, które wypracowali i skutecznie zastosowali w ataku na szyfry Enigmy wojsk lądowych. Ten atak przyniósł natychmiastowy sukces, ułatwiony dzięki brakowi łącznicy w Enigmie C. Polacy łatwo i trafnie zidentyfikowali cechy modelu maszyny (29 klawiszy, ruchomy reflektor, specyficzna rola litery X itd.). Zauważyli też najważniejszą cechę szyfrów Kriegsmarine – odmienność wykorzystywanych procedur od używanych w innych rodzajach sił zbrojnych. Od najwcześniejszego okresu trójliterowe klucze depesz nie były wybierane samodzielnie przez szyfrantów, lecz pobierane z listy kluczy; ponadto były one uzupełniane do czterech znaków, co sygnalizowało zamiar przejścia w późniejszym okresie na klucze czteroznakowe.

Opis maszyny zaprezentowany w dokumencie oraz okoliczności jej użycia w Kriegsmarine rodzą kilka pytań, na które brakuje odpowiedzi w związku z obecnym stanem wiedzy. W świetle dostępnej dokumentacji producenta Enigmy model maszyny C używany w Krigsmarine, począwszy od 1926 r., był wyposażony w nieruchomy reflektor, który można było umieścić w urządzeniu w jednym z czterech możliwych położeń. Z notatek polskich kryptologów wynika, że reflektor analizowanej maszyny był ruchomy. Albo kryptologów spisujących raport bez dostępu do źródłowej dokumentacji zawiodła pamięć, albo w naszej wiedzy dotyczącej rodziny maszyn Enigma istnieje luka. W świetle powszechnie przyjętej chronologii 1 października 1934 r. Enigma C została zastąpiona w Kriegsmarine przez model Enigma M1, tożsamy co do zasady z modelem Enigma I wykorzystywanym w armii lądowej (różnice dotyczyły np. opisu pierścieni maszyny: liczbowych w przypadku maszyny Wehrmachtu, literowych w Kriegsmarine). Jednak autorzy raportu przedstawiają sposób wykorzystania Enigmy C jeszcze w 1936 r.: tekst jawny był przed zaszyfrowaniem kodowany znanym z wcześniejszej praktyki kodem czteroznakowym. Stąd wynika wniosek, że Enigma M1 nie tyle zastąpiła Enigmę C, ile została wprowadzona równolegle do niej, a z czasem wyparła starszy model z użytku. Niemieccy kryptolodzy, świadomi słabości wynikającej z braku łącznicy, usiłowali podnieść bezpieczeństwo szyfru tworzonego przez maszynę typu C i wymagali kodowania tekstu jawnego przed jego szyfrowaniem Enigmą. Środki ostrożności, które podejmowali, okazały się jednak bezskuteczne: Polacy rozpracowali zarówno konstrukcję maszyny, jak i nietypowe procedury szyfrowania wiążące się z jej użyciem.

Najbardziej interesujące są zawarte w raporcie informacje dotyczące użycia w Kriegsmarine Enigmy M1, wykorzystywanej w marynarce (z pewnymi zmianami) od 1 października 1934 r. do końca II wojny światowej. Raport zawiera dane o interesującej i wcześniej nieznanej niekonsekwencji kryptologów Kriegsmarine. W wersji wprowadzonej do użytku 1 października 1934 r. Enigma M1 była wyposażona w pięć wirników, spośród których w maszynie montowano tylko trzy (podobnie,

jak w maszynach Wehrmachtu i Luftwaffe, począwszy od grudnia 1938 r.). Pozwalało to na łamanie kluczy depesz w dniach, w których obejmowały one jedynie wirniki znane z Enigmy wojsk lądowych. Stanowiły one około 10 proc. wszystkich depesz. Ta liczba wystarczała na to, aby potwierdzić praktykę znaną z okresu użycia Enigmy C, tj. czerpanie kluczy depesz wyłącznie z listy przygotowanej wcześniej, ale była niewystarczająca do rekonstrukcji ich kompletnej listy. W dniu 16 listopada 1936 r. nieoczekiwanie wycofano z użytku dwa dodatkowe wirniki; pozostawiono wyłącznie wirniki znane z Enigmy Wehrmachtu. Pozwoliło to na łamanie bieżących depesz przy pomocy tych samych metod, którymi łamano depesze wojsk lądowych i lotnictwa. Złamane depesze umożliwiały rekonstrukcję listy kluczy. Lista stanowiła przepustkę do depesz archiwalnych sprzed zmiany – wystarczyło skorzystać ze starej metody rusztu, aby określić połączenia dodatkowych wirników używanych przed listopadem 1936 r. Polacy nazwali je później wirnikami IVM i VM, od M jak *Marine* (marynarka), żeby uniknąć konfuzji ze standardowymi wirnikami IV i V. Odczytanie depesz archiwalnych pozwoliło na zidentyfikowanie (oprócz bazowego) także dwóch specjalnych wariantów szyfru: oficerskiego i sztabowego (admiralskiego). Biuro Szyfrów rozpracowało całkowicie wariant oficerski, dla sztabowego natomiast zabrakło czasu i zapewne materiału szyfrowego.

W dniu 1 maja 1937 r. nastąpiła kolejna zmiana procedury szyfrowania. Odtąd indywidualny klucz depeszy nie był szyfrowany z wykorzystaniem maszyny, ale za pomocą zewnętrznego podstawienia, niezależnego od Enigmy. Podobnie jak przy innych zmianach, Niemcy popełnili przy zmianie procedury błąd, który mógł ich kosztować sekret szyfru. Torpedowiec o sygnale wywoławczym AFA nie otrzymał w porę informacji o nowej procedurze szyfrowania (lub tabel pozwalających na szyfrowanie klucza depeszy) i w ciągu kilku pierwszych dni maja wykorzystywał starą procedurę, rozpracowaną przez polskie Biuro Szyfrów. W rezultacie Polacy odczytali wiele depesz Kriegsmarine z okresu 1–8 maja 1937 r. Okazało się, że ustawienia maszyny nie uległy zmianie od 27 kwietnia do 8 maja, co dało kryptologom obszerny materiał do analiz. Pozwolił on w znacznej mierze określić sposób szyfrowania klucza depeszy. Okoliczności złamania szyfru Kriegsmarine po zmianie w maju 1937 r. są epizodem, który w analizowanym dokumencie jest opisany nieco mniej szczegółowo niż w raportach z Bletchley Park, zwłaszcza w oficjalnej *Historii Baraku 8* pod redakcją Mahona (szczegóły dotyczące sygnału wywoławczego okrętu, którego depesze umożliwiły Polakom włamanie do szyfru, pochodzą właśnie z tego raportu). W konkluzji epizodu Mahon zapisał, że Polacy (…) *stosując opisaną metodę, łamali około 16 depesz dziennie, dochodząc do wniosku, że szyfrowanie klucza depeszy stanowi jakąś formę podstawienia bigraficznego, jednak nie posunęli się znacznie poza ten punkt.* (…) *Polacy zwrócili uwagę na jeszcze jedną możliwość, tzn. że trygramy nie były wybierane przypadkowo*. Opis Mahona potwierdza, że Polacy trafnie zidentyfikowali najważniejsze cechy procedury szyfrowania klucza depeszy, a pójście dalej wymagało rekonstrukcji lub zdobycia tabel używanego w niej podstawienia bigraficznego.

Do tej pory materiał zawarty w polskim raporcie uzupełniał lub korygował informacje zamieszczone w powojennych raportach z Bletchley Park. Dotarliśmy do miejsca, w którym polskie i brytyjskie raporty nieco się rozchodzą. Zgodnie z raportami brytyjskimi Alan Turing poszerzył szczelinę otwartą przez Polaków: *Turing w istocie rozwiązał najważniejszą część problemu klucza depeszy*[6]. W rzeczywistości matematyk nie posunął się poza punkt osiągnięty w 1937 r. przez zespół Biura Szyfrów

[6] A.P. Mahon, *The History of Hut Eight*, United Kingdom 2010, s. 14.

i nie mógł przekroczyć tego punktu tak długo, jak długo tablice bigramów pozostawały nieznane. Zgodnie z oficjalną *Historią Baraku 8* przełom nastąpił dopiero 19 kwietnia 1940 r. W trakcie kampanii norweskiej Brytyjczycy zdobyli i przeszukali uzbrojony niemiecki trawler „Polares". W ich ręce wpadły dokumenty, które (…) *dostarczyły precyzyjnych informacji na temat sposobu szyfrowania klucza depeszy, ustawienia łącznicy i pozycję bazową 23 i 24 kwietnia*[7]. Zdobyte dokumenty ostatecznie potwierdziły trafność wcześniejszych ustaleń Polaków oraz zgodnych z nimi domysłów Alana Turinga. Przełom był jednak połowiczny: dzięki „fantowi z Narwiku" Brytyjczycy zdołali odczytać depesze z sześciu dni, od 22 do 27 kwietnia, po czym (poza incydentalnymi sukcesami) Enigma Kriegsmarine ponownie zamilkła na rok; nadal brakowało tablic bigramów. Dopiero 9 maja 1941 r. na pokładzie opuszczonego przez załogę okrętu podwodnego U-110 znaleziono nie tylko instrukcje obsługi, lecz także tabele bigramów, które umożliwiły efektywny start dekryptażu szyfrów niemieckiej marynarki. W swoich pracach teoretycznych nad złamaniem szyfrów Kriegsmarine Brytyjczycy nie posunęli się poza punkt osiągnięty w 1937 r. przez polskich kryptologów. Przełom stał się możliwy dopiero po zdobyciu dokumentów na pokładzie U-Boota, po czym brytyjscy kryptolodzy zdołali utrzymać kontrolę nad szyfrem, mimo późniejszych zmian. Nieco przewrotnie można w tym miejscu przypomnieć cytowaną wcześniej wypowiedź Dilly'ego Knoxa: (…) [n]*igdy tego nie rozpracowali, musieli to ukraść przed laty, a następnie obserwowali rozwój, jak każdy by potrafił, jednak na początku musieli to ukraść lub kupić*.

Polski raport informuje o wydarzeniach lapidarnie: (…) [s]*zczegóły nowego systemu szyfrowania poznano dopiero, gdy Anglikom udało się w 1940 roku odnaleźć instrukcje procedury na pokładzie zatopionego U-Boota. Nie możemy opisać tutaj procedury szczegółowo, odsyłając czytelnika do fotograficznych reprodukcji zdobytych dokumentów*. Wiemy, że instrukcje użycia Enigmy opisujące m.in. sposób szyfrowania klucza depeszy zdobyto na pokładzie uzbrojonego trawlera „Polares", a nie na pokładzie U-Boota. W tym samym rozdziale Polacy opisują jednak zdobycz nieznanych do tej pory wirników Enigmy Kriegsmarine: (…) [w] *1940 roku Anglicy znaleźli na pokładzie zatopionego U-Boota dwa wirniki, noszące oznaczenia VI i VII*. Istotnie, 12 lutego 1940 r. trałowiec HMS Gleaner zatopił niemiecki okręt podwodny U-33, a w kieszeniach uratowanych niemieckich marynarzy znaleziono wirniki VI i VII. Zapewne Brytyjczycy nie informowali aliantów zbyt szczegółowo o okolicznościach swych zdobyczy, w rezultacie w świadomości Polaków dwa odrębne wydarzenia połączyły się w jeden epizod.

Ostatni rozdział raportu potwierdza, że przytoczone przez Langera okoliczności jego powstania odpowiadają faktom. Zadaniem autorów było sporządzenie swego rodzaju inwentaryzacji wkładu trzech krajów w triumf nad Enigmą. Jego autorzy poszli po linii najmniejszego oporu. W zasadniczej części raportu podkreślali raczej pożytki ze współpracy kryptologów trzech krajów, niż rozbierali na części składowe zasługi wniesione przez każdą nację z osobna. Dopiero w zakończeniu raportu dodali tabelaryczne podsumowanie, w którym sumiennie wyliczyli elementy sukcesu, dzieląc je pomiędzy współpracujące kraje. Taka forma musiała wzbudzić irytację inicjatora raportu. Zlecając jego wykonanie, musiał być przekonany, że wydźwięk całości będzie jednoznaczny i przypisze Francji oraz jemu samemu rolę przewodnią w kryptologicznym triumfie. Tymczasem w tabeli pracowicie wyliczono ponad 20 elementów wniesionych przez Polaków, sześć elementów wkładu Brytyjczyków

[7] Tamże, s. 22.

i zaledwie jeden istotny element wkładu Francuzów – dostarczenie dwóch ważnych dokumentów. Bertrand musiał czuć się rozczarowany. Przez kilka lat sumiennie dostarczał Polakom klucze do szyfru przekazywane przez niemieckiego zdrajcę i miał nadzieję, że tak istotny z jego punktu widzenia wkład zostanie odnotowany w bilansie. Nie wiedział, że decyzją szefów polskiego Biura Szyfrów klucze trafiają prosto do sejfu Maksymiliana Ciężkiego i nie docierają na biurka kryptologów. Ciężki wychodził z rozsądnego założenia, że w przypadku wzrostu napięcia międzynarodowego komunikacja z francuskim szpiegiem zostanie przerwana, a Polacy zostaną pozbawieni najważniejszych informacji właśnie w chwili, gdy ich znaczenie dramatycznie wzrośnie. Ufał swoim kryptologom i zakładał, że pozbawieni dostępu do kluczy opracują własne metody ich rekonstrukcji. Matematycy nie zawiedli jego zaufania; Ciężki nigdy nie musiał sięgać do sejfu po materiały od Bertranda. Zapewne jednak nikt nie poinformował o tym Francuza, który poczuł się urażony czymś, co uznał za minimalizowanie jego wkładu w dekryptaż Enigmy.

Dwa aspekty analizowanego dokumentu wymagają dodatkowego komentarza. Pierwszy dotyczy jego początkowych rozdziałów. Po zarysowaniu tematu w dwóch wstępnych sekcjach autorzy wrzucają czytelnika na głęboką wodę, prezentując matematyczne podstawy swoich sukcesów. Podczas pracy nad tekstem znali jego domyślnych adresatów i mieli pełną świadomość, że matematyka zdecydowanie nie jest ich żywiołem. Gdyby zależało im jedynie na ukazaniu tła swojej pracy, zapewne wystarczyłby rozbudowany przypis lub matematyczny załącznik dyskretnie dołączony w końcowej części dokumentu. Lokując sekcje poświęcone teoretycznym podstawom sukcesu na początku tekstu, jego autorzy pragnęli zwrócić uwagę na to, co uważali za najważniejszy aspekt swojej pracy – na rolę matematyki w sukcesie. Musieli rozumieć, a co najmniej przeczuwać, charakter rewolucji w kryptologii, jaka była skutkiem ich triumfu. Przed Rejewskim, Różyckim i Zygalskim nikt nie podejmował poważnych prób zaprzęgnięcia zaawansowanej matematyki w służbę kryptologii. Użycie najprostszych metod statystycznych w celu zliczenia częstotliwości występowania pojedynczych znaków, bigramów lub trygramów w tekstach jawnych nie zasługuje na uwagę. Nawet gdy służby kryptologiczne kilku krajów świata zdecydowały się zatrudniać matematyków, sięgały bardziej po ludzi niż metody reprezentowanej przez nich dyscypliny naukowej. Ojciec współczesnej kryptologii amerykańskiej William Friedman umieścił w prasie ogłoszenie o zamiarze zatrudnienia kilku „rządowych matematyków" ponad rok po poznańskim kursie kryptologii. Jednak zatrudnieni przez niego Solomon Kullback, Frank Rowlett i Abraham Sinkov wspominali później, jak w pierwszych latach pracy przygotowywali słowniki kodowe, rzucając karty ze słowami kodu w strumień powietrza z wentylatora, zapewniając tym samym ich losowy porządek. Upłynęło sporo czasu, zanim zaczęli korzystać z matematycznego instrumentarium.

Rozpoczęcie raportu poświęconego złamaniu Enigmy właśnie od podstaw teoretycznych wskazuje na to, że jego autorzy byli świadomi znaczenia matematycznej rewolucji w kryptologii, którą zainicjowali. Kiedy oddali swoje dzieło w ręce Brytyjczyków, ci w znaczeniu czysto praktycznym rozwinęli ich dokonania na wielką skalę, jednak w innym sensie ich zaangażowanie przyniosło regres. Algebraiczne metody stosowane przez Polaków miały olbrzymią zaletę: gwarantowały możliwość złamania szyfru. Brytyjczycy od pierwszych chwil traktowali je nieco nieufnie, zauważając, że warunkiem zastosowania polskich metod jest występowanie podwójnie szyfrowanego klucza depeszy. Od pierwszych dni po spotkaniu w Pyrach przygotowywali się do nieuniknionego ich zdaniem momentu, w którym ten warunek

nie będzie spełniony. Jako remedium proponowali metody łamania szyfru oparte na jego własnościach statystycznych (sito E, banbaryzm, później zautomatyzowane metody łamania szyfrów dalekopisowych z wykorzystaniem urządzenia Colossus itp.). Doraźnie mieli rację – przed rozpoczęciem kampanii francuskiej Niemcy usunęli dotychczasową słabość w procedurze użycia Enigmy. Algebraiczne podejście Polaków stało się chwilowo bezużyteczne. Jednak brytyjski sukces dotyczący nowego wariantu szyfru miał swoją cenę: Brytyjczycy czytali szyfr Enigmy tylko wtedy, gdy dysponowali wiarygodnym i stabilnym fragmentem prawdopodobnego tekstu depesz. Bardziej długofalowym efektem ich podejścia był wieloletni, ścisły mariaż kryptologii ze statystyką i teorią prawdopodobieństwa. Trzeba było wielu lat, aby kryptolodzy powrócili do algebraicznego podejścia Mariana Rejewskiego i jego kolegów, przywracając równowagę zastosowań matematyki w kryptologii.

Drugim wątkiem zasługującym na uwagę jest przedstawiona przez autorów ocena wartości międzyalianckiej współpracy kryptologicznej. Pisali swój tekst najwcześniej w drugiej połowie 1940 r. W tym czasie zainicjowana rok wcześniej współpraca należała w zasadzie do przeszłości. Kryptolodzy przedwojennego Biura Szyfrów doznali zawodu ze wszystkich stron. Po ewakuacji z Polski spotkali się z despektem ze strony własnych rodaków, którzy nie dopuścili ich do służby w odradzającej się we Francji armii polskiej, kierując zespół dość bezceremonialnie pod rozkazy Francuzów. Jak wynika ze wspomnień matematyków, Francuzi nie potrafili zorganizować pracy w sposób, który pozwoliłby na wykorzystanie doświadczenia i wiedzy kryptologów Biura Szyfrów. Brytyjczycy, na których lojalną współpracę Polacy mogli liczyć w ciągu minionego roku, przerwali kontakt z chwilą upadku Francji. Autorzy raportu musieli odczuwać wielkie osamotnienie. Mimo to konsekwentnie podnosili znaczenie współpracy trzech krajów nad łamaniem Enigmy i wynikające z niej wymierne pożytki. Można jedynie spekulować, jak wielkie sukcesy odnieśliby kryptolodzy Francji, Wielkiej Brytanii i Polski, gdyby ich dowódcy dostroili się do sposobu myślenia podwładnych i nie tylko zezwolili na kontynuację współpracy, lecz także na nadanie jej takich form, jakie w późniejszym okresie przybrała (nie bez początkowych zgrzytów) współpraca kryptologów Wielkiej Brytanii i USA.

Preface

The cryptological conference which took place in Pyry, July 24-27, 1939, was effectively the start of cryptological cooperation among the Allies, which in due course was to affect the outcome of World War II. The meeting of cryptologists from Poland, France and Great Britain was characterised by a considerable load of emotions, easy to read in the participants' memoirs. The reports they submitted refer more to the true or plausible motivations of the parties attending the meeting, the twists and turns of actions in its course and the final arrangements, rather than the essential content: the scope of the information provided by the Polish cryptologists, which had determined the scale of their success in dealing with German Enigma ciphers. The Poles knew the scope of their knowledge concerning Enigma, and did not have anything to prove. The foreign participants at the conference did not have to report the Polish methods of attack on the Enigma cipher; they had received a comprehensive compendium of knowledge about Enigma, prepared by the Polish cryptologists in the weeks preceding the meeting in Pyry; this document had been prepared in German, being the only language known by all the conference participants. This compendium was the total foundation for the cryptological cooperation of the Allies, which in the end turned out to be one of the factors determining the outcome of World War II. Therefore, it is somewhat unfortunate that for nearly eighty years after the end of this conflict, when the vast majority of documents describing the war achievements of Allied cryptologists had been made available to historians, the document under discussion, which is of such fundamental importance, had remained unavailable.

The report of the cryptologists of the Polish Cipher Bureau, did not, for obvious reasons, survive in the Polish archives. One might like to say - luckily. A part of the archives of the Polish pre-war Intelligence fell, as a result of a fatal error, into German hands just after the end of the September campaign. Many Polish intelligence agents paid for this neglect with their lives. Fortunately, the Germans found in the archives only three messages originally encrypted by Enigma and considered their find to be accidental, assuming that a systematic decryption operation would have left more extensive traces. The main archive of the Polish Cipher Bureau had been destroyed during the evacuation of the unit towards the Romanian border. As fuel for the cars forming the evacuation convoy ran out, people, equipment and documents had to be shoe-horned into fewer and fewer vehicles. Finally, near Lutsk (in today's Ukraine), it became necessary to burn the crates of documentation and bury the equipment in order to save the Bureau's most important asset - the people. When in October 1939 the Cipher Bureau team slowly reformed in Paris, it had only two Enigma copies along with the knowledge and the experience of the cryptologists.

At this point, the decision to share the secret of Enigma with the cryptologists of France and Great Britain began to pay dividends. The documents and the copies of the machine which had been given to the Allies as a result of the July meeting in Pyry were now safe, allowing the Poles to focus on resuming their decryption work, instead of having to concentrate their efforts on the laborious and time-consuming

recovery of their knowledge from before September 1939. At the same time, British cryptologists carefully studied the materials which they had received from Poland. This is evidenced by reports written by heads of individual sections after the end of hostilities. Conel H. O'D. Alexander wrote in his "Cryptographic History of Work on the German Naval Enigma" that:

> Nearly all the early work done on Enigma was done by Polish cryptographers who handed over full details of the very valuable results they had obtained just before the war began. (...) Looking back at the work done by the Poles and considering how little was known of the theory of machine cyphers when they started and how meagre was the mechanical equipment at their disposal one is filled with admiration for their work. (...) Our subsequent success owed much to their early efforts.[1]

A.P. Mahon shares Alexander's opinion. In the official "The History of Hut Eight 1939–1945": *Nearly all the early work on German Naval Enigma was done by Polish cryptographers who handed over the details of their very considerable achievements just before the outbreak of war.* A comment contained in the Mahon report confirms that *... the Poles devised a new method which is of considerable interest. Their account of this system, written in stilted German, still exists and makes amusing reading for anyone who has dealt with machines*.[2] Mahon took over the leadership of Hut 8 only in the final phase of the war, so he knew about the early period of work on the cipher only from intermediaries (mainly Alan Turing) and from the preserved documents. His comment confirms that the compendium prepared by the cryptologists of the Polish Cipher Bureau for the participants of the Pyry meeting was available at Bletchley Park in the period immediately after the end of World War II. On the other hand, Mahon's reference above is the last trace of this memorandum in the available sources; until today, no one has found any trace in the archives, although it should be there and it should be declassified along with other documents describing the early period of struggle with the German cipher.

The availability of a memorandum in the Allied archives is an important element of the discussion concerning the role and contribution of Allied cryptologists, not so much in breaking the Enigma cipher, as in initiating a revolution in cryptology that enabled early successes, and in the long run transformed the face of the discipline. The lack of reliable, first-hand information on the contribution of individual countries to the victory over Enigma meant that, during the Second World War, narratives presenting the achievements of the Polish cryptologists in a distorting mirror started to appear. The then head of British cryptologists, Alastair Denniston, wrote after returning from Warsaw that when he was still there:

> It was only when we got back into a car to drive away that he [Dillwyn Knox] suddenly let himself go and, assuming that no one understood any English, raged & raved that they were lying to us now as in Paris. The whole thing was a pinch he kept on repeating—they never worked it out—they pinched it years ago & have followed developments as anyone could but they must have bought it or pinched it.[3]

---

[1] Conel H.O'D. Alexander, *Cryptographic History of Work on the German Naval Enigma*, p. 17.

[2] A.P. Mahon, *The History of Hut Eight 1939–1945*, p. 13.

[3] R. Erskine, *The Poles Reveal their Secrets: Alastair Denniston's Account of the July 1939 Meeting at Pyry*, "Cryptologia" 2006, Volume 30 issue 4, p. 10.

In a report dated July 30th, which he wrote after he had returned to London, Knox changed his tune a little, writing:

> Let's get this straight. (...) The Poles have got the machine to Sept 15th 38 out by luck. (...) If we are to attempt this [decryption of Enigma] we should examine their system and statistics (if any) with considerable scepticism. (...) I am fairly clear that Schessky [Ciężki] knows very little about the machine & may try to conceal the facts from us. The young men [the three cryptologists] seem very capable and honest.[4]

If Knox, who had participated in the Pyry meeting, presented such an unreliable image of events, other chroniclers, who were not directly involved in the early stages of the cooperation of cryptologists, were condemned to speculation and repetition of stories resulting from ignorance or prejudice. Meanwhile, events had occurred in such a way that, among the chroniclers documenting the works and achievements of Bletchley Park, immediately after the end of World War II, there was no one still around who had been actively involved in the early stage of cooperation. Dilly Knox himself had died in February 1943, defeated by the disease he had been fighting even before attending the meeting in Pyry. Alastair Denniston had been removed from the position of the head of Bletchley Park in February 1942 and had transferred to the post of the head of the section of G.C. & C.S. which dealt with breaking diplomatic codes and ciphers. He did not participate in the editing of post--war reports on the role of the centre, whose work he had managed for around half the war's duration. Finally, Alan Turing, who had not participated in the conference in Pyry but knew the results directly from Knox and Denniston, was also persuaded to abandon Bletchley Park towards the end of 1942, and therefore did not contribute to the reports written after the war. These reports' completion rested in the hands of people who knew about the Polish events from second- or even third-hand. In this situation it is understandable that even in the reports written by such reliable and systematic people as Stuart Milner-Barry, there were notes that were inconsistent with historical events. In a part of the report "History of Hut 6", to which Milner--Barry contributed, we find the following passage:

> It is historically uncertain how the Poles obtained the wiring of the wheels and machine, and it was not a subject on which they were very communicative. Certainly they made extensive use of secret agents and it is most probable that they obtained photographs of keys and messages with clear-text. The essential fact that the machine diagonal was alphabetical they admitted to have discovered through one agent, though they claimed, no doubt with justice, that they could have reconstructed it mathematically.[5]

This theme of theft and secret agents was to have a real career over a long time. The story of the breaking of the Enigma cipher was not revealed in a planned way, but it happened quite prematurely, at least in the opinions of the British and American successors to Bletchley Park. Several unpublished statements and fragmentary references in early publications indicate that the outline of the truth was already known in the environment of British historians by the mid-1960s. The perhaps so-

[4] Ibidem, pp. 10, 11.
[5] "The History of Hut 6", Volume I (HW 43/70), p. 44.

mewhat controversial British historian, David Irving, knew this, it seems. Probably aware of his reputation among other historians, he had to recognise that he should put key issues safely in someone else's words and chose for this purpose the renowned historian from the London School of Economics, Donald Cameron Watt. In the preface to Irving's book, "Breach of Security", published in 1968, Watt wrote that [Great Britain] (...) *received from Polish Military Intelligence keys and machines for decoding German official military and diplomatic ciphers*.[6] Neither Watt's indiscretion, nor an indication a year earlier from Poland (a single sentence about the breaking of German ciphers by the Polish pre-war intelligence service, included in Władysław Kozaczuk's book „Bitwa o tajemnice"[7]), attracted any attention from historians or from cryptology veterans. It was not until the publication in 1973 of the book[8] written by the then retired French general, Gustave Bertrand, that a storm was unleashed. It seems, moreover, that this happened to a lesser extent due to the sensational disclosure of the breaking of Enigma, but rather due to the historical distortions and traditional French taunts addressed to the perfidious Englishmen. These made it impossible to pass over the French general's publication; however, at the same time it was by no means permissable to confirm his version of history even on those issues in which Bertrand had honestly reported the events, and not only because of the sensitivity of the British conscience. It was the first half of the 1970s, Europe remained divided by the Iron Curtain, evoking at best quiet confrontation between the West and the world of communism. The cryptologists of both camps continued to rely on ciphering machines the construction of which had been derived from Enigma. Admitting that the Enigma had already been broken during World War II would serve as an obvious warning to an adversary concerning the security of his modern ciphers.

The special services of the United Kingdom and the United States apparently recognised that Bertrand's revelations had come out far too early. Because the fact of the Enigma decryption had been revealed and it was no longer possible to put the genie back into the bottle, it was necessary to use a technique as old as the world – disinformation. The British persuaded the World War II veteran, Frederic W. Winterbotham, to participate in this effort. Winterbotham was once one of the creators of the distribution system of decrypted information to the most important government agencies and command staffs, but in this role he had no contact with cryptological work itself. In his book "The Ultra Secret", published in 1974, he included many curiosities such as the "bronze goddess" – a machine used to break the code; however, from the point of view of his peers, the key part of the story was probably the Poles' participation in the victory over Enigma:

> In 1938 a Polish mechanic had been employed in a factory in Eastern Germany which was making (...) some sort of secret signalling machine. (...) In due course the young Pole was persuaded to leave Warsaw and was smuggled out under a false passport (...); installed in Paris where (...) he was given a workshop. With the help of a carpenter to look after him, he began to make a wooden mock-up of the machine he had been working on in Germany.[9]

[6] William Kimber and Co. Ltd., 1968, pp. 33, 34.

[7] W. Kozaczuk, *Bitwa o tajemnice: Służby wywiadowcze Polski i Niemiec 1918-1939*, Warszawa 1967. Generally translated as „Battle for Secrets" or „Struggle for secrets".

[8] G. Bertrand, *Enigma, ou la plus grande énigme de la guerre 1939-1945*, Paris 1973, Plon.

[9] Weidenfeld and Nicholson, 1974. p. 10.

A year later, another Briton, Anthony Cave Brown, published a book "Bodyguard of Lies" in which he told a similar story:

> Gibson [head of the MI6 station in Prague] (...) met a Polish Jew [previously employed in machine production] who had offered to sell MI-6 his knowledge of Enigma (...) [for] £10,000, a British passport, and a resident's permit for France."[10] After checking his credibility, the story continues, MI6 installed him in a suite in Paris, where Lewiński played back Enigma data from memory.

Finally, in 1976, William Stevenson published a biography of the similarly named Sir William Stephenson, who during the war had been the head of the British intelligence unit in the US, entitled "A Man Called Intrepid", in which he presented a slightly different version of the Poles' acquisition of the Enigma secret: *The new Enigmas were being delivered to frontier units, and in early 1939 a military truck containing one was ambushed.*[11] The versions presented by each of the British writers differed from each other, but contained a common thread as their key element and which was consistent with the speculations of Knox and of his successors in Bletchley Park: the success of the Poles, in their struggles with Enigma, had been based on obtaining a copy of the machine by theft or otherwise. This contained a clear message for a cryptological adversary: as long as you are able to protect the physical security of your encryption machines, your ciphers are also secure.

If the revelations of British historians were, as we assume, deliberate disinformation, it was at an embarrassingly low level, and would probably not have been able to mislead even novices within the secret services. However, it brought an unexpected side effect, the results of which have, up to the present day, put a barrier in the way of telling the historical truth about the breaking of Enigma. In the mid-1980s, the British had to recognise that Enigma-based machines were slowly coming out of use, and therefore the truth about Enigma could no longer harm anyone, so they began the gradual disclosure of source documents about its history. From the end of the 1980s, anyone who wanted to know the history of the breaking of Enigma, could, without much difficulty, get acquainted with the basic source documents as well as summaries developed with the participation of veterans of the allied cryptological centres. In spite of this, some historians, as well as their contemporaries, have had a tendency to repeat the old disinformation. Norman Davies in his 2006 book "Europe at War 1939-1945: No Simple Victory" described in a similar way the role of Poles in breaking the Enigma: *Pre-war Polish Intelligence learned that the German military were developing* (...) *a code based on a commercial machine called 'Enigma'. Polish agents penetrated the factory where the enhanced machine was being built, and learned the exact details of its design.*[12] In 2010, Richard Aldrich presented in his book "GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency: *Before the Polish Secret Service was forced to flee Warsaw, its agents had achieved the remarkable feat of stealing several examples of the military Enigma from the German factory in which they were made.*[13]

In this context, the many years of effort by Polish historians spent searching the Allied archives to find and to disclose a copy of the memorandum provided by

[10] W.H. Allen & Co. Ltd, 1977. p. 17.
[11] Sphere Books Ltd, 1981. p. 53.
[12] Pan Macmillan Ltd., 2007, p. 38.
[13] Harper Press, 2011, p. 22.

the Poles in Pyry are understandable. The memorandum, if it has been preserved to this day, is the most authoritative confirmation of Poland's contribution to breaking the Enigma cipher. One can argue that this role is played by other documents produced by Polish cryptologists during different periods of their activity. Especially significant is the so-called "Document L" which was attached to Gwido Langer's report concerning the Polish Cipher Bureau's pre-war activity. This document, probably produced during the first half of 1940, was found in the collections of the Sikorski Institute in London. Its brief character allows us to guess that it is an attempt to reconstruct from memory the sources lost during the evacuation from Poland and, consequently, does not fully reflect the scope of information provided to the Allies in July 1939. Two parts of Marian Rejewski's post-war memories were recorded in 1967 and 1974 respectively; the time lag from the described events and the lack of access to even rudimentary source documents also limit these memories' usefulness as a reference point for the analysis of the Polish contribution to breaking the cipher. What's more, both documents survived only in Polish archives, which to some extent, limits their usefulness when seeking to discuss the role of cryptologists of several countries in triumphing over Enigma.

All attempts to find a copy of the original Pyry report in the Polish allies' war archives have been, and thus far remain, ineffective. However, in 2016, this author located a document in the archives of the French armed forces, which is probably a shortened version of the report being sought, based on the full text to which the authors must have had access, and supplemented with a description of events between July 1939 and June 1940. Consequently, this document is currently the best known summary of the contribution of the Poles to breaking Enigma, coming from the Allied archival resources. The document is part of the collection declassified on December 2, 2015, by decision of the Direction Générale de la Sécurité Extérieure and subsequently transferred to the archive of the Service Historique de la Défense in Vincennes[14]. The composition of the collection shows clearly that it formed part of the private archive of the then retired French army general, Gustave Bertrand, the war-time leader of the team of Polish cryptologists. It is also known that, as part of the liquidation of the semi-clandestine cryptological centre which operated from November 1940 to November 1942 near Uzès in the unoccupied part of France, Bertrand concealed the archives by hiding them in his mother's home in Grasse. After the liberation of the south of France in 1944, he recovered the documents, but immediately after his death on May 23, 1976, his property in Théoule-sur-Mer, in which he had served as mayor, was searched by army representatives who confiscated a large number of documents. Judging from the information given by the general's widow concerning the volume of seized files, what was finally revealed in 2015 represents only a fraction of the Bertrand archive.

The undated and unsigned manuscript was marked in the inventory as a "technical document in German" *(Notice technique en allemande)*; it was accompanied by a handwritten translation into French. Coincidence allowed us to know the circumstances and reasons why the document was made. The post-war report of Colonel Langer on the activity of Branch 300 and the evacuation of the centre from France[15] states that

[14] Service historique de la défense, SHD DE2016 ZB25.
[15] IJP 709/133/5, p. 39.

> (...) in Fouzes (where we were quartered at that time) Bolek [a code name for Gustave Bertrand] requested the production of a detailed document in which would be presented in an objective manner to what extent each of the three partners contributed to the solution of the Enigma machine problem. The document was prepared by Marian Rejewski and Henryk Zygalski. When Bolek studied it, he said that the whole work must be changed, because reading it in its current form, one gets the impression that the French had done almost nothing.

The question of the authorship of that document is somewhat complex. Langer indicated that it was written by Marian Rejewski and Henryk Zygalski only, which may show that it was created in the period after the death of Jerzy Różycki, or at least during his stay in North Africa in 1941. On the other hand, the chronology of the events described in the document covers the period to the second half of June 1940. From Bertrand's memoirs and Langer's reports it is known that cryptologists continued the decryption of Enigma at least till the end of 1941. It can be assumed that the memorandum written in 1941 or later would contain at least some references to these works. The lack of such references indicates the second half of 1940 to be the most likely time for the creation of this document. In Marian Rejewski's "Memories", we learn that, in the early phase of work in the centre of P.C. Cadix, the French had had problems with providing the cryptologists with intercepted Enigma-encrypted messages. To encourage the team whose morale was collapsing as a result of their forced move to France, Bertrand provided the cryptologists with a set of Swiss messages encrypted with a commercial Enigma; these the Poles quickly broke. The preparation of summaries and reports is part of the classical operation of every bureaucracy; therefore, it is probable that the document under discussion was created in the second half of 1940, when the cryptologists' French superiors attempted to occupy them with any kind of work. However, if this guess is correct, the memorandum is most likely the collective work of all three: Rejewski, Różycki and Zygalski. The omission by Langer of Różycki's name in the report submitted after the end of the war may have been dictated by the mechanism of psychological repression of the memory of that cryptologist after his untimely death. We know that during his interrogation at Eisenberg Castle in March 1944, Langer referred to the work of only two mathematicians, apparently adjusting his memory (or at least his testimony) to reality after Różycki's death. In the post-war report, an identical mechanism could have applied.

The document bears the title *ENIGMA. Kurzgefasste Darstellung der Auflösungsmethoden*, that is: *Enigma. An abridged presentation of solution methodologies*. The use of the word "abridged" in the title unequivocally suggests the existence of a fuller version of the same text. The only document that could perform such a role would be a report prepared for the participants of the meeting in Pyry. This is confirmed by several circumstances. First of all, it is known that the Pyry report was produced in the German language, German being the only language in which all of the participants of the meeting could communicate. Given the circumstances of the edition of the text, there would have been no reasons to have used the language of the enemy. The production of such a document in German indicates that it constituted, according to its title, an abbreviated version of a source text previously produced in the same language. The second circumstance, which indicates that the authors had access to their original report, is its level of detail, especially when comparing it with "Document L" from at least half a year earlier. "Document

L" corresponds to about half of the text being analysed and omits some interesting threads therein contained. In particular, this applies to several sections devoted to the analysis of Kriegsmarine ciphers. Post-war comments from British cryptologists clearly confirm that the Poles shared with them the results of their work concerning the use of Enigma by the German navy. We will also see further that the British never managed to go beyond the results which the Poles had achieved solely using cryptological theory. Identification of the missing elements of the cipher and the final breaking of the Kriegsmarine Enigma cipher were a consequence of finding documents on board several captured enemy ships. Meanwhile, in the previously known Polish sources ("Document L", along with Marian Rejewski's *Memories*), the decryption of the Kriegsmarine Enigma was briefly mentioned, but without much detail. A comparison of British reports with the content of Polish documents clearly indicates that the British referred to some document provided by the Poles other than the texts known so far. Extensive information about the history of the decryption of the Kriegsmarine Enigma by the Polish Cipher Bureau appears for the first time in this document.

Differences between the presumed original and the document under discussion are not purely a result of the shortening of the former. The report prepared in connection with the conference in Pyry could not, of course, cover that conference itself or the events that followed it. The document under discussion leads the narrative to the point immediately preceding the supposed time of its editing. Thanks to this, we have the opportunity to learn about events up till the surrender of France as observed from the Polish point of view. The report includes the conference in Pyry and an early period of tripartite Allied cryptological cooperation. The authors provide information about the earliest successes of British cryptologists; from the attack method developed by Dilly Knox, to the change of the encryption procedure preceding the French campaign, and the further defeat of that changed procedure by the Herivel method. The last chapter confirms the circumstances of the report submitted by Gwido Langer: it contains a list of elements of the participants' contribution to the cryptological alliance in breaking the Enigma ciphers. One can understand the nervousness of Gustave Bertrand after reading the document - against the background of the achievements of Polish and British cryptographers, the contribution of the French as described in these two documents is rather modest.

A significant part of the information presented in the report reproduces issues known from other, previously available documents. However, its unique character comes down to two specific items. It is the only document currently known to summarise the contribution of the Poles to the breaking of Enigma and the early stage of allied cryptological cooperation from the Allied archives. At the same time, it is the broadest summary of the period disclosed so far, derived from sources other than Anglo-Saxon. According to the letter containing Bertrand's orders causing the study to take place, though probably with a result not exactly matching his intentions, the scope of the memorandum allows extended analysis of the contributions of the cryptologists from the three countries to breaking the Enigma relative to the current state of knowledge. Let's start the review of the document with the elements which contain important details.

In Chapter 2, which is devoted to the beginning of the Polish struggle against Enigma, Rejewski confirms unequivocally that the Polish intelligence had gained important information about the machine long before Gustave Bertrand in autumn 1931 had given the Poles two documents from Hans-Thilo Schmidt. One could have guessed this from Rejewski's *Memories* in which the earliest stages of attack on the

Enigma cipher were described, as he used a nomenclature referring to Enigma G rather than the model I, which Bertrand's revelations concerned. Most historians suggest that Bertrand's documents allowed the cryptologist to build a mathematical model of the machine. The scope of the Poles' knowledge about Enigma, as described by Rejewski, and the use of terminology referring to Enigma G, indicate that he had started working on a mathematical model of the machine based on data obtained independently by Polish intelligence; the documents provided by Bertrand only confirmed, and added some details to the assumptions previously made.

Chapter 4 shows an obvious compromise between obligations to an employer and professional pride. We know from Langer that the report was commissioned by Bertrand and that it was intended to present the contributions of the three countries to the breaking of Enigma. Knowing from other sources the character of Bertrand, we can assume that he expected confirmation of significant involvement, if not of a key role, of France and of himself, in this success. His conviction about the decisive role in the undertaking was strengthened even by the flattery included in the correspondence with the British partner. On August 3, shortly after returning from Poland, the head of British cryptologists, Alastair Denniston, wrote to Bertrand: *I want to emphasise that we owe everything solely to you; I am counting on the future cooperation of our trio, in which you must play a leading role.* The cryptologists worked hard to find any circumstance which would enhance the role of France and the French and they found it in the documents provided to the Poles in 1931 and 1932. They noted that *It should be stressed that these documents, and in particular the daily keys, decisively influenced the progress of work. Without them, the Enigma cipher solution would have been delayed for years.* The first sentence is an additional confirmation of the conclusion formulated above. The authors of the report raise the importance of knowing only the key of the day, thus making it clear that the Enigma instruction manual provided was not the decisive document for the outcome of their work. This probably meant that Rejewski was able to build a mathematical model of the machine based on information obtained earlier and independently by Polish intelligence. The Poles emphasise the crucial meaning of knowing the day's keys only to moderate this proposition immediately; without it, the solution of the Enigma cipher would probably also be possible, although [it] *would have been delayed for years*. The topic of the solution of Enigma without the documents provided by the French returns a bit later, when, in Chapter 7, the authors outline the method which, in their opinion, would allow breaking the cipher without outside help. Modern cryptologists have confirmed that this method does actually lead to breaking the cipher, provided that certain assumptions are met. The lack of archived messages from this period does not allow the confirmation that these assumptions were actually met. We must therefore accept the assurance of the authors that the French contribution did prove decisive for success in the struggle with Enigma, although this claim only applies to the practice of decryption; the documents provided did accelerate the breaking of the cipher by at least a year. However, after confirming this fact, Rejewski and his colleagues immediately weakened the strength of their own argument, by demonstrating that on the basis of cryptological theory alone they could also have coped without the keys provided, breaking the Enigma with purely mathematical methods.

While editing Chapter 6, the authors did not realise that they were simultaneously arguing with British cryptologists. In Chapter 5, the cryptologists described how they reconstructed the connections of the input rotor, known as the 'substitution E':

(...) the problem was that they did not know the substitution E. It seems that the efforts of British cryptologists have failed. Subsequent studies of the Polish Cipher Bureau proved that the substitution E can be determined analytically (provided the knowledge of substitution S), but in reality they were found by trial and error.

"Trial and error" does not quite reflect the essence of Marian Rejewski's success. For the reconstruction of the substitution E he used not so much the trial and error method; rather his intuition and his knowledge of the secrets of the German soul. Knowing that in the commercial model of the machine the connections of the input rotor correspond to the arrangement of the machine's keys, he assumed that in the military model, the systematic Germans would have also reached for some form of order. The simplest option was an alphabetical arrangement and that, in fact, proved to be the solution. The success achieved thereby, however, did not satisfy Rejewski and over time he also developed a purely analytical method of reconstruction of the input rotor connections, which is described in Chapter 6 of the report. The authors were unaware that in the British reports from Warsaw and subsequent studies by British cryptologists the question of the reconstruction of the input rotor became one of the key issues. Dilly Knox had already in the first report from Warsaw[16] reported that *The Poles have got* [were reading] *the machine to Sept 15th 38 out by luck.* He was referring to Rejewski's finding of the connections of the input rotor, attributing a greater role to luck than to the psychological intuition of the cryptologist. During the meeting in Pyry, Rejewski apparently tried to convince the attendees that, separately from his intuitive solution, he had also developed a mathematical method for the reconstruction of the input rotor's connections. This part of the conversation must have taken place in French, because the Briton noted a declaration of the Poles in the form *nous l'aurion pu trouver aussi par mathematique*[17], and he then pretended that he had poor knowledge of that language, adding that the declaration probably referred to the date of finding a solution. In the post-war report, to which Milner-Barry contributed in[18] 1945, there is written: *The essential fact that the machine diagonal was alphabetical they admitted to have discovered through one agent, though they claimed, no doubt with justice, that they could have reconstructed in mathematically.* The narration initiated by Knox, according to which luck was to be a decisive factor in the success of the Poles, soon after the end of the war developed into a version that then lingered for decades: agents were responsible for the breaking of Enigma by the cryptologists. This narrative persisted even though documents in the Allied archives clearly confirmed the intellectual honesty of the Poles.

The content of Chapter 13 is basically also known from other documents that describe Polish methods of breaking the cipher, yet it deserves a short commentary. It describes the method of identifying the right rotor using a method proposed by Jerzy Różycki, which was known within the group of Polish cryptologists as the "Metoda Zegara" or as the "Clock Method". This method uses the cipher property originally described in 1922 by the father of contemporary American cryptology, William Friedman, and nowadays referred to as the "Index of Coincidence". The interest of researchers was for a long time aroused by the fact that the description of the method used by the Poles did not use the terminology introduced by the original di-

[16] R. Erskine, *The Poles Reveal...*, p. 10.
[17] "We would have been able to work this out using mathematics as well".
[18] "The History of Hut 6", Volume I (HW 43/70), p. 44.

scoverer of the method to the slightest extent. The original work by Friedman, containing the description of the Index of Coincidence, was classified immediately after publication and was declassified only in the 1970s. The short period of its availability meant that its basic principles were known in selected circles of cryptologists, in particular in the USA and in France (where a reprint of Friedman's work had been issued). The question is whether Jerzy Różycki or any of his colleagues learned the concept of the index of coincidence during their training or did he develop it himself, discovering, independently of Friedman, one of the key tools of modern cryptology? Marian Rejewski wrote that he had discovered in France that the program of the cryptological course carried out in Poznań in 1929 was based strictly on the book of one of the leading French cryptologists, Marcel Givierge, "Cours de cryptographie". In the currently available English translation of the book, Friedman's name and reference to the index of coincidence appear only in the one-sentence footnote to a publication which was not available during the period of the Poles' work on the cipher. In this situation, the content of the original French edition of the book becomes interesting; maybe the Index of Coincidence was discussed in more detail there? This author's research, conducted jointly with Philippe Guillot, has allowed him to access the original edition of the book. The explanation of the index of coincidence has in that book an identical structure as in the English translation; the Poles could not have learned the nature of the tool based on the description in the book. This fact alone does not determine the possibility of Jerzy Różycki's independent development of the Index of Coincidence, although it increases the probability of such a course of events.

In the literature, it is usual to propose that the change of the method of use of Enigma, which was introduced on September 15, 1938, defeated the decryption methods in use by the Poles at that time, making the further reading of Enigma encrypted messages dependent on two new methods – the Bomby[19] and Zygalski's sheets. The content of Chapter 21 confirms the ineffectiveness of most of the previously developed methods of attack, but contradicts the claim of the basis of decryption using only the Bomby and the sheets. During this period, the Polish cryptographers already possessed such a deep knowledge of the subtleties of the Enigma cipher that in many cases they were able to cope by capturing the interdependencies of the message key characters; these interdependencies were completely invisible to other people. Perhaps the methods described in this chapter explain how the Poles were able to read the cipher in the first half of 1939, when the Bomby lost their effectiveness, and Zygalski's sheets were not yet available. Contrary to the claims of British cryptologists (see the fragment *The Poles have got* [were reading] *the machine to Sept 15th 38 out by luck* in the Knox report above), the Polish Cipher Bureau was reading at least some German messages up till the last days before the outbreak of the war. In Chapter 27, the authors of the report emphasise that *A month later, the German-Polish war broke out. The messages from 25th August 1939, the day of general mobilisation in Germany, were broken (...)*. At this point, the Bomby were no longer useful, and the Poles had Zygalski's complete set of sheets only for two of the 60 possible rotor sequences. It is known that during this period, the keys to the cipher used by the German armed forces mandatorily used at least one of the new rotors which had been put into use in December 1938, so the sheets at the disposal of the Cipher

[19] In this Introduction, the term „Bomba" (plural „Bomby") is used to denote the Polish machine, and is used to differentiate this device from the later, British, „Bombe" (plural „Bombes").

Bureau did not guarantee a solution. Polish cryptologists had therefore to break the cipher using other methods, probably similar to those outlined in Chapter 21.

The chapters beginning with Chapter 27 describe the events after the outbreak of war. As far as their own work in this period is concerned, the Poles refer to their quiet resignation:

> The Polish cryptologists were sitting at the Enigmas constantly, tapping messages and manipulating sheets, so as not to let the British outperform us completely. (...) It was thus understandable that the Polish cryptologists did not achieve significant cryptological results anymore, and the focus of theoretical work shifted to London.

In the Poles' reports, references to the successes of British colleagues begin to appear. Some of them were based on the theoretical pre-war works of the Polish Cipher Bureau: *British cryptologists have implemented yet another method developed earlier by the Poles.* This idea was to create a catalog not only specifying the location of the female cases, but also identifying the characters concerned. Having such a catalog basically facilitated the verification of possible solutions identified using Zygalski's sheets. The Poles did not manage to realise this idea themselves, because the enormous amount of work necessary to create the catalog required its automation. The British, who had constructed the necessary equipment for making the sheets, also used them to implement the Polish idea accompanying the catalog's sheets: *Thanks to their financial and organisational capacity they put our plans into practice, which otherwise would not have seen the light of day*,(...). In the reports from the war activity of Bletchley Park, however, there are no comments pointing to the Polish origin of the idea that underlies the new method of breaking the cipher.

Chapter 28 is devoted entirely to Knox's observations, which allowed the breaking without much effort of, especially, multi-part dispatches. Chapter 30 describes the Herivel method, which during the French campaign helped to overcome the impasse caused by another change in the way Enigma was used. In this case, the Poles however noted modest satisfaction, adding to the success of the young British cryptologist with a correction concerning the turnover points of the new rotors: *Corrections were found and immediately communicated to the British. Only then could Herivel's method be applied effectively.* This fact was not reflected in British sources.

Finally, Chapter 31 describes changes made by the enemy on the eve of the French campaign. The cessation of the double-encryption of the message key was a heavy blow for the Poles who relied on that feature for most, if not all of the decryption methods which they were using. However, it was the Poles who detected the change being prepared and worked out the structure of the new system. Some German cipher clerks used it prematurely, on the eve of its official introduction. Because the Poles at that time already had Zygalski's sets manufactured by the British, they were regularly breaking the keys of German messages. With the keys to the cipher on April 30, they identified messages based on a procedure that was to come into regular use on the following day and easily worked out the nature of the new system, transferring information about its characteristics to London.

The fact that the Poles were breaking the messages being exchanged on a separate S.D. Communication network is known from other sources; however the report being analysed contains many unknown details. The data in Chapter 32 is an additional confirmation that the Poles were still breaking Enigma messages on the eve of the outbreak of World War II: *the last broken day was 31st July 1939.*

Starting from Chapter 33 we deal with matters known so far only in broad outline. The very fact of the Poles breaking the Kriegsmarine messages was known from previously available materials, but its details and above all the scope remained unavailable. The lack of data on the contribution of the Poles led to the conviction that the main burden of struggle with the Kriegsmarine Enigma was carried by British cryptographers, Alan Turing here making the most important contribution to the success. The information contained in Chapters 33–35 makes it necessary to re-analyse the adopted version of the story.

The struggle with the Kriegsmarine ciphers must have been a separate area of interest for Polish cryptologists, remaining somewhat in the shade compared to the other areas of study. This conclusion is prompted by the position of the chapters devoted to this issue in the entire report. The main part of the study maintains (with a significant exception, which we comment on below) a chronologically sequential structure; the chapters devoted to the Kriegsmarine ciphers were added outside this structure, as if they were independent subjects. A few comments scattered in the report confirm that, for purely practical reasons, the German Navy's communications were not the main interest of the Polish Cipher Bureau. In Chapter 2, we find information that *Many years after the creation of the Polish Cipher Bureau, the shortage of staff did not allow attention to be paid to the cipher material coming from the German navy*. In Chapter 34, the cryptologists complain about the difficulties in the attacks on the Kriegsmarine Enigma as a result of having *insufficient cipher material*. Taking account of the fact that Poland was not a maritime power, the character of work on the Kriegsmarine Enigma is perfectly understandable. Even so, the Cipher Bureau achieved impressive results in attacks against the German navy codes and ciphers.

Describing the codes used by the Kriegsmarine prior to the implementation of Enigma (Chapter 33) does not fall within the scope of our analysis. The Poles' adventures with the Kriegsmarine Enigma began in the formal sense only after the German Navy brought the Enigma C model into service at the beginning of 1926, and in a practical sense only in 1933, when the cryptologists decided to apply the methods that they had developed and had successfully used in the attack on the Army's Enigma ciphers. This attack brought immediate success, rendered easier by the lack of a plugboard on the Enigma C. The Poles easily and accurately identified the features of the machine model (29 keys, movable reflector, the specific role of the letter X, etc.). They also noticed a key feature of the Kriegsmarine ciphers, namely that different procedures were used from those used in other branches of the armed forces. From the earliest period, the three-letter message keys were not chosen by the cipher clerks themselves, but were taken from a key list; in addition, they were complemented with the fourth character, which signalled an intention to switch to four-character keys at a later date.

The description of the machine presented in the document and the circumstances of its use by the Kriegsmarine do give rise to a few questions that have not yet been answered, given the current state of knowledge. From the available Enigma manufacturer's documentation, it can be seen that the model C used in the Kriegsmarine from 1926 was equipped with a stationary reflector that could be placed in the device in one of four possible orientations. However, the notes of the Polish cryptologists indicate that the reflector of the machine which they analysed did rotate. Either the cryptologists writing the report without access to source documentation failed to remember this, or there is a gap in our knowledge of the Enigma ma-

chine family. In the light of the universally accepted chronology, on October 1, 1934, Enigma C was replaced in the Kriegsmarine by the Enigma M1 model, the same in principle as the Enigma I model used by the land army (the differences concerned e.g. the labelling of the machine's rings–numbers for the Wehrmacht machine, letters for the Kriegsmarine machine). However, the authors of the report describe the use of Enigma C as late as in 1936: the plain text was encoded prior to encryption, using a four–character code; a method known from previous usage. It follows from this, that the Enigma M1 did not replace Enigma C so much as it was introduced in parallel with it, eventually replacing the older model. German cryptologists, aware of the weakness resulting from the lack of a plugboard, tried to increase the security of the cipher created by the C machine by requiring the pre-encryption of the plaintext before its further encryption with Enigma. However, these precautionary measures proved ineffective: the Poles nevertheless worked out both the construction of the machine and the coding procedures associated with its use.

The most interesting is the information contained in the report on the use of the Kriegsmarine Enigma M1, used in the navy (with some changes) from October 1, 1934 to the end of World War II. The report contains information about the interesting and previously unknown inconsistency of Kriegsmarine cryptologists. In the version introduced for use on November 1, 1934, the Enigma M1 was equipped with five rotors, of which only three were mounted in the machine at one time (as in the Wehrmacht and Luftwaffe machines from December 1938). This allowed breaking the keys of the messages on days when only rotors known from the army Enigma were in use. Such messages constituted about 10% of all messages. This number was enough to confirm the practice known from the period of use of the Enigma C, i.e., drawing the keys only from a previously prepared list, but it was insufficient to reconstruct the complete list. On November 16, 1936, the two additional rotors were unexpectedly discontinued, leaving only the rotors known from the Wehrmacht Enigma. This allowed the breaking of current dispatches using the same methods as for the land forces' and air service messages, and these broken messages made it possible to reconstruct the key list. The key list provided a gateway to the archived pre-change messages; it was enough to use the old grill method to determine the connections of the additional rotors used before November 1936. The Poles later called them IVM and VM rotors, using M (as in *Marine*) to avoid confusion with the standard IV and V rotors. Reading these archived messages enabled identification of two special variants of the cipher: Officers and Staff (Admiral). The Cipher Bureau worked solely on the Officer variant; for the Staff variant, there was both a lack of time and, probably, a shortage of encrypted messages.

On May 1, 1937, there was another change to the encryption procedure. From that point on, the individual key of the message was not encrypted using the machine, but with the help of an external method independent of the Enigma substitution. As with other changes, the Germans made a mistake when changing the procedure, which would cost them the secret of the cipher. A torpedo boat with call signal AFA did not receive timely information about the new encryption procedure (or the tables allowing the encryption of the message key) and during the first few days of May it used the old procedure already known to the Polish Cipher Bureau. As a result, the Poles read a number of Kriegsmarine messages from May 1-8, 1937. It turned out that the machine settings did not change in the period from April 27 to May 8, which gave the cryptologists extensive material to analyse, enabling them to largely

determine the encryption of the message key. The circumstances of the Kriegsmarine cipher breaks after the change in May 1937 gave rise to an episode which in the analysed document is described in a little less in detail than in the Bletchley Park reports, in particular in the official "History of Hut 8" edited by Mahon (i.e. details of the ship's call sign, which made it possible for the Poles to break into the code). In the conclusion of the episode, Mahon noted that *By this method they* [the Poles] *broke out about 15 messages a day and came to the conclusion that the indicating system involved a bigram substitution but they got little further than this.* (...) *The Poles pointed out another possibility, viz, that the trigrams were still probably not chosen at random.* Mahon's description confirms that the Poles had correctly identified the most important features of the key encryption procedure, and that going further would have required the reconstruction or acquisition of the tables used in the bigram substitution.

Until now, the material contained in the Polish report supplemented or corrected the information contained in the postwar reports of Bletchley Park. We have now reached a point where the Polish and the British reports diverge a bit. According to British reports, Alan Turing expanded the gap opened by Poles: *Turing had in fact solved the essential part of the indicator problem*[20]. In fact, the mathematician did not go beyond the point reached in 1937 by the Cipher Bureau team and could not cross this point as long as the bigram tables remained unknown. According to the official "History of Hut 8", the breakthrough came only on April 19, 1940. During the Norwegian campaign, the British captured and searched the armed German trawler "Polares" (the "Narvik Pinch"[21]). Documents that *revealed the precise form of the indicating system,* [and] *supplied the Stecker and Grundstellung for April 23rd and 24th*[22] thus fell into their hands. The documents thereby obtained finally confirmed the accuracy of earlier findings of the Poles and Alan Turing's opinion. The breakthrough, however, was half-way: thanks to the "Narvik Pinch" the British managed to read the messages for 6 days, from 22 to 27 April, after which (except in incidental successes) the Kriegsmarine Enigma again fell silent for a year; the bigram tables were still missing. It was not until May 9, 1941, that not only the operating instructions, but also the bigram tables, which enabled the effective start of the decryption of German navy codes, were found on board the submarine U-110 after it had been abandoned by its crew. In their theoretical work on breaking the Kriegsmarine ciphers, the British did not go beyond the point reached in 1937 by Polish cryptologists. The breakthrough became possible only after getting the documents which were on board the U-boat, and thereafter the British cryptologists managed to continue breaking the code despite further subsequent changes. Somewhat perversely, it can be recalled here the statement of Dilly Knox quoted earlier: *they never worked it out - they pinched it years ago & have followed developments as anyone could but they must have bought it or pinched it.*

The Polish report succinctly gives information about these events: *The details of the new encryption system were only learned when, in 1940, the British were able to recover instructions from a sunken U–Boot. We cannot describe the procedure here in detail, and refer the reader to photographic reproductions of the acquired documents.* We know that instructions for using Enigma, describing among other things the method of encrypting the message key, had been found on board the armed trawler "Polares", not on board of a U-boat. In the same chapter, however, the Poles describe the acquisition of the

[20] "Hut 8 History", p. 14.
[21] http://www.ellsbury.com/gne/gne-024.htm.
[22] "Hut 8 History", p. 22.

previously unknown rotors of the Kriegsmarine Enigma: *In 1940 the British found two rotors marked VI and VII in a sunken U-Boat.* Indeed, on February 12, 1940, the minesweeper HMS Gleaner sank the German submarine U-33, and the rotors VI and VII were found in the pockets of the rescued German sailor. Probably the British did not inform the Allies in detail about the circumstances of their gains, and as a result the two separate events, in the consciousness of the Poles, merged into one episode.

The last chapter of the report confirms that the circumstances quoted by Langer do correspond to the facts. The task of the authors was to make a kind of inventory of the contributions of the three countries to the triumph over Enigma. The authors followed the line of least resistance. In the main part of the report, they emphasised the benefits of cooperation of the cryptologists from the three countries rather than separating out the contributions made by each nation. Only at the end of the report did they add a summary table, in which they conscientiously enumerated the components of triumph over Enigma, dividing them between the cooperating countries. Such a result must inevitably had irritated Bertrand, the initiator of the report. When requesting this report, he must have been convinced that its tone would have unambiguously assigned France a leading role in the cryptological triumph. However, the table has more than 20 elements contributed by the Poles, six areas of British input and only one important element on the part of France–he delivery of the two important documents. Bertrand must have been disappointed. For several years, he had conscientiously provided the Poles with keys to the cipher supplied by the German traitor, and he had hoped that the contribution, so important from his point of view, would have been recorded in the balance sheet. What he did not know was that, by the decision of the heads of the Polish Cipher Bureau, these keys had been sent straight to Maximilian Ciężki's safe, bypassing the cryptologists' desks. Ciężki worked from a reasonable assumption that in the event of an increase in international tension, communication with the French spy would be interrupted, and the Poles would then have been deprived of information about the keys just at the moment when their significance would have increased dramatically. He trusted his cryptologists and assumed that, if deprived of access to the keys, they would develop their own methods of reconstructing them. The mathematicians did not disappoint his trust; Ciężki never needed to reach the safe for the information supplied by Bertrand. Probably, however, no one had informed the Frenchman, who in the end would have felt offended by what he would have considered to be an act which had seriously reduced the effectiveness of his contribution to the decryption of Enigma.

Two aspects of the document under discussion require additional commentary. The first concerns its initial chapters. After scratching the surface of the topic in the two initial sections, the authors throw the reader in at the deep end by presenting the mathematical basis for their successes. While working on the text, they knew its default recipients and were fully aware that mathematics was definitely not their element. If they had only wanted to show the background of their work, probably an expanded footnote or mathematical appendix would have been discreetly attached as the final part of the document. By placing the sections devoted to the theoretical foundations of their success at the beginning of the text, its authors wanted to draw the reader's attention to what they considered the most important aspect of their work: the role of mathematics in their success. They must have comprehended, or at least felt the nature of the cryptological revolution, that was the result of their triumph. Before Rejewski, Różycki and Zygalski, no one had made serious attempts to harness advanced mathematics in the service of cryptology. The use of the sim-

plest statistical methods for counting the incidence of single characters, bigrams, or trigrams in text does not merit attention. Even when the cryptological services of several countries around the world decided to employ mathematicians, they reached for the people more than for the methods of their scientific discipline. The father of contemporary American cryptology, William Friedman, placed in the press an announcement about the intention to employ several "government mathematicians" over a year after the Poznań cryptology course. However, Solomon Kullback, Frank Rowlett and Abraham Sinkov later recalled how they prepared code dictionaries in the first years of their work by throwing cards with the words of the code into the air stream of the fan, thus ensuring their random order. It took a long time before they started using more mathematically sound methods.

The release of the report concerning the breaking of Enigma from theoretical foundations showed that its authors were aware of the significance of the mathematical revolution in cryptology which they initiated. When they gave their work to the British, they had developed their achievements, in a purely practical sense, on a large scale, but in a different sense their involvement brought regression. The algebraic methods which the Poles used had a huge advantage: they practically guaranteed the possibility of breaking the cipher. From the very beginning, the British treated this approach with some suspicion, noting that the condition for the Polish methods to work was the occurrence of the twice-encrypted message key. From the first days after the meeting in Pyry, they were preparing for the inevitable moment when that condition would no longer hold. As a remedy, they proposed methods of breaking ciphers based on statistical properties (the "E" rack[23],[24], Banburismus[25], later automated methods of breaking teletypewriter ciphers using the Colossus device, etc.). They predicted this correctly; before the start of the French campaign, Germany removed the weakness in the Enigma usage procedure, and the Poles' algebraic approach became temporarily useless. However, the British success over the new variant of the cipher had its price; the British could only read the Enigma cipher when they could get a reliable and stable piece of probable text, the so-called "crib", in the messages. A more long-term effect of their approach was the long-term close marriage of cryptology with statistics and probability theory. It took many years for cryptologists to return to the algebraic approach of Marian Rejewski and his colleagues, restoring the balance of applications of mathematics in cryptology.

The second topic that deserves attention is the assessment by the authors of the value of inter-Allied cryptogical cooperation. They wrote their text at the earliest in the second half of 1940. At that time, the cooperation initiated a year earlier was basically a thing of the past. The cryptologists of the pre-war Cipher Bureau were disappointed from all sides. After the evacuation from Poland, they met with disrespect from their own countrymen, who did not allow them to serve in the Polish army reborn in France, leaving them quite unceremoniously under French orders. According to the mathematicians' memoirs, the French were not able to organise work in a way that would have made it possible to use the experience and knowledge of the cryptologists of the Cipher Bureau. The British, on whose loyal cooperation the Poles had been able to rely in the course of the previous year, ceased contact after the

[23] http://www.ellsbury.com/profsbk/profsbk-140.htm
[24] https://www.codesandciphers.org.uk/anoraks/rack.htm
[25] https://en.wikipedia.org/wiki/Banburismus

fall of France. The report's authors must have been feeling great loneliness. Nevertheless, they consistently raised the importance of the cooperation between the three countries over the breaking of the Enigma and the tangible benefits resulting from it. One can only speculate on what further great successes might have been achieved by the cryptologists of France, Great Britain and Poland if their commanders had tuned in to their subordinates' way of thinking, and not only allowed the continuation of cooperation, but also gave it forms that later would assume (not without hiccups) cooperation between UK and US cryptologists.

Przedmowa do wydania drugiego

Istotną zmianą wprowadzoną do drugiego wydania publikacji *Sztafeta Enigmy. Odnaleziony raport polskich kryptologów* jest uzupełnienie go o fotokopię tłumaczenia oryginału raportu na język francuski i odpis tego tłumaczenia. Tekst francuski nie obejmuje całości oryginalnego dokumentu − niektóre rozdziały pominięto całkowicie, inne przetłumaczono dokonując skrótów, dodano także kilka not objaśniających pojęcia używane w oryginale. Różnice charakteru pisma przekładu (przekład zachował się wyłącznie w rękopisie) wskazują na to, że pracowały nad nim dwie osoby. Porównanie go z dostępnymi, odręcznymi zapiskami polskich kryptologów pozwala na wykluczenie autorstwa większości z nich. Z drugiej strony, użycie w przekładzie neologizmów, które nie występują ani w potocznym, ani w literackim języku francuskim, może wskazywać na autorstwo osoby, dla której francuski był językiem obcym. Można także dopuścić założenie, że tłumaczenia dokonały osoby słabo zorientowane we francuskiej terminologii matematycznej i technicznej, większość neologizmów bowiem dotyczy właśnie tych obszarów. Redaktor raportu do chwili obecnej nie zdołał odnaleźć żadnych odręcznych zapisków dwojga najbardziej prawdopodobnych autorów tłumaczenia − Gustave'a Bertranda i jego żony, Mary Bertrand. Nie można więc ani potwierdzić, ani wykluczyć, że to oni dokonali tłumaczenia.

Pewne wnioski dotyczące celu opracowania francuskiego przekładu nasuwa wybór rozdziałów i zakres dokonanych skrótów − objęły one przede wszystkim rozdziały prezentujące historię złamania szyfru Enigmy, w całości natomiast przetłumaczono fragmenty opisujące matematyczne podstawy dokonywania prób deszyfrażu. Pamiętając notę pułkownika Gwidona Langera ilustrującą cel opracowania raportu, należy podkreślić, że pominięcie rozdziałów o charakterze historycznym wydaje się czytelne. Raport nie spełnił oczekiwań jego zleceniodawcy, Gustave'a Bertranda, którego zdaniem w niewystarczającym stopniu podkreślił zasługi Francji i jego samego w złamaniu szyfru. Pominięcie fragmentów historycznych pozwoliło zapewne na przeniesienie akcentów dyskusji o złamaniu szyfru z wkładu Polski, Wielkiej Brytanii i Francji w cały sukces na czysto techniczną analizę metod deszyfrażu i tym samym na zminimalizowanie największej wady tekstu z punktu widzenia Bertranda.

Poza dodaniem francuskiego przekładu, we wstępie do pierwszego wydania raportu oraz w treści przypisów wprowadzono nieliczne korekty, odzwierciedlające zmianę stanu wiedzy Redaktora od momentu publikacji pierwszego wydania materiału.

Preface to the second edition

An important novelty of the second edition of the report is the addition of a photocopy and a transcript of the French translation. The term "translation" is somewhat misleading. The French text does not cover the whole of the original document; some chapters have been omitted completely, others have been translated with abbreviations, and some explanatory notes on the terms used in the original have been added. Differences in the nature of the handwriting (the French translation has only been preserved in the manuscript) indicate that two people worked on it. Comparison of the script with available, handwritten notes by Polish cryptologists allows to exclude the authorship of the majority of the Polish team members. On the other hand, the use in translation of neologisms that do not appear in everyday or literary French may indicate the authorship of a person for whom French was a foreign language. Alternatively, translation can be attributed to the people who were poorly versed in French mathematical and technical terminology, as most neologisms concern these areas. The editor of the report has so far been unable to locate any samples of the handwritten text of the two most probable authors of the translation, Gustave Bertrand and his wife, Mary Bertrand. This does not allow to confirm or exclude their authorship.

The abbreviations included mainly chapters presenting the history of breaking the cipher, while sections describing the mathematical basis of the attack on the Enigma were translated in the entirety. Remembering the aforementioned Langer's note illustrating the purpose of the report, the omission of historical chapters seems understandable. In Bertrand's opinion, the report did not sufficiently emphasize the merits of France and his own around breaking the cipher. The omission of historical sections probably allowed the discussion to shift from the contribution of the three countries to the level of purely technical analysis of the methods of breaking the cipher, thus minimizing the key flaw of the text from Bertrand's point of view.

In addition to the French translation, only a few corrections have been made to the text of the introduction to the first edition and the texts of the footnotes, reflecting the change in the state of knowledge between the two editions.

Raport – fotokopia oryginału

E N I G M A

Kurzgefasste Darstellung

der Auflösungsmethoden.

Inhaltsverzeichnis.

Seite

1. Einleitung 3

2. Die Anfänge 5

3. Zykelntheorie 6

4. Zwei wichtige Schriftstücke 8

5. Substitutionentheorie 9

6. Die Substitution E 14

7. Die Substitution S 15

8. Einige Ziffern 17

9. Auffindung der Spruchschlüssel 19

10. Methode der charakteristischen Schlüssel 20

11. Die statistische Methode 20

12. Methodungleicher Buchstaben 21

13. Bestimmung der rechten Walze 22

14. Der Rost 24

15. Der Katalog F 26

16. Der Zyklometer 27

17. Grundstellung und Ringstellung 28

18. Einige Bemerkungen 29

19. Neue Netze. Beständige Änderungen 30

20. Umkehrwalze B 30

21. Neue Chiffrierwalzen 31

22. Änderung des Chiffriersystems 32

23. Auffindung der Walzenlage 33

Seite

24. Bomben 5

25. Die Netze 37

26. Die Warschauer Konferenz 38

27. Kriegsausbruch. Vignolles 41

28. Methode Knox 42

29. Kataloge zu den Netzen 43

30. Methode Herivel 43

31. Drittes Chiffrierverfahren 44

32. Chronologische Übersicht über die Änderungen des Schlüsselverfahrens im Heer und in der Luftwaffe 45

33. Das Funknetz des Sicherheitsdienstes 47

34. Die Schlüsselverfahren der deutschen Kriegsmarine vor Einführung der Enigma 49

35. Die Marine-Chiffriermaschine mit 29 Tasten 50

36. Die Anwendung in der deutschen Kriegsmarine der Enigma-Chiffriermaschine mit 26 Tasten 55

37. Chronologische Übersicht über die Anwendung von Enigma-Chiffriermaschinen in der deutschen Kriegsmarine 60

38. Teilnahme der drei Staaten an der Lösung der Enigma. 61

1.Einleitung.

Bereits wenige Jahre nach Beendigung des Weltkrieges begann die deutsche Wehrmacht zur Verschlüsselung von Nachrichten,die auf dem Funkwege übersandt werden sollten,sich der "Enigma-Chiffriermaschine" zu bedienen.

Als erste führte,wie es scheint,die deutsche Kriegsmarine dieses Schlüsselverfahren bei sich ein.Jedenfalls ist gewiss, dass sie es bereits im Jahre 1926 benutzte,während seine Anwendung im deutschen Heer erst ab 15.Juli 1928 festgestellt wurde.

Am 1.August 1935 folgte dann mit der Einführung der Enigma die deutsche Luftflotte,vom September 1937 ab bediente sich ihrer der Sicherheitsdienst,auch von der Polizei wurde sie benutzt.Während sich so der Gebrauch der Enigma in der deutschen Wehrmacht immer mehr verbreitete,begannen andere Schlüsselmethoden,wie z.B.das Doppelwürfelverfahren, allmählich zu verschwinden,sodass bereits eine gewisse Zeit vor Beginn des Deutsch-Polnischen Krieges 1939 beinahe alles,was von deutschen Institutionen militärischen oder halbmilitärischen Charakters dem Funkwege anvertraut wurde,mit der Enigma-Maschine verschlüsselt war.Die Lösung dieses Schlüsselverfahrens bildete daher für die Generalstäbe Polens,Frankreichs und Grossbritanniens ein Problem von erstklassiger Bedeutung.Im Laufe der Jahre wurde der Typ der Maschine mehrfach geändert.Vor Einfüh-

rung der Enigma "K" mit Steckerverbindung,die noch heute im Gebrauch ist,benutzte das deutsche Heer in der Zeit vom 15.Juli bis 31.Mai 1930 die Enigma "G" mit Stöpselstellung.Bei den ~~Wehrkreisnummern~~ ~~Wehrkreisstäben~~ bediente man sich eine Zeit lang einer selbstschreibenden Maschine,der sogenannten "Enigma II",die jedoch anscheinend als unpraktisch bald aus dem Verkehr gezogen wurde.Die deutsche Kriegsmarine wiederum wandte bis September 1934 einen Maschinentyp mit 29 statt mit 26 Tasten an und ging erst ab Oktober 1934 zum Gebrauch derselben Maschine wie das deutsche Heer über.Übrigens bewahrte die deutsche Kriegsmarine auch späterhin eine gewisse Selbstständigkeit,indem sie in gewissen Zeiträumen eine grössere Anzahl von Schlüsselwalzen benutzte als die übrigen Formationen.Grundsätzlich kann man jedoch sagen,dass ab Oktober 1934 bis heute nur ein Maschinentyp gebraucht wird,derselbe,dessen sich das deutsche Heer seit 1.Juni 1930 bedient.

Im folgenden wird skizziert,auf welche Weise es dem Schlüsseldienst des polnischen Generalstabes gelang,den oben angeführten Typ der Enigma wiederherzustellen und welche Verfahren weiterhin ausgedacht wurden,um das eingehende Chiffriermaterial fast stets laufend zu lösen,trotz sämtlicher Veränderungen und Verbesserungen,die andauernd vom deutschen Schlüsseldienst eingeführt wurden,um das Verfahren absolut unlösbar zu machen.Es wird auch dargestellt werden,von wie grosser Tragweite die Zusammenarbeit der Generalstäbe Polens,Frankreichs und Grossbritanniens sich in dieser Hinsicht erwies.

2.Die Anfänge.

Noch mehrere Jahre nach Gründung des polnischen Schlüsseldienstes konnte aus Personalmangel dem einlaufenden Schlüsselmaterial der deutschen Kriegsmarine keine Beachtung geschenkt werden. Daher wurde das Erscheinen der Enigma erst in dem Augenblick bemerkt,als sich ihrer das deutsche Heer zu bedienen begann,d.h. im Jahre 1928.

Unter den einlaufenden Sprüchen,die von deutschen Militärfunkstationen aufgegeben wurden,zeigten sich damals neben solchen, die wie bisher nach dem Doppelwürfelverfahren geschlüsselt waren, auch andere,die zweifellos den Charakter eines Substitutionsverfahrens aufwiesen.Man begann sich mit ihnen zu beschäftigen und stellte leicht fest,dass die sechs ersten Buchstaben eines jeden Spruches eine besondere Bedeutung hatten und wahrscheinlich den Schlüssel des gegebenen Spruches darstellten.

Gleichzeitig gelang es dem polnischen Nachrichtendienste,in den Besitz mehrerer kleiner Schriftstücke zu kommen,aus denen hervorging,dass vom 15.Juli 1928 ab im deutschen Heer neben den bisherigen Schlüsselverfahren als neues das "Maschinenschlüsselverfahren Enigma G" in Kraft trat,dass bei der Enigma * eine Stöpselstellung (während bei dem späteren Typ eine Steckerverbindung) vorhanden war,und dass jede Dienststelle im gewissen Zeitabständen eine Anzahl von Schlüsseln zugeteilt bekommt,von denen jeder aus drei Zahlen nicht grösser als 26 besteht.

Es war nunmehr klar, dass das neue Schlüsselverfahren, das man entdeckt hatte, identisch mit dem Enigmaschlüsselverfahren war. Um das Studium dieses Verfahrens zu erleichtern, wurde vom polnischen Generalstab eine Enigma vom Handelstypus angekauft, bei der selbstverständlich die Walzen ganz andere Schaltungen hatten, als bei der im Dienste des Heeres stehenden Maschine, die sich aber auch sonst noch, wie sich später herausstellte, in mehrerer Hinsicht stark von der letzteren unterschied. Die Untersuchungen dieses Schlüsselverfahrens wollten jedoch nicht recht von der Stelle rücken und wurden nach einiger Zeit abgebrochen.

3. Zykelntheorie.

Die Wiederaufnahme der Arbeiten erfolgte im Jahre 1932. Man unterzog die 6 ersten Buchstaben der Sprüche einer erneuten Untersuchung und stellte dabei folgendes fest: Für jeden Tag wird eine gewisse Stellung der Walzen, eine und dieselbe für sämtliche Schlüssler, festgesetzt. Daraufhin wählt sich jeder Schlüssler drei beliebige Buchstaben, schlüsselt sie zweimal hintereinander ausgehend von der für diesen Tag festgesetzten Stellung der Walzen und setzt die so erhaltenen 6 Buchstaben in den Anfang des Spruches ein.

Auf diese Weise entstehen zwischen dem 1. und 4., bezw. 2. und 5. bezw. 3. und 6. Buchstaben der Sprüche gewisse Beziehungen, die eine rein mathematische Behandlungsweise gestatteten und die Grundlage der späteren Wiederherstellung der Enigma bildeten.

Man verfährt folgendermassen: Man nimmt irgendeinen Spruch, schreibt dessen ersten Buchstaben und ~~stets~~ rechts davon dessen vierten Buchstaben auf.Dann sucht man einen Spruch,in dem der zuletzt aufgeschriebene Buchstabe als erster Buchstabe auftritt und schreibt rechts von ihm dessen vierten Buchstaben auf.So verfährt man weiter,bis man zum ersten Buchstaben zurückkehrt.Das erhaltene Ergebnis nennt man einen Zyklus.Man kann nun folgende Sätze beweisen:

1) Zykeln derselben Länge treten stets in gerader Zahl auf.

2) Buchstaben eines Zyklus werden durch Buchstaben hervorgerufen,die in einem anderen,gleichlangen Zyklus auftreten.

3) Wird ein Buchstabe X durch einen Buchstaben Y hervorgerufen,so wird der rechts von X stehende Buchstabe durch den links von Y stehenden Buchstaben hervorgerufen.

Diese drei Sätze lösten teilweise die Aufgabe,die Spruchschlüssel zu rekonstruieren,und bestimmt hätte man schon damals dieses Problem vollständig gelöst,wenn nicht gerade in diesem Augenblick Hilfsmittel zur Verfügung gestellt worden wären,die die Arbeiten in andere Bahnen lenkten.

4.Zwei wichtige Schriftstücke.

In dieser Zeit gelangte nämlich die polnische Schlüsselstelle in den Besitz zweier Schriftstücke von ausserordentlicher Bedeutung.Das erste dieser beiden Schriftstücke trug die Überschrift: "Anleitung zum Maschinenschlüsselverfahren",während das andere die sogenannten Tagesschlüssel zur Enigma für die Monate Oktober und Dezember 1931 enthielt.Diese Schriftstücke erhielt die polnische Schlüsselstelle vom französischen Generalstab,der in ihren Besitz durch seinen Nachrichtendienst gelangt war.Es muss betont werden,dass der Besitz dieser Schriftstücke und zwar besonders der Tagesschlüssel entscheidend den Fortgang der Arbeiten beeinflusst hat.Ohne diese Dokumente wäre die Lösung des Enigmaschlüsselverfahrens zumindest um Jahre verzögert worden.Andererseits mag jedoch auch festgestellt werden,dass es weder der französischen noch der englischen Schlüsselstelle gelungen war,das Verfahren zu lösen,trotzdem beide Stellen im Besitz dieser Schriftstücke waren.Übrigens wird weiter unten eine Methode angegeben werden,die eventuell auch ohne den genannten Schriftstücken zum Ziele geführt haben würde.

Aus dem ersten der genannten Dokumente ging hervor,dass ab 1.Juni 1930 an Stelle der bisherigen Enigma mit Stöpselstellung eine neue Enigma mit Steckerverbindung trat.Weiter erfuhr man noch folgendes:

1) Die Maschine enthält 3 Schlüsselwalzen,deren Lage verändert werden kann.Änderung der Walzenlage erfolgt alle drei Monate.

2) Die Umkehrwalze ist fest (im Gegensatz zur Enigma-Handelsmaschine).

3) Die Schlüsselwalzen sind mit einem Zahlen-,bezw.Buchstabenring versehen.Änderung der Ringstellung erfolgt täglich.

4) Die Steckerverbindung vertauscht 6 Paar Buchstaben.Änderung der Steckerverbindung erfolgt täglich.

5) Die Stellung,von der aus der Spruchschlüssel geschlüsselt wird,heisst Grundstellung.Änderung der Grundstellung erfolgt täglich.

Das zweite Dokument enthielt,wie bereits bemerkt wurde,die Tagesschlüssel,d.h.Walzenlage,Grundstellung,Ringstellung,Steckerverbindung,für die Dauer von zwei Monaten.

5.Substitutionentheorie.

Man schritt nun zur Bewältigung des Hauptproblems,d.h.zur Rekonstruktion der Walzenschaltungen.Man bediente sich hierbei einer mathematischen Theorie,der so genannten Substitutionentheorie,die selbstverständlich hier nicht auseinandergesetzt werden kann,sondern vielmehr als bekannt vorausgesetzt wird.Man muss sich natürlich nicht vorstellen,dass es einfach genügte, bekannte Sätze der Substitutionentheorie anzuwenden,um das Ergebnis zu erhalten.Im Gegenteil war auf dem Wege zum Endziele eine ganze Reihe überaus schwieriger Hindernisse zu überwinden.

Im folgenden geben wir kurz den eingeschlagenen Gedankengang an. Das Schlüsselverfahren Enigma ist ein Substitutionsverfahren, d.h.die Maschine setzt in jeder Position der Walzen für die Buchstaben des Alphabets andere Buchstaben ein.Wir bezeichnen mit A_1 die Substitution,der die Buchstaben des Alphabets unterworfen sind,wenn sich die Walzen in der für den gegebenen Tag festgesetzten Grundstellung befinden,mit A_2 die Substitution in der nächstfolgenden Stellung der Walzen u.s.w.bis A_6.

Wenn man über eine genügende Anzahl von Sprüchen verfügt (im Durchschnitt etwa 80),so wird man mit Hilfe der Zykelntheorie zunächst die Produkte A_1A_4 ; A_2A_5 ; A_3A_6 bilden können,die daher als bekannt vorausgesetzt werden können.Wir bezeichnen nun weiter durch

S die Substitution hervorgerufen durch die Steckerverbindungen.

C_γ " " " " rechte Schlüsselwalze.

C_β " " " " mittlere "

C_α " " " " linke "

U " " " " die Umkehrwalze.

E " " " " " Eintrittwalze.

Q =(1,2,3,4,5,6,.....24,25,26)

Wenn während des Chiffrierens des Spruchschlüssels die mittlere Walze sich nicht fortbewegt,was ziemlich wahrscheinlich ist und was wir im Folgenden voraussetzen wollen,so können die Substitutionen A_1 bis A_6 auf folgende Weise dargestellt werden:

$$A_1 = \quad S\,E\,C_\gamma C_\beta C_\alpha U\, C_\alpha^{-1} C_\beta^{-1} C_\gamma^{-1} E^{-1} S^{-1}$$

$$A_2 = S\,E\,Q\,C_\gamma C_\beta C_\alpha U\, C_\alpha^{-1} C_\beta^{-1} Q\, C_\gamma^{-1} E^{-1} S^{-1}$$

$$A_3 = S\,E\,Q^2 C_\gamma C_\beta C_\alpha U\, C_\alpha^{-1} C_\beta^{-1} Q^2 C_\gamma^{-1} E^{-1} S^{-1}$$

$$\vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots$$

$$A_6 = S\,E\,Q^5 C_\gamma C_\beta C_\alpha U\, C_\alpha^{-1} C_\beta^{-1} Q^5 C_\gamma^{-1} E^{-1} S^{-1}$$

Die erste Schwierigkeit, die zu überwinden war, bestand darin, dass nicht nur die rechten, sondern auch die linken Seiten der Gleichungen unbekannt sind, bekannt sind nur die Produkte $A_1 A_4$, $A_2 A_5$, $A_3 A_6$. Die Zyklentheorie lehrt nun jedoch, dass die Substitution A_1 in den meisten Fällen nicht mehr als etwa hundert Bezeichnungen annehmen kann und, dass gleichzeitig jede Bezeichnung von A_1 eindeutig die Substitution A_4 festsetzt. Dasselbe gilt von A_2 und A_5, bezw. A_3 und A_6. Man kann sich also vorstellen, dass sämtliche Bezeichnungen von A_1 bis A_6 aufgeschrieben sind. Auf diese Weise kann man die erste Schwierigkeit als überwunden betrachten, auf Kosten allerdings einer vielfachen Vergrösserung der Arbeitzeit, denn bei den weiteren Operationen müssen sämtliche möglichen Bezeichnungen für A_1 bis A_6 der Reihe nach eingesetzt werden.

Die zweite Schwierigkeit ist noch viel ernster. Trotz grösster Bemühungen nämlich, die noch jahrelang aus theoretischen Gründen fortgesetzt wurden, nachdem die Walzenschaltungen schon längst gefunden waren, liessen sich die oben angeführten Gleichungen auf

keine Weise lösen,das grösste Hindernis stellte stets die Substitution S,d.h.die Steckerverbindung dar.Man hat zwar schliesslich eine Methode gefunden,die vielleicht zum Ziele geführt hätte,sie setzte jedoch die Kenntnis der Substitutionen A_1 bis A_6 (und nicht bloss der Produkte A_1A_4,A_2A_5,A_3A_6),die Kenntnis der Substitution E,und ferner recht umfangreiches Material voraus.

So wurde denn die zweite und Hauptschwierigkeit auf dem Wege zur Lösung der Enigma vor allem durch das vom französischen Generalstab zur Verfügung gestellte Schriftstück,das die Steckerverbindungen für zwei Monate enthielt,überwunden.

Die dritte Schwierigkeit beruhte auf der Unkenntnis der Substitution E.Es scheint,dass dies das Hindernis war,an dem die Bemühungen der englischen Kryptologen gescheitert sind.Spätere Untersuchungen in der polnischen Schlüsselstelle ergaben,dass man die Substitution E auf deduktivem Wege hätte finden können (vorausgesetzt,dass S bekannt ist),in Wirklichkeit jedoch fand man E durch Probieren.Man nahm zunächst an,die Substitution E sei dieselbe wie in der Enigma-Maschine vom Handelstypus,d.h.:

Q	W	E	R	T	Z	U	I	O	A	S	D	F	G	H	J	K	P	Y	X	C	V	B	N	M	L
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Als man mit dieser Annahme kein Resultat erzielte,glaubte man anfangs,dass am gewählten Tage während des Chiffrierens der Tagesschlüssel eine Verschiebung der mittleren Walze stattfände. Man wiederholte also die ganzen Operationen noch einmal auf dem

Material einer anderen Tages und,als man wieder kein Ergebnis erzielte,nahm man einen dritten und vierten und fünften Tag.

Die Arbeiten,die bereits Monate dauerten,sollten schon abgebrochen werden,als man noch einen Versuch machte und zwar unter der Annahme

$$\Sigma = \begin{pmatrix} A & B & C & D & E & F & G & H & I & J & K & L & M & N & O & P & Q & R & S & T & U & V & W & X & Y & Z \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 & 26 \end{pmatrix}$$

Diesmal hatte man Glück,die Annahme stellte sich als richtig heraus und führte zur Lösung der Aufgabe.

Zur Orientierung des Lesers wird mitgeteilt,dass zur Auffindung der Schaltungen der rechten Walze unser oben angeführtes System von 6 Gleichungen zunächst auf folgende Form gebracht werden muss.

$$E^{-1}S^{-1}A_1 S E Q^{-1} E^{-1} S^{-1} A_1 S E Q^3 = C_\gamma \left[C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1} Q^{-3} C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1} Q^3\right] C_\gamma^{-1}$$

$$Q^{-1}E^{-1}S^{-1}A_2 S E Q^{-1} E^{-1} S^{-1} A_2 S E Q^4 = C_\gamma Q^{-1} \left[C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1} Q^{-3} C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1} Q^3\right] Q\, C_\gamma^{-1}$$

$$Q^{-2}E^{-1}S^{-1}A_3 S E Q^{-3} E^{-1} S^{-1} A_3 S E Q^5 = C_\gamma Q^{-2} \left[C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1} Q^{-3} C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1} Q^3\right] Q^2 C_\gamma^{-1}$$

Die Gleichungen sind trotz ihrer Länge nicht besonders kompliziert.Alle Ausdrücke auf der linken Seite sind bekannt,alle Ausdrücke auf der rechten Seite haben einen gemeinsamen Mittelteil.Durch Elimination dieses Teiles erhält man $C_\gamma Q\, C_\gamma^{-1}$,und hieraus unmittelbar C_γ,d.h.die Schaltungen der rechten Walze.

Man musste selbstverständlich noch die Schaltungen der linken,mittleren und Umkehrwalze auffinden sowie die Positionen,

bei denen die Walzen sich drehten,da man jedoch hierbei keine grundsätzlich neuen Methoden anwandte,so mögen die diesbezüglichen Arbeiten übergangen werden.

6.Die Substitution E.

Wir wollen kurz skizzieren,wie man die Substitution E auch deduktiv hätte finden können.

Da wir im Besitze der Tagesschlüssel für zwei Monate sind, können wir leicht zwei solche Tage finden,in denen sowohl die Walzenlage als auch die Position der rechten Walzen,d.h.die Differenz zwischen Grund- und Ringstellung der rechten Walze dieselbe ist.Wir stellen für diesen beiden Tage die zwei Gleichungssysteme A_1 bis A_6 auf,und erhalten,wenn wir zur Abkürzung

$$F = C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1}$$

setzen und die Buchstaben,die sich auf den zweiten Tag beziehen, unterstreichen:

$$A_1 = \quad S\,E\,C_\gamma F C_\gamma^{-1} E^{-1} S^{-1} \qquad \underline{A}_1 = \quad \underline{S}\,E\,C_\gamma \underline{F} C_\gamma^{-1} E^{-1} \underline{S}^{-1}$$

$$A_2 = S\,E\,Q\,C_\gamma Q^{-1} F\,Q\,C_\gamma^{-1} Q^{1} E^{-1} S^{-1} \qquad \underline{A}_2 = \underline{S}\,E\,Q\,C_\gamma Q^{-1} \underline{F}\,Q\,C_\gamma^{-1} Q^{1} E^{-1} \underline{S}^{-1}$$

$$A_3 = S\,E\,Q^2 C_\gamma Q^{-2} F\,Q^2 C_\gamma^{-1} Q^{-2} E^{-1} S^{-1} \qquad \underline{A}_3 = \underline{S}\,E\,Q^2 C_\gamma Q^{-2} \underline{F}\,Q^2 C_\gamma^{-1} Q^{-2} E^{-1} \underline{S}^{-1}$$

$$\vdots \qquad\qquad \vdots \qquad\qquad \vdots$$

$$A_6 = S\,E\,Q^5 C_\gamma Q^{-5} F\,Q^5 C_\gamma^{-1} Q^{-5} E^{-1} S^{-1} \qquad \underline{A}_6 = \underline{S}\,E\,Q^5 C_\gamma Q^{-5} \underline{F}\,Q^5 C_\gamma^{-1} Q^{-5} E^{-1} \underline{S}^{-1}$$

Hieraus bilden wir folgende Gleichungen,in denen die rechten Seiten bekannt sind:

$$S^{-1}A_1 S\, \underline{S^{-1}A_1 S} = \quad E\, C_\gamma P \underline{P}\, C_\gamma^{-1} E^{-1}$$

$$S^{-1}A_2 S\, \underline{S^{-1}A_2 S} = E\, Q\, C_\gamma Q^{-1} P \underline{P}\, Q\, C_\gamma^{-1} Q^{-1} E^{-1}$$

$$\vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots$$

$$S^{-1}A_6 S\, \underline{S^{-1}A_6 S} = E\, Q^5 C_\gamma Q^{-5} P \underline{P}\, Q^5 C_\gamma^{-1} Q^{-5} E^{-1}$$

Durch Elimination von $P\,\underline{P}$ erhalten wir die Ausdrücke:

$$E\,(Q\, C_\gamma Q^{-1} C_\gamma^{-1}) E^{-1}$$

$$E\, Q\,(Q\, C_\gamma Q^{-1} C_\gamma^{-1}) Q^{-1} E^{-1}$$

$$E\, Q^2 (Q\, C_\gamma Q\, C_\gamma) Q^{-2} E^{-1}$$

$$\vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots$$

$$E\, Q^4 (Q\, C_\gamma Q^{-1} C_\gamma^{-1}) Q^{-4} E^{-1}$$

und hieraus durch ~~—~~ Elimination von $Q\, C_\gamma Q^{-1} C_\gamma^{-1}$ zunächst $E\, Q^{-1} E^{-1}$, und hieraus unmittelbar E.

Der Weg zum Ergebnis ist recht lang, besonders wenn die Substitutionen A_1 bis A_6 selbst nicht, sondern nur die Produkte $A_1 A_4$, $A_2 A_5$, $A_3 A_6$ bekannt sind, und die tatsächliche ~~Auffindung~~ Auffindung der hier skizzierten Operationen würde eine Person sicherlich mehrere Monate lang in Anspruch nehmen. Jedenfalls über möge festgestellt werden, dass, wenn nur die Steckerverbindungen bekannt sind, man stets auf diese oder auf andere Weise zum Ziel gelangt wäre.

7. Die Substitution S.

Wir wollen endlich noch einen Weg zeigen, wie man wahrscheinlich auch zum Ziele gelangt wäre, wenn man sich nicht im Besitze der Schlüssel für zwei Monate befunden hätte. Es muss hierbei

allerdings vorausgesetzt werden, dass die Substitution E bekannt ist oder wenigstens erraten wird, wie es ja schliesslich in Wirklichkeit geschehen ist. Ferner muss angenommen werden, das die Substitutionen A_1 bis A_6 selbst und nicht bloss die Produkte $A_1A_2, A_1A_3, A_2A_5, A_3A_6$ bekannt sind. Auch das hätte man sicherlich erzielt. Und endlich müssen wir über so umfangreiches Materiel verfügen, dass wir in mehreren hundert Tagen die Substitutionen A_1 bis A_6 bilden können. Wenn alle diese Voraussetzungen erfüllt sind so ist zu erwarten, dass man zwei Tage findet, in denen die Walzenlage dieselbe ist, die Differenz zwischen Grund- und Ringstellung der linken und mittleren Walze dieselbe ist, und die Differenz zwischen Grund- und Ringstellung der rechten Walze sich nicht mehr als 3 unterscheidet. Tritt ein solcher Fall ein, so ist er leicht aufzudecken. Denn nehmen wir etwa an, die Positionen der rechten Walzen unterscheiden sich in den beiden Tagen um 3, so dass etwa die Substitutionen A_1 und A_4 in derselben Position entstehen. Dann müssen zunächst einmal die Produkte A_1A_2 und A_4A_5 einerseits und die Produkte A_1A_3 und A_5A_6 andererseits einander ähnlich sein, wie man sich leicht überzeugt, wenn man die betreffenden Gleichungen aufschreibt:

$$A_1A_2 = S(E\,G\,Q\,Q\,G\,Q^{-1}E^{-1})S^{-1} \qquad A_4A_5 = \underline{S}(E\,G\,Q\,Q\,G\,Q^{-1}E^{-1})\underline{S}^{-1}$$

$$A_2A_3 = S(EQG\,Q\,G\,Q^{-2}E^{-1})S^{-1} \qquad A_5A_6 = \underline{S}(E\,Q\,G\,Q\,Q\,G\,Q^{-2}E^{-1})\underline{S}^{-1}$$

wobei man zur Abkürzung $C_\alpha C_\beta C_\gamma U C_\gamma^{-1} C_\beta^{-1} C_\alpha^{-1} = G$ gesetzt hat.

Ferner kann man aus den Gleichungen $A_1 A_4$ und $A_4 A_5$ einerseits und aus den Gleichungen $A_2 A_3$ und $A_5 A_6$ andererseits das Produkt $S\underline{S}$ errechnen und dies Produkt muss in beiden Fällen gleich sein. Und schliesslich muss das Produkt $S\underline{S}$ aus mindestens 14 Zykeln bestehen.

Die Hauptschwierigkeit besteht nun darin, dass man auf diese Weise nur das Produkt $S\underline{S}$ und nicht die Substitutionen S und $\underline{S}$ einzeln erhält. Es zeigt sich aber, dass im Allgemeinen S und $\underline{S}$ nur mehrere hundert verschiedene Werte annehmen werden. Wir müssen also diese Werte der Reihe nach in unseren Gleichungen einsetzen und versuchen, zu einem Ergebnis zu gelangen. Eine sehr grosse Arbeit, die sicherlich unausführbar wäre, wenn auch noch die Substitutionen A_1 bis A_6 nicht einzeln, sondern nur ihre Produkte zu zweien bekannt wären.

8. Einige Ziffern.

Eine vollständige Beschreibung der Maschine Enigma würde den Rahmen dieser Skizze weit überschreiten. So wollen wir uns denn begnügen einige Zahlen anzugeben, um zu zeigen, ein wie starkes Instrument vom kryptologischen Standpunkt aus die Enigma darstellt, vorausgesetzt natürlich, dass sie richtig angewandt wird.

Die Anzahl verschiedener Walzenlagen beträgt bei drei Walzen

$$3.2.1 = 6$$

und bei fünf Walzen

$$5.4.3. = 60$$

Die

Die Zahl der verschiedenen Grundstellungen und Ringstellungen beträgt

$$26^3 = 17576$$

Die Zahl verschiedener Positionen der Walzen beträgt mithin (zusammen mit den Walzenlagen) bei drei Walzen

$$105456$$

und bei fünf Walzen

$$1054560$$

Die Zahl verschiedener Steckerverbindungen beträgt bei 6 Paaren

$$\frac{26!}{2^6 \cdot 6!14!} = 100391791500$$

und bei zehn Paaren

$$\frac{26!}{2^{10} \cdot 10!6!} = 150738274937250$$

Die Zahl verschiedener Schaltungen für die Umkehrwalze beträgt

$$\frac{26!}{13!\ 2^{13}} = 7905853580625$$

und für die übrigen Walzen

$$26! = 403291587620262925584000000$$

Die letzte Zahl kann man sich folgendermassen veranschaulichen: Wenn sämtliche die Erdkugel bewohnenden Menschen in jeder Sekunde je eine Schaltung ausführen würden, so würden sie ihre Arbeit erst nach sechs Milliarden Jahren beenden (wobei nebenbei bemerkt werden möge, dass angeblich die Welt erst seit 2 Milliarden Jahren existiere).

9.Auffindung der Spruchschlüssel.

Folgendes Problem ist bisher gelöst worden:Bei Kenntnis der Schlüssel für zwei Monate die Walzenschaltungen auffinden.Damit ist jedoch die Aufgabe nicht beendet.Es handelt sich vielmehr jetzt um die Lösung des umgekehrten Problems:Bei bekannten Walzenschaltungen die Schlüssel finden.

Zunächst wurde im technischen Büro der polnischen Schlüsselstelle die Enigma vom Handelstyp so umgeändert,dass sie zum Lesen von Militärsprüchen dienen konnte.Daraufhin wurde das Spruchmaterial für die zwei Monate,für die Schlüssel vorhanden waren, gelöst und hierbei eine Reihe von Fehlern,die von den Schlüsslern begangen wurden,entdeckt und natürlich ausgenutzt.Diese Fehler dienten vor allem zur Auffindung der Spruchschlüssel d.h. der Schlüssel,die von den Chiffranten willkürlich gewählt,zweimal geschlüsselt und daraufhin am Anfang des Spruches eingesetzt werden.Im Laufe der Jahre gelang es zwar den Deutschen,ihr Schlüsselpersonal so zu schulen,dass immer weniger Fehler begangen wurden,die Entwicklung in dieser Richtung ging jedoch genügend langsam von statten,so dass es stets gelang,in der Zwischenzeit immer raffiniertere Methoden auszusinnen,um trotz allem die Spruchschlüssel auffinden zu können.

10.Methode der charakteristischen Schlüssel.

In der ersten Zeit nach Einführung der Enigma wählten die Schlüssler mit Vorliebe solche Schlüssel,die aus 3 gleichen Buchstaben bestanden wie AAA,BBB,u.s.w.Die Methode der charakteristischen Schlüssel beruhte nun darauf,mit Hilfe der Zyklentheorie die einzelnen Zykeln so einander zuzuordnen,um möglichst viele aus drei gleichen Buchstaben bestehenden Schlüssel zu erhalten.Bald jedoch wurde den Schlüsslern die Wahl dreier gleicher Buchstaben verboten.Daraufhin begannensie,sich solche Buchstaben zu wählen,die sich auf dem Glühlampenfeld der Maschine

Q W E R T Z U I O

A S D F G H J K

P Y X C V B N M L

quer oder wagerecht nebeneinander befinden,wie ASD,QAY,QWE,u.s.w. Es genügte jetzt die Zykeln so einander zuzuordnen,dass möglichst viele Schlüssel wie ASD u.s.w.entstanden.

11.Die statistische Methode.

Bald aber wurde auch das verboten.Inzwischen bemerkte man jedoch,dass die Buchstaben des Alphabets in den Schlüsseln nicht mit gleicher Häufigkeit auftraten.So zum Beispiel traten auf als erste Buchstaben in den Schlüsseln vor allem die Buchstaben A und Q,als zweite Buchstaben sämtliche Vokale,als dritte Buchstaben

die Buchstaben L und O.Andere Buchstaben dagegen wie J oder Y kamen nur selten vor.Man verfertigte also eine Statistik der Buchstabenfrequenzen und bemühte sich dann,die Zykeln so einander zuzuordnen,um eine möglist gute Übereinstimmung mit der Statistik zu erzielen.Die Buchstabenfrequenzen schwankten übrigens im Laufe der Zeit,so dass ab und zu die Statistik verändert werden musste.Auch waren die Buchstabenfrequenzen andere im Heer und andere in der Luftwaffe.Im Sicherheitsdienst wurden die Schlüssel so sorgfältig gewählt,dass sämtliche Buchstaben mit derselben Frequenz auftraten und die statistische Methode also nicht angewandt werden konnte.

12.Methode ungleicher Buchstaben.

Nach dem Verbot,drei gleiche Buchstaben als Schlüssel zu wählen,vermieden die Schlüssler aufs sorgfältigste selbst solche Schlüssel,in denen auch nur zwei gleiche Buchstaben auftraten, wie AAB,oder FVF.Dieses Merkmal war das beständigste von allen und hat sich bis zum heutigen Tage erhalten.Die auf diesem Merkmal aufgebaute Methode hatte den Vorteil,dass man oft ganz mechanisch vorgehen konnte.

Nehmen wir etwa an,am gegebenen Tage hätten wir Zykeln von folgender Gestalt:

(SAIZELWDPBOHU)(YCRKXPJQNGVMT)
(AZHNUGWMSPLR)(QBYKPDZVJIOT)(C)(X)
(AZCSYBVMFJPDO)(NUGTIRHQKXEWL)

Wir haben dann nebenstehende Figur und zwei analoge Figuren aufzuzeichnen und hierauf in den leeren Rechtecken diejenigen Zuordnungen von Zykeln zu streichen, die die Gleichheit zweier Buchstaben nach sich ziehen würden. Wenn man über eine genügende Anzahl von Sprüchen verfügt, wird schliesslich nur ein Fall übrig bleiben.

S	TYCRKXFJQNGVM
A	MTYCRKXFJQNGV
I	VMTYCRKXFJQNG
Z	GVMTYCRKXFJQN
E	NGVMTYCRKXFJQ
L	QNGVMTYCRKXFJ
W	JQNGVMTYCRKXF
D	FJQNGVMTYCRKX
P	XFJQNGVMTYCRK
B	KXFJQNGVMTYCR
O	RKXFJQNGVMTYC
H	CRKXFJQNGVMTY
U	YCRKXFJQNGVMT

AZHNUGWMSFLR	
TOIJVEDPKYBQ	
QTOIJVEDPKYB	
BQTOIJVEDPKY	
YBQTOIJVEDPK	
KYBQTOIJVEDP	
PKYBQTOIJVED	
DPKYBQTOIJVE	
EDPKYBQTOIJV	
VEDPKYBQTOIJ	
JVEDPKYBQTOI	
IJVEDPKYBQTO	
OIJVEDPKYBQT	
	C
–	X

13. Bestimmung der rechten Walze.

Nachdem man so in den meisten Fällen in der Lage war, die Spruchschlüssel wiederherzustellen, trat man jetzt zur Auffindung der Tagesschlüssel, d.h. Walzenlage, Steckerverbindung, Ringstellung, Grundstellung. Man begann mit der Bestimmung der Walzenlage.

Wenn man zwei beliebige deutsche Sätze, jeder hundert Buchstaben lang, untereinander schreibt, so werden durchschnittlich in 8 Kolonnen je zwei gleiche Buchstaben auftreten. Diese Eigenschaft bleibt auch dann bestehen, wenn man beide Sätze nach einem und

demselben Verfahren verschlüsselt.Nimmt man dagegen zwei sinnlose Texte zu je 100 Buchstaben,in denen sämtliche Buchstaben mit etwa derselben Frequenz auftreten und schreibt sie untereinander,so wird man im Durchschnitt nur 4 Kolonnen mit je zwei gleichen Buchstaben antreffen.Diese Eigenschaft benutzt man,um die rechte Walze zu bestimmen.Wenn man nämlich über genügendes Spruchmaterial verfügt,so wird man eine Anzahl Paare von Sprüchen finden,derart,dass in jedem Paar die ersten sowie die zweiten Buchstaben der Schlüssel einander gleich,die dritten Buchstaben dagegen voneinander verschieden sind.Man schreibt nun die beiden Sprüche eines Paares so untereinander,dass Buchstaben,die bei der gleichen Position der Walzen geschlüsselt wurden,senkrecht untereinander zu stehen kommen.A priori sind jedoch zwei Fälle möglich,je nachdem,wann die Drehung der mittleren Walze erfolgt.Man zählt also nach ,wieviel Kolonnen mit gleichen Buchstaben in beiden Fällen vorkommen und muss im richtigen Falle,im Allgemeinen wenigstens,etwa zweimal soviel Kolonnen erhalten als im falschen Fall.Man erfährt hierdurch,in welchem Intervall die mittlere Walze sich dreht,und,wenn man so mit sämtlichen Paaren verfährt,wird man fast stets das Intervall so einengen können, dass hierdurch die rechte Walze,die ja die Drehung der mittleren Walze bewirkt,eindeutig bestimmt wird.Die übrigen Walzen bestimmt man später auf andere Weise.

14.Der Rest.

Die nächste Arbeitsphase bestand in der Auffindung der Steckerverbindung.Es war dies ein ziemlich schwieriges Problem,doch schliesslich ersann man eine Methode,die davon ausging,dass erstens während des Schlüsselns des Spruchschlüssels eine Drehung der mittleren Walze nur etwa einmal in 5 Fällen eintritt, und dass zweitens die Steckerverbindung eine Anzahl Buchstaben unverändert lässt.

Zur Veranschaulichung der Methode stellen wir uns zunächst einmal vor,die Steckerverbindung sei nicht vorhanden.Dann kann man die sechs Gleichungen für die Substitutionen A_1 bis A_6 auf folgende Gestalt bringen:

$$\begin{aligned}
&Q^{x} C_\gamma Q^{-x} E^{-1} A_1 E\, Q^{x} C_\gamma Q^{-x} = P \\
&Q^{x+1} C_\gamma Q^{-x-1} E^{-1} A_2 E\, Q^{x+1} C_\gamma Q^{-x-1} = P \\
&\vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \\
&Q^{x+5} C_\gamma Q^{-x-5} E^{-1} A_6 E\, Q^{x+5} C_\gamma Q^{-x-5} = P
\end{aligned}$$

In diesen Gleichungen ist alles bekannt mit Ausnahme von $P = C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1}$ und des Exponenten x.Denn wenn wir auch dank der vorgehenden Methode wissen,welche Walze sich auf der rechten Seite befindet,so wissen wir doch nicht,welches ihre Position ist.

Wir verfahren also auf die Weise,dass wir für x der Reihe nach die Werte von 0 bis 25 einsetzen und jedesmal P aus jeder der sechs Gleichungen errechnen.Die sechs Substitutionen P werden

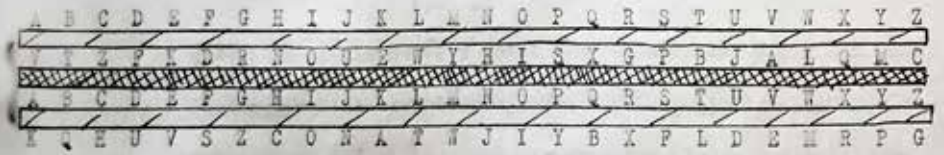
jedesmal untereinander verschieden sein mit Ausnahme eines einzigen Falles,wo sie sämtlich denselben Wert annehmen.Auf diese Weise erhalten wir x,d.h.die Position der rechten Walze und zugleich auch die Substitution F,die wir noch später benötigen werden.

In der Praxis geht man in der Weise vor,dass man auf einem Bogen Papier der Reihe nach die zweiten Zeilen der Substitutionen $C_y, C_y^2, \ldots C_y^{25}$ folgendermassen aufschreibt:(die ersten Zeilen der Substitutionen würden stets lauten 1 2 3 4...26)

7 19 3 15 23 11 20 4 16 26 10 14 22 2 17 6 25 9 1 21 12 18 5 24 13 8
18 2 14 22 10 19 3 15 25 9 13 21 1 16 5 24 8 26 20 11 17 4 23 12 7 6
1 13 21 9 18 2 14 24 8 12 20 26 15 4 23 7 25 19 10 16 3 22 11 6 5 17
: :

(das Beispiel ist willkürlich).

Hierauf schreibt man auf einem zweiten Bogen mit Öffnungen (daher der Name Rost) die 6 Substitutionen A_1 bis A_6 in folgender Form auf:



: :

Nach diesen Vorbereitungen legt man den Rost auf den ersten Bogen und verschiebt ihn so lange von oben nach unten,bis in einer bestimmten Lage die in den Öffnungen erscheinenden Substitutionen F sämtlich identisch sind.Das trifft natürlich nur dann

ein,wenn keine Steckerverbindungen vorhanden sind.Im entgegengesetzten Fall ändert sich das Bild,da jedoch die Steckerverbindungen nicht sämtliche Buchstaben vertauschen,wird man in einer bestimmten Lage gewisse Analogien zwischen den 6 verschiedenen Substitutionen F bemerken.Man muss nun versuchen,die Buchstaben der Substitutionen A_1 bis A_6 so umzustellen,dass alle F identisch werden.Gelingt dies,so ergeben die Umstellungen der Buchstaben die gesuchten Steckerverbindungen,und zugleich erhält man die Position der rechten Walze sowie die Substitution F.

15.Der Katalog F.

Nachdem so die rechte Walze und ihre Position bereits bekannt war,hätte man die linke und mittlere Walze und ihre Positionen einfach so bestimmen können,dass man direkt auf der Maschine sämtlichen möglichen Fälle probierte.Um sich jedoch täglich dieselbe unnütze Arbeit zu ersparen,verfertigte man ein- für allemal einen Katalog,der sämtlichen möglichen Substitutionen F,deren es

$$6.26.26 = 4056$$

gibt,enthielt.Es genügte jetzt die Substitution F,die man beim Suchen der Steckerverbindung erhalten hatte,im Kataloge nachzuschlagen,um sofort Lage und Stellung der linken und mittleren Walze zu erfahren.

16.Der Zyklometer.

Die Methode,die man anwandte,um die Steckerverbindungen zu finden,war nicht nur lang und umständlich,sondern sie führte auch nicht immer zum Ergebnis.Übrigens setzte sie die Kenntnis der Spruchschlüssel voraus,und die Methoden,diese Schlüssel zu finden,waren ebenfalls zeitraubend und nicht immer vom Erfolg gekrönt.So sah man sich denn nach anderen Methoden um,die schneller und sicherer zum Ziele führen könnten.Man verfiel darauf, dass die Gestalt der Zykeln erstens invariant gegenüber den durch die Steckerverbindungen verursachten Substitutionen sei,und zweitens ein Charakteristikum des betreffendenTages bildete,in dem Sinne nämlich,dass zwei Tage,deren Zykeln die gleiche Gestalt hätten,verhältnismässig selten vorkommen konnten.So kam man denn auf den Gedanken,die Zykeln in sämtlichen möglichen Positionen der Walzen,deren es bei drei Walzen,wie bereits gesagt,

105456

gab,zu katalogisieren.Um diese Arbeit zu bewältigen,baute man eine besondere Maschine,den Zyklometer,der aus zwei Enigmen bestand,die so gekoppelt waren,dass in jeder Position eine grössere oder kleinere Anzahl von Glühlampen gleichzeitig aufleuchtete, je nach der Länge des entsprechenden Zyklus.Mehr als ein Jahr verging,ehe die Arbeit beendet war,dann aber fand man in der Regel schon nach wenigen Minuten Walzenlage,Position der Walzen und Steckerverbindungen des betreffenden Tages.

17.Grundstellung und Ringstellung.

Unter Position der Walzen verstehen wir stets die Differenz zwischen Grund- und Ringstellung.Um also in den völligen Besitz der Tagesschlüssel zu gelangen,mussten noch die beiden letzten Elemente des Tagesschlüssels,d.h. Grund- und Ringstellung,gesondert gefunden werden.Dazu genügt es offenbar nicht,sich auf das Studium der Spruchschlüssel zu beschränken,vielmehr muss auf den Inhalt der Sprüche zurückgegriffen werden.

Als man das Materiel von Oktober und Dezember 1931,für das Schlüssel vorhanden waren,löste,bemerkte man,das der Text sehr vieler Sprüche mit den BuchstabenAN begann.

Um also Grund- und Ringstellung gesondert zu erhalten,nahm man irgendeinen Spruch,von dem man vermutete,dass er mit den Buchstaben AN begann und probierte in sämtlichen Positionen der Maschine,ob diese Annahme möglich ist.Eine langwierige Arbeit,wenn man bedenkt,dass dabei $26^3 = 17576$ Positionen untersucht werden müssen.

Später überzeugte man sich,dass,wenn ein Spruch mit den Buchstaben AN begann,a priori gewisse Positionen der rechten Walze unmöglich waren.Und da man täglich über eine ganze Anzahl von Sprüchen verfügte,in denen man ein AN am Anfang erhoffen durfte, so gelang es meistens rein rechnerisch die richtige Position der rechten Walze zu erhalten.

18.Einige Bemerkungen.

Bei der Beschreibung des Rostes und des Zyklometers wurde vorausgesetzt,dass während des Schlüsselns des Spruchschlüssels die mittlere Walze sich nicht drehte.In Wirklichkeit ist diese Voraussetzung nicht unbedingt erforderlich,ja die Auffindung von Grund- und Ringstellung ist sogar besonders leicht gerade dann, wenn eine Drehung der mittleren Walze eintritt.Wir überlassen es dem Leser zu ermitteln,wie sich in solchen Fällen die Verhältnisse gestalten.

Man hat bemerkt, dass innerhalb eines Tages, ~~dass~~ die sechs die Grund und Ringstellung bildenden Zahlen bezw.Buchstaben stets voneinander verschieden waren.Diese Feststellung führte nicht nur in gewissen Fällen zu bedeutender Vereinfachung der Arbeit,sondern sie erlaubte es auch in späteren Jahren die Methode Herivel,von der noch die Rede sein wird,zweckmässig anzuwenden.Es gab übrigens auch Zeiträume,wo sogar stets in vier aufeinander folgenden Tagen alle 24,die Grund- und Ringstellungen bildenden Zahlen bezw.Buchstaben voneinander verschieden waren.

Ähnliche Entdeckungen hat man zu verschiedenen Zeiten auch mit den Steckerverbindungen gemacht.

19.Neue Netze.Beständige Änderungen.

Im Masse wie sich die deutsche Wehrmacht entwickelte,wurde auch die Zahl der Heeresfunkstellen immer mehr vergrössert.Dabei wurde allmählich ebenfalls die Zahl der Funknetze,die sich alle derselben Enigma,jedoch mit anderen Tagesschlüsseln bedienten,vermehrt.So bildete z.B.die neugegründete deutsche Luftflotte mit dem 1.August 1935 ihr eigenes Funknetz mit eigenen Tagesschlüsseln.

Um die Unauflösbarkeit des Enigmaverfahrens sicherzustellen, wurden verschiedene Neuerungen eingeführt.Ab 1.Februar 1936 wurde die Walzenlage monatlich,und ab 1.Oktober 1936 sogar täglich geändert.Gleichzeitig wurde die Zahl der Steckerverbindungen geändert,sie betrug nicht mehr 6,wie bisher,sondern 5 bis 8.Und schliesslich wurde noch am 2.November 1937 die bisherige Umkehrwalze aus dem Verkehr genommen und durch eine neue,die sogenannte Umkehrwalze B,ersetzt.

20.Umkehrwalze B.

Von Seiten der deutschen Schlüsselrx wurde die Unvorsichtigkeit begangen,in den Funksprüchen vom September 1937 von der bevorstehenden Änderung der Umkehrwalze zu reden.So war man denn in der polnischen Schlüsselstelle auf die Änderung vorbereitet und wunderte sich nicht,als die Gestalt der Zykeln vom 2.November 1937 im Kataloge nicht aufzufinden war.Dagegen konnte man

natürlich nach wie vor mit Hilfe des Rostes die Steckerverbindungen sowie die rechte Walze und ihre Position bestimmen.

Unbekannt blieben nur die linke und mittlere Walze sowie ihre Positionen.Das ergab 2.26.26 = 1352 mögliche Fälle und jeder dieser Fälle bestimmte eine Umkehrwalze.

Durch Vergleich dieser 1352 Umkehrwalzen in zwei verschiedenen Tagen konnte leicht die richtige Umkehrwalze ermittelt werden.

21.Neue Chiffrierwalzen.

Im September 1937 bildete sich ein neues Funknetz,nämlich das Funknetz des Sicherheitsdienstes,einer politischen Organisation, von der noch später die Rede sein wird.Das Schlüsselverfahren war in diesem Netze im Grossen und Ganzen dasselbe ,wie in der Armee, jedoch wurden gewisse Neuerungen nicht gleichzeitig,sondern mit einer bestimmten Verspätung eingeführt.So z.B.wurde am 15.September 1938 das Schlüsselverfahren im Heere und in der Luftwaffe vollständig umgestaltet,dagegen blieb es im Sicherheitsdienst noch mehrere Monate lang unverändert,ein grosser Fehler,der sich sofort rächen sollte.Denn bereits drei Monate später wurden,diesmal gleichzeitig in allen Netzen,zwei neue Chiffrierwalzen,die Walzen IV und V eingeführt.Da in diesem Augenblicke das Netz des Sicherheitsdienstes sich noch des alten Verfahrens bediente,konnten die Schaltungen dieser Walzen in ähnlicher Weise gefunden werden,wie die Schaltungen der Umkehrwalze B.Es erübrigt sich

wohl,in Einzelheiten einzugehen,es möge nur angedeutet werden, dass man sich hierbei zweier Tage,in denen eine Drehung der mittleren Walze eintrat,bediente.Wäre im Sicherheitsdienst das neue Chiffrierverfahren früher eingeführt worden,so hätte man wohl kaum die Schaltungen der Walzen IV und V auf kryptologischem Wege erhalten.

22.Änderung des Chiffriersystems.

Dank den beschriebenen Methoden konnten bis September 1938 tagtäglich sämtliche Netze d.h.Heer,Luftwaffe,Sicherheitsdienst, Marine (von der noch weiter unten die Rede sein wird) in oft unglaublich kurzer Zeit gelöst werden.

Die Sachlage änderte sich jedoch vollkommen,als am 15.September 1938 ein neues Chieffrierverfahren eingeführt wurde und hierdurch die bisherigen Errungenschaften polnischer Kryptologen auf diesem Gebiete ernsthaft bedroht wurden.

Das neue Schlüsselverfahren beruhte darauf,dass die Grundstellung nicht mehr eine und dieselbe war für sämtliche Sprüche eines Tages,sondern vom Spruch zu Spruch wechselte.

Wir wollen das neue Schlüsselverfahren an einem Beispiele erläutern.Der Schlüssler wählt sich zwei Buchstabentripel,z.B. SKR WTC,stellt die Maschine auf SKR ein und schlüsselt die Buchstaben WTC zweimal hintereinander (wie bisher),wobei er etwa die sechs Buchstaben KFDLSF erhalten möge.

Die Grundstellung SKR wird unverschlüsselt in dem Kopf des Spruches, die sechs Buchstaben KFD LSF am Anfang des Spruches eingesetzt, und der Spruch selbst wird von der Stellung WTC aus verschlüsselt (also so wie bisher). Dass das neue Verfahren gerade so, wie beschrieben, und nicht anders war, erfuhr man dadurch, dass bereits am Vortage der Systemänderung einige Schlüssler sich des neuen Verfahrens bedienten, was natürlich wieder ein grober Fehler war.

23. Auffindung der Walzenlage.

Da bei dem neuen System die Spruchschlüssel nicht mehr von ein- und derselben Position aus verschlüsselt werden, so wurde die Zykelntheorie und die darauf aufgebauten Methoden der Spruchschlüssel, des Rostes und des Zyklometers hinfällig.

Man liess jedoch die Arme nicht hängen, sondern schritt zur Untersuchung des neuen Verfahrens. Als erstes stellte man fest, dass wenn das Spruchmaterial innerhalb eines Tages und eines Netzes genügend umfangreich war, man von Zeit zu Zeit auf Paare von Grundstellungen traf, deren erste und zweite Buchstabe identisch, und deren dritte Buchstaben im Alphabet nebeneinander oder fast nebeneinander standen, wie etwa TKP und TKR. Wenn dann zufälligerweise auch in den Spruchschlüsseln gleiche Buchstaben an entsprechenden Stellen auftraten, so konnte man hieraus bisweilen schlussfolgern, welche Walzen sich recht oder in der Mitte befinden. Wir

wollen die verschiedenen Möglichkeiten an einigen Beispielen klarmachen.

1) Angenommen, wir hätten zwei Sprüche mit folgenden Schlüsseln gefunden:

Grundstellung	Spruchschlüssel
TKP	ANV CKS
TKR	VTS JLM

In diesem Fall ist sicher, dass zwischen den Buchstaben P und R eine Drehung der mittleren Walze stattfindet, d.h., dass ~~xxxxx~~ rechts sich die Walze I befindet, da diese und nur diese eine Drehung zwischen Q und R hervorruft. Im entgegensetzten Falle würden den gleichen Buchstaben V auch gleiche Buchstaben B (oder J) entsprechen.

2)

Grundstellung	Spruchschlüssel
TKP	ANV CKS
TKR	VTS BLM

In diesem Falle ist es wenig wahrscheinlich, dass eine Drehung zwischen P und R eintritt, dass also rechts sich die Walze I befindet.

3) Auch Grundstellungen mit verschiedenen <u>mittleren</u> Buchstaben können Aufschlüsse über die Walzenlage bieten, wie folgendes Beispiel zeigt:

Grundstellung	Spruchstellung
TKP	ANV CKS
TLR	VTS JLM

Zwischen P und R kann keine Verschiebung der mittleren Walze

eintreten,also ist die rechte Walze sicher verschieden von der Walze I.

4) Ja sogar aus Grundstellungen mit verschiedenen ersten Buchstaben lassen sich bisweilen Schlüsse über die Walzenlage ziehen.

Grundstellung	Spruchschlüssel
TJG	CMS GER
UKG	CWT GLJ

In diesem Falle ist es wahrscheinlich,dass zwischen J und K sich die linke Walze gedreht hat,dass also in der Mitte sich die Walze IV befindet.

In anderen Fällen lassen sich ähnliche Schlüsse ziehen.

24.Bomben.

Bereits wenige Tage nach Einführung des neuen Schlüsselverfahrens hatte man einen Plan gefasst,wie man die entstandenen Schwierigkeiten aus dem Wege schaffen könnte.Unser Ideengang war folgender:

Nehmen wir eine Anzahl von Sprüchen und schreiben deren Grundstellungen und Spruchschlüssel auf.

1.KTL WOC DRB	7.GRA FDR YWD
2.SVW KKM IYS	8.MDO OIW YZW
3.JOT IWA BAN	9.KJC FSW RSZ
4.EDC DSP LJC	10.SGF TEY ASR
5.GKD QAV GHA	11.AGH EDF RHF
6.BWK TCA TOC	12.JBR WLT SOQ

Richten wir jetzt unsere Aufmerksamkeit auf den Spruch Nr3. In dessen Spruchschlüssel kommt der Buchstabe W zweimal im Abstande von 3 Buchstaben vor.Das bedeutet,dass in einer ganz bestimmten Position der Maschine der Buchstabe W einen uns unbekannten Buchstaben,sagen wir etwa X,ergeben und drei Positionen später derselbe Buchstabe W wieder denselben Buchstaben X ergeben würde.Nehmen wir nun noch an,der Buchstabe W werde durch die Steckerverbindung nicht berührt,eine Annahme,die bei 5 bis 8 Steckerverbindungen in 50% aller Fälle zutreffend ist.

Dann konnte man die richtige Position der Walzen dadurch ermitteln,dass in zwei Maschinen,deren Positionen sich um 3 unterscheiden,der Buchstabe W gleichzeitig getastet und daraufhin in beiden Maschinen die Walzen synchronisch gedreht werden.Jedesmal, wenn in beiden Maschinen gleichzeitig derselbe Buchstabe aufleuchtet,haben wir es mit einem Fall zu tun,der möglicherweise richtig ist und daher besonders untersucht werden muss.

Da jedoch solche Fälle allzu häufig auftreten würden,hilft man sich in der Weise,dass man nicht einen,sondern drei Sprüche,in deren Spruchschlüsseln der Buchstabe W zweimal im Abstande von 3 Buchstaben vorkommt,benutzt.In unserem Beispiel wären es die Sprüche Nr 3,5,und 8.Nur muss man sich natürlich nicht zweier, sondern sechs Maschinen bedienen.Es wäre aber in Wirklichkeit höchst umständlich und unzweckmässig,wollte man wirklich mit

sechs einzelnen Maschinen manipulieren. Vielmehr ersann man eine Maschine, Bombe genannt, die 6 Enigmen entsprach, elektrisch angetrieben wurde und jedesmal automatisch anhielt, wenn ein günstiger Fall vorlag. Es wurden in der polnischen Schlüsselstelle sechs solche Bomben montiert, für jede Walzenlage eine (denn die Walzen IV und V wurden erst später eingeführt), wobei jede Bombe alle möglichen 17576 Fälle in 1½ Stunden bewältigte.

25. Die Netze.

Die Bomben befanden sich noch im Bau, als bereits neue Änderungen eintraten. Am 15. Dezember 1938 wurden die Walzen IV und V eingeführt, die Anzahl der möglichen Walzenlagen also verzehnfacht, und zwei Wochen später die Zahl der Steckerverbindungen auf 7 - 10 erhöht. Durch diese Änderungen verloren die Bomben praktisch den grössten Teil ihrer Bedeutung, da die Lösung eines Tages zu viel Zeit beanspruchen würde. Es gelang zwar bisweilen, dank der früher angegebenen Methode die Walzenlage teilweise zu bestimmen, aber nur dann, wenn umfangreiches Material vorhanden war, was verhältnismässig selten eintrat. Auch war die Anwendbarkeit der Bomben durch die Steckerverbindungen eingeschränkt.

Man schuf daher bereits sehr früh eine neue Methode, die von der Zahl der Steckerverbindungen unabhängig war.

Zur Darlegung dieser neuen Methode müssen wir zunächst einen

neuen Begriff, den der männlichen und weiblichen Positionen, einführen. Kehren wir noch einmal zu den auf Seite 35 angegebenen Sprüchen zurück:

1.KTL WOC DRB	7.GRA PDR YWD
2.SVW XKA IYS	8.MLO OTG YUC
3.JOT IXA BQN	9.KJC PCW RQL
4.EDC DSP LJC	10.SGF TEY ASR
5.GKD WAV GHA	11.AGR MDP RHP
6.BWK ZCA TOC	12.JBR NLT SOX

Ein Fall wie im Spruchschlüssel Nr.3, dass derselbe Buchstabe (in unserem Beispiel S) zweimal im Abstand von drei Buchstaben vorkommt, kann nicht in sämtlichen Positionen der Maschine eintreten. Vielmehr haben Rechnungen ergeben, dass solche Fälle in etwa 40% aller Positionen eintreten (genau genommen beträgt das Verhältnis $1-\frac{1}{\sqrt{e}}$, wobei e die Basis der natürlichen Logarithmen ist). Diese Positionen nennen wir weibliche Positionen, die übrigen heissen männliche Positionen. In unserem Beispiel gehören die sechs Sprüche Nr. 3,5,6,8,9,11 bestimmt weiblichen Positionen an, während von den übrigen Sprüchen nichts ausgesagt werden kann. Die Steckerverbindungen haben natürlich Einfluss auf die in den Spruchschlüsseln auftretenden Buchstaben, nicht aber auf das Geschlecht der Position (ob weiblich oder männlich).

Man könnte daher einen Katalog mit sämtlichen weiblichen Positionen anfertigen, und in diesem Kataloge nachsuchen, ob man nicht sechs weibliche Positionen findet, die in denselben Abständen auftreten, wie die Grundstellungen: JOU, GKD, BWK, MDR, KJD, AGK; (dabei müssen auch eventuell Drehungen der mittleren wie auch der linken Walze berücksichtigt werden.)

Da dies jedoch praktisch unausführbar wäre, so ging man anders vor; man stellte die sogenannten Netze her: Für jede Walzenlage werden sämtliche weiblichen Positionen auf 26 Bogen Papier, von denen jeder 26×26 Felder, und zwar in vierfacher Ausführung enthält, eingetragen. Die verschiedenen Bogen entsprechen den 26 Positionen der linken Chiffrierwalze, die 26×26 Felder der mittleren und rechten Walze. Der Grund der vierfachen Ausführung wird unten erklärt werden. Die Felder die den weiblichen Positionen entsprechen, werden durchlocht. (Daher der Name Netz.)

Nun werden, um auf unseres Beispiel zurückzugehen, sechs von den 26 Bogen in einer Reihenfolge und in einer Lage, die den gegenseitigen Entfernungen der Grundstellungen entspricht, aufeinander gelegt. Wenn gleichzeitig in allen sechs Bogen an derselben Stelle ein Loch erscheint, so haben wir es mit einem möglicherweise richtigen Falle zu tun, der besonders geprüft werden muss. Um alle möglichen Fälle zu erschöpfen, müssen die Bogen der Reihe nach zyklisch vertauscht werden. Auf jedem Bogen befinden sich die 26×26 Felder in vierfacher Ausführung, weil die Bogen nicht direkt, sonder gegenseitig verschoben aufeinander gelegt werden. Die Erzielung des Ergebnisses ist von einem überaus sorgfältigen Aufeinanderlegen der Bogen in der richtigen Lage abhängig. Deshalb wurde stets vor Beginn der Arbeit auf einem besonderen Zettel, dem sogenannten Menu, die Reihenfolge und gegenseitige Lage der Bogen festgelegt.

Die Kenntnis, welche Position weiblich und welche männlich sind, wurde den Katalogen zum Zyklometer entnommen, denn offenbar entsprechen weibliche Positionen denjenigen Substitutionen, in denen Zykeln vorkommen, die aus einem Buchstaben bestehen.

Das Prüfen der richtigen Fälle geschah auch mit Hilfe des Zyklometers. Da dies ziemlich zeitraubend war, trug man sich mit dem Gedanken, besondere Kataloge herzustellen, in denen nicht nur die weibliche Positionen, sondern auch alle Buchstaben, die in den eingliedrigen Zykeln vorkommen, eingetragen wären. Aber dieser Gedanke wurde erst später, und zwar von der englischen Schlüsselstelle, ver-wirklicht.

26.Die Warschauer Konferenz.

In der polnischen Schlüsselstelle wurden zwei Sätze von je 26 Netzen für zwei Walzenlagen mit der Hand angefertigt,und man überzeugte sich,dass die Idee der Netze vollkommen brauchbar war. Ganz anders jedoch stellte sich die Ausführung dieser Idee dar.

Während die weiblichen Positionen für die Walzenlagen I II III, I III II,... III II I direkt den Katalogen entnommen werden konnten, müsste man für die übrigen 54 Walzenlagen die weiblichen Positionen erst ermitteln,entweder mittels des Zyklometers,was mehrere Jahre beansprucht hätte,oder mit Hilfe einer neuen kostspieligen Maschine,woran man zunächst noch nicht denken xxxxte wollte.Ferner war das handmässige Perforieren bereits der beiden ersten Sätze von je 26 Netzen recht mühsam gewesen,so dass man für den Rest der Arbeit ebenfalls besondere Apparate benötigt haben würde.Und schliesslich würde ,wenn schon alles fertig wäre,das Manipulieren mit den 60 Sätzen von Netzen,um die einzelnen Tage zu lösen,ein zahlreiches Hilfspersonal erfordern.

Da die polnische Schlüsselstelle nicht in der Lage war,all diese Schwierigkeiten selbst zu bewältigen,entschloss man sich,das Geheimnis der Enigma,das bisher sorgsam gehütet war,auch der französischen und englischen Schlüsselstelle anzuvertrauen.

Am 26.Juli 1939 trat in Warschau eine dreitägige Konferenz unter Teilnahme von Vertretern der französischen und englischen Schlüsselstelle in Sachen der Enigma zusammen.Es stellte sich heraus,dass weder unsere französischen noch englischen Fachgenossen die ersten Schwierigkeiten haben überwinden können.Die Walzenschaltungen waren ihnen unbekannt,mithin auch etwaige Auflösungsmethoden.Wir legten ihnen die Ergebnisse unserer siebenjährigen Arbeiten,sowie die Schwierigkeiten,auf die wir zuletzt gestossen waren, vor.Von Seiten der Engländer wurde bereitwilligst Hilfe in der Ausführung der Netze für die 60 Walzenlagen versprochen.

27.Kriegsausbruch.Vignolles.

Einen Monat später brach der deutsch-polnische Krieg aus. Es gelang noch,den 25.August 1939,den Tag der allgemeinen Mobilmachung in Deutschland,zu lösen,als bereits die Evakuation begann. Die Bomben,Zyklometer,Enigmen,Netze,sämtliche Akten und Aufzeichnungen wurden mitgenommen,aber auf dem Wege zur rumänischen Grenze vernichtet.Einzig und allein zwei Enigmen wurden gerettet.In Bukarest nahm sich der drei Spezialisten von der Enigma die französische Botschaft an und schickte sie sofort nach Paris,wo sie gastfreundschaftlich aufgenommen wurden.Wenige Wochen später schuf der französische Generalstab in Vignolles,einem Schlösschen unweit Gretz,20 km. von der Hauptstadt entfernt,ein Büro,wo polnische Kryptologen samt Hilfspersonal unter Leitung von Oberstleutnant Langer versuchten,die in Polen unterbrochene Arbeit wiederaufzunehmen.Man begann wieder mühselig,wie bereits schon einmal in Warschau,die Netze mit der Hand zu fabrizieren,eine Arbeit,die wohl erst nach Jahren beendet worden wäre.

Jetzt aber begann die Warschauer Konferenz Früchte zu tragen.Es stellte sich heraus,dass in der Zwischenzeit die Engländer eine Maschine konstruiert hatten,die ihnen ermöglichte,die Netze für sämtliche 60 Walzenlagen in wenigen Wochen herzustellen.Aber Proben, die mit diesen Netzen in England angestellt wurden,ergaben kein Ergebnis.Da glücklicherweise die Netze in zwei Exemplaren hergestellt waren,konnten uns die Engländer ein Exemplar zur Verfügung stellen, was sie auch freundlichst taten.Sobald diese Netze in Vignolles ankamen,begann eine angestrengte Arbeit,und bald waren zwei Tage,der 28.10.1939 und der 6.1.1940 gelöst.Die Schlüssel wurden sofort nach England übersandt,und es wurde klar,dass von nun ab alles Material, wie in früheren Zeiten,gelöst werden würde.

Die Engländer haben ihre Arbeit glänzend organisiert.Sie verfügten über umfangreiches Spruchmaterial und zahlreiches Personal.Die Mehrzahl der gelösten Tage stammte von ihnen.

Auch in Vignolles wurde fieberhaft gearbeitet.Da es aber darauf ankam, möglichst viel Spruchmaterial zu lösen und zu lesen,um es im Generalstab auszuwerten,so sassen denn die polnischen Kryptologen tagaus tagein an den Enigmen und tasteten die Sprüche ab oder manipulierten mit den Netzen,um von Zeit zu Zeit auch einen Tag zu lösen und sich nicht ganz von den Engländern distanzieren zu lassen. Alles mechanische Arbeiten,wozu sicherlich Spezialisten nicht nötig waren.So ist es denn nicht zu verwundern,dass von polnischen Kryptologen keine [redacted] Ergebnisse mehr erzielt wurden,sondern, dass der Schwerpunkt kryptologischer Untersuchungen sich nach London übertrug.

28.Methode Knox.

Der englische Kryptolog Knox hatte bemerkt,dass die deutschen Schlüssler oft als Grundstellung diejenigen Buchstaben wählten, die nach Beendigung des Schlüsselns des vorgehenden Spruches in den Fenstern der Maschine erscheinen.Besonders häufig trat dies in vielteiligen Sprüchen auf.Es genügte also in solchen Fällen von der Grundstellung die Länge des vorhergehenden Spruches zu subtrahieren,um den Spruchschlüssel des vorhergehenden Spruches (unverschlüsselt) zu erhalten.Erhielt man dabei charakteristische Schlüssel wie ASD,WER,OKL,...in mehreren Teilen eines vielteiligen Spruches, so war man sicher,dass der Schlüssler einen solchen Fehler begannen hat.Da bei der Substraktion der Spruchlänge von der Grundstellung eventuelle Drehungen der mittleren und linken Walzen berücksichtigt werden müssen,so konnte man auf diese Weise teilweise die Walzenlage bestimmen und dadurch im glücklichen Falle die Arbeit des Auflösens von 60 auf 3 Walzenlagen herabsetzen.Richtig war auch,dass mit Hilfe der Methode Knox die (unverschlüsselten) Spruchschlüssel einiger Sprüche bekannt waren.

Diese Methode hatte besonders während des norwegischen Feldzuges wertvolle Dienste geleistet,wo Tag auf Tag gelösst wurde,wobei sich überaus wichtiges und interessantes Material ergab.

29.Kataloge zu den Netzen.

Inzwischen verwirklichten die Engländer noch eine Idee polnischer Kryptologen.Es wurde bereits erwähnt,dass das Verifizieren der mittels der Netze erhaltenen möglichen Fälle mit Hilfe des Zyklometers ziemlich zeitraubend war.Man musste jedesmal,wenn ein günstiger Fall vorlag,die Buchstaben,die den weiblichen Charakter der Positionen bestimmten,mit Hilfe des Zyklometers aufsuchen,und mit den Buchstaben der betreffenden Spruchschüssel vergleichen.Man trug sich bereits in Polen mit dem Gedanken,Kataloge herzustellen,die die in Frage kommenden Buchstaben sämtlicher weiblicher Positionen enthalten sollten,jedoch technische Schwierigkeiten verhinderten die Ausführung dieser Idee.Jetzt wurde sievon den Engländern mit Hilfe derselben Maschine,die die Netze angefertigt hat,realisiert,ein weiteres glänzendes Beispiel,wie fruchtbar sich die polnisch-französisch-englische Zusammenarbeit erwies.Dank den finanziellen und organisatorischen Möglichkeiten unserer Londoner Fachgenossen wurden unsere Pläne,die sonst wohl nie das Licht der Welt erblickt hätten,ohne Rücksicht auf Kosten und Schwierigkeiten in Wirklichkeit umgesetzt.

30.Methode Herivel.

Ein anderer englischer Kryptolog machte die Entdeckung,dass einige der deutschen Schlüssler,wenn sie nach Mitternacht oder am Morgen die Enigma für den betreffenden Tag einstellten,die Walzen zur Ringeinstellung nicht herausnahmen und nicht drehten,und als Grundstellung für den ersten Spruch des Tages die Buchstaben wählten,die sie in den Fenstern der Maschine erblickten.Infolgedessen unterschied sich die Grundstellung dieses ersten Spruches nicht viel von der für diesen Tag festgesetzten Ringstellung.

Durch Vergleich der Grundstellungen von Sprüchen,die von verschiedenen Schlüsslern nachts oder in der frühen Morgenstunden chiffriert wurden,konnte man oft die Ringstellung genau oder mit grosser Annäherung ausfindig machen.Dank dieser Feststellung wurde die zur Lösung erforderliche Arbeitszeit ganz ausserordentlich abgekürzt, sodass oft am frühen Morgen die Engländer bereits im Besitze des Schlüssels für den ganzen Tag waren.

Zu dieser Methode möge noch folgendes hinzugefügt werden.Als die Schaltungen der Walzen IV und V gefunden wurden,konnte die Lage des Buchstabenringes für diese Walzen nicht eindeutig festgesetzt werden. Es gab je 26 verschiedene Lagen,von denen die ersten besten ausgewählt wurden.Man war sich jedoch darüber im Klaren,dass diese Lagen mit den originalen Lagen in den Walzen nicht identisch waren.Nachdem eine grössere Anzahl von Tagen (vor der Entdeckung Herivels)gelöst war,erinnerte man sich daran,dass früher die drei die Ringstellung bildenden Buchstaben stets voneinander verschieden waren.Wenn dieses Merkmal auch jetzt bestehen sollte (was sehr wahrscheinlich war),so mussten die Lagen der Buchstabenringe in den Walzen IV und V einer gewissen Korrektur unterzogen werden.Diese Korrektur wurde gefunden und den Engländern sofort mitgeteilt.Erst durch diese Korrektur konnte das Verfahren Herivel angewandt werden.

31.Drittes Schlüsselverfahren.

Am 1.Mai 1940, ~~der~~ Beginn der deutschen Offensive gegen Belgien und Holland wurde das Schlüsselverfahren nochmals geändert.Der Spruchschlüssel wurde nicht mehr zweimal,sondern nur einmal verschlüsselt. Im Kopf des Spruches werden jetzt sechs Buchstaben angegeben,die die ersten bedeuten die Grundstellung,die drei folgenden den chiffrierten Spruchschlüssel.

Der Sachverhalt wurde dadurch geklärt,dass die deutschen Schlüs

ler wieder,wie schon einmal ,die Unvorsichtigkeit begingen,bereits am Vorabend der Neueinführung eine Anzahl von Sprüchen nach dem neuen Verfahren zu schlüsseln.Dieser Tag,der 20.April 1940,wurde gelöst, nebenbei bemerkt von polnischen Kryptologen,und so stellte sich denn heraus,worauf das neue Verfahren beruhte.

Es war wieder ein sehr harter Schlag.Die Netze und die Kataloge zu den Netzen wurden völlig unbrauchbar,es blieben nur noch die Methoden Knox und Herivel bestehen.Mit Hilfe dieser Methoden versuchten die polnischen Kryptologen,die vorübergehend von Vignolles nach Paris versetzt waren,wenigstens einen Tag zu lösen,jedoch vergeblich.

Die Engländer hatten mehr Erfolg.Sie verfügten über bedeutend umfangreiches Material,und so gelang es ihnen,nach einer dreiwöchentlichen Pause wieder einen Tag,den 20.Mai 1940,zu lösen,und bald darauf fast sämtliche folgenden Tage.Sie übersandten regelmässig die Schlüssel,und so sassen wieder Tag und Nacht die polnischen Spezialisten an den beiden aus Warschau stammenden Enigmen,um das überaus wertvolle Spruchmaterial lesen zu helfen.Nach der Evakuation von Paris wurde die Arbeit in La Ferté-St.Aubin fortgesetzt,wo ebenfalls Tag und Nacht gearbeitet wurde und erst unmittelbar vor dem Waffenstillstand wurde sie abgebrochen.Der letzte Tag,für den die Engländer die Schlüssel übersandten,war der 16.Juni 1940.

32. Chronologische Übersicht über die Änderungen des Schlüsselverfahrens im Heer und in der Luftwaffe.

15.Jul.1928 – 31.Mai 1930	Enigma G mit Stöpselstellung				
1.Jun.1930 – 31.Jan.1936	Enigma I mit Steckerverbindungen	Walzenlage ändert sich alle drei Monate	Steckerverbindungen tauschen sechs Paar Buchstaben	Umkehrwalze A	Walzen I - III Erstes Schlüsselverfahren. Grundstellung dieselbe für alle Sprüche. Spruchschlüssel zweimal verschlüsselt.
1.Feb.1936 – 30.Sep.1936		Walzenlage ändert sich jeden Monat			
1.Okt.1936 – 1.Nov.1937		Walzenlage ändert sich täglich	Steckerverbindungen tauschen 5-8 Paar Buchstaben		
2.Nov.1937 – 14.Sep.1938				Umkehrwalze B	Walzen I - V Zweites Schlüsselverfahren. Grundstellung wechselt von Spruch zu Spruch. Spruchschlüssel zweimal verschlüsselt.
15.Sep.1938 – 14.Dez.1938			Steckerverbindungen tauschen 7-10 Paar Buchstaben		
15.Dez.1938 – 31.Dez.1939			Steckerverbindungen tauschen zehn Paar Buchstaben		Drittes Schlüsselverfahren. Grundstellung wechselt von Spruch zu Spruch. Spruchschlüssel einmal verschlüsselt.
1.Jan.1940 – 30.Apr.1940					
1.Mai 1940					

33.Das Funknetz des Sicherheitsdienstes.

Das Funknetz des Sicherheitsdienstes wurde bereits auf Seite 31. erwähnt.Da dieses Netz,abgekürzt S.D.genannt,sich eines Schlüsselverfahrens bediente,dass in Einzelheiten von demjenigen des Heeres und der Luftflotte abwich,so möge es hier etwas genauer beschrieben werden.

Bis 1.August 1939 bestand der Hauptunterschied zwischen dem Verfahren S.D.und den übrigen Verfahren darin,dass der Text der Sprüche mit dreistelligen Satzbuchgruppen vermischt war.Das Satzbuch diente anscheinend vor allem dazu,den Inhalt der Sprüche abzukürzen.Es war nicht besonders schwer,dieses Satzbuch zu lösen, doch wurde es alle paar Monate geändert und durch ein umfangreicheres ersetzt,sodass man die Arbeit stets aufs neue beginnen musste.

Der Spruchschlüssel wurde wie im Heer und in der Luftflotte zweimal verschlüsselt,doch wurde er nicht immer am Anfang,sondern bisweilen auch an anderen Stellen eingesetzt.Ausserdem wurden während der Dauer von mehreren Monaten die Buchstaben der Spruchschlüssel noch mittels eines besonderen Tauschalpfabets überschlüsselt.Die Gültigkeit eines Tauschalphabets betrug jeweils einen Monat.

Die Spruchschlüssel wurden sehr sorgfältig gewählt,sodass nur die Methode ungleicher Buchstaben und der Zyklometer angewandt werden konnten.

Sprüche,die mit den Buchstaben AN begannen,kamen nicht vor.Um also Grund- und Ringstellung gesondert zu finden,musste man von anderen charaktristischen Eigenschaften des Spruchinhalts ausgehen. Es stellte sich heraus,dass in sehr vielen Sprüchen der vierte

und fünfte oder der fünfte und sechste Buchstabe QY lautete,und dass man also mit diesen Buchstaben ebenso vorgehen konnte wie im Heer mit den Buchstaben AN.

Ihrem Inhalt nach waren die Sprüche von grosser Wichtigkeit. Es waren sehr oft Berichte von ausserhalb Deutschlands sich befindenden Agenten des Sicherheitsdienstes,und man konnte sich mit ihrer Hilfe ein Bild über die weit verzweigte Organisation des deutschen Spionagedienstes machen.

Das am 15.September 1938 im Heer und in der Luftflotte eingeführte zweite Schlüsselverfahren wurde im S.D.Netz nicht beachtet.Eswurde nach wie vor nach dem alten System geschlüsselt, nur wurde durch Einsetzen in den Kopf der Sprüche einer dreistelligen Buchstabengruppe das neue System vorgetäuscht.Dagegen trat am 1.August 1939 eine völlige Änderung des Verfahrens ein, dass man nicht enträtseln konnte.Seit dieser Zeit blieben die Sprüche des S.D.-Netzes unauflösbar.Der letzte gelöste Tag war der 31. Juli 1939.

Aus Mangel an Unterlagen kann eine chronologische Zusammenstellung der im S.D.-Funknetz eingetretenen Veränderungen der verschiedenen Schlüsselmittel wie Satzbücher,Tauschalphabete, Einsatzstellen für Spruchschlüssel,usw.nicht angegeben werden.

34.Die Schlüsselverfahren der deutschen Kriegsmarine vor Einführung der Enigma.

Die Schlüsselverfahren,die die Deutsche Kriegsmarine anwandte,unterschieden sich,obwohl seit dem Jahre 1924 auch dort dieselbe Enigma wie im Heere benutzt wurde,sehr wesentlich von denen des Heeres und der Luftwaffe.Es wäre daher unzweckmässig gewesen, wollte man die Ergebnisse,die auf diesem Gebiete erzielt wurden, chronologisch zwischen die übrigen Arbeiten einflechten.Sie mögen jetzt am Ende dieser Skizze zusammengestellt werden.

Die im Funkverkehr der deutschen Kriegsmarine vorkommenden Sprüche werden stets verschlüsselt in zwei-,drei- oder vierstelligen Buchstabengruppen angegeben,wobei Teilgruppen (z.B.am Ende der Sprüche) nicht vorkommen.Hauptsächlich wurde der vierstellige Chiffre benutzt und nur dieser wurde in der polnischen Schlüsselstelle bearbeitet.

Die in den Jahren 1921 - 1925 angewandten vierstelligen Chiffres waren stets überschlüsselte Satzbücher.Die erste und letzte Gruppe eines jeden Spruches waren Blind- oder Kenngruppen.Die übrigen Gruppen waren verschlüsselte Codegruppen.Weder die Überschlüsselung noch die Satzbücher konnten gelöst werden.

In den Jahren 1926 - 1927 wurden zwei vierstellige Chiffres angewandt.Einer von ihnen war ein gewöhnliches Satzbuch ohne weitere Überschlüsselung.Dieses Satzbuch wurde im Jahre 1933 gelöst.Die Codegruppen bestanden ausschliesslich aus 18 Buchstaben:

A B E F G I K L N O P S T U W X Y Z.

Das Satzbuch war sehr umfangreich und besass wahrscheinlich über 90 000 Codegruppen,von denen für ungefähr 10 000 die Bedeu-

tungen gefunden werden konnten. */

35.Die Marine-Chiffriermaschine mit 29 Tasten.

In der Zeit vom Januar 1926 bis September 1934 wurde von der deutschen Kriegsmarine eine Chiffriermaschine zum Verschlüsseln von Funksprüchen benutzt.Die Maschine war eine Enigma-Chiffriermaschine,die sich jedoch in folgenden Einzelheiten von der im Heere gebrauchten Enigma-Chiffriermaschine unterschied:

1/.Die Maschine besass 29 Tasten und ebensoviel Glühlampen für die 29 Buchstaben des deutschen Alphabets mit den Umlauten.

2/.Beim Niederdrücken der Taste X leuchtete stets die Glühlampe X auf.

3/.Weder Stöpselstellungen noch Steckerverbindungen waren vorhanden.

4/.Die Schaltung der Eintrittswalze war folgende:

A	Ä	B	C	D	E	F	G	H	I	J	K	L	M	N	O	Ö	P	Q	R	S	T	U	Ü	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	

5/.Die Zahl der Chiffrierwalzen betrug fünf,von denen gleichzeitig drei in die Maschine eingesetzt wurden.

6/.Die Zähne der Chiffrierwalzen waren nicht mit den Ringen,sondern mit der Walzeneinfassung verbunden.

7/.Die Umkehrwalze war beweglich;man konnte sie wie jede Chiffrierwalze einstellen.

---

*/ Der zweite der beiden vierstelligen Chiffres war,wie sich herausstellte,mittels einer Chiffriermaschine verschlüsselt. Er wird auf Seite 52 beschrieben.

6/.Die Ringe besassen Zahlen von 1 - 26.

Obwohl diese Chiffriermaschine schon ab 1926 im Gebrauch war, gelang es sie erst an Hand der Sprüche aus den Jahren 1931 - 1934 zu rekonstruieren.In dieser Zeit wurden die Sprüche auf dieselbe Weise wie im Heere verschlüsselt,das heisst,also,dass für jeden Tag eine Grundstellung festgesetzt wurde,bei welcher der aus 3 Buchstaben bestehende Spruchschlüssel zweimal verschlüsselt wurde.Die so erhaltenen zwei dreistelligen Buchstabengruppen wurden durch Voransetzung je eines blinden Buchstabens in vierstellige Gruppen verwandelt,von denen die erste am Anfang und die zweite am Ende des Spruches eingesetzt wurde.Auf diese beiden Gruppen konnte auf dieselbe Weise wie im Heer die Zykelntheorie angewandt werden.

Das Bilden der Substitutionen A_1A_4 ,A_2A_5 und A_3A_6 war jedoch dadurch erschwert,dass das Spruchmaterial unzureichend war.Um so schwerer war es die Spruchschlüssel selbst zu erhalten.Erst im Jahre 1933 wurde dies erheblich leichter,als sich herausstellte, dass die Spruchschlüssel,die einem Verzeichniss entnommen wurden, keine Umlautbuchstaben enthielten.Man konnte jetzt die Zykeln so einander zu ordnen,dass Buchstaben die in der ersten Gruppe der verschlüsselten Spruchschlüssel nicht vorkamen,auf Umlaute fielen.

Eine weitere Schwierigkeit beruhte in der Unkenntnis der Schaltung der Eintrittswalze.Sie wurde jedoch glücklich erraten ebenso wie dies bei der Heeresmaschine geschehen war.Man setzte dabei voraus,dass keine Steckerverbindungen vorhanden sind,was sich als

richtig ergab.Im entgegengesetzten Fall wäre die Rekonstruktion der Maschine wahrscheinlich gescheitert.Und so fand man denn,ebenso wie im Heer,die Walzenschaltungen.

Jetzt kehrte man zu den Sprüchen aus früheren Jahren zurück. Im Jahre 1926 wurden innerhalb von Zeitabschnitten,die mehrere Tage umfassten,sämtliche Sprüche von ein- und derselben Position der Walzen ausgehend (also anders wie im Heere) verschlüsselt.Um den Spruchinhalt in einem dieser Zeitabschnitte zu finden,ging man folgendermassen vor: man fand zwei Sprüche,die allem Anschein nach denselben Spruchinhalt besassen,wobei jedoch in einem Fall vom Schlüssler ein Buchstabe ausgelassen worden war.Die entsprechenden Buchstaben beider Sprüche mussten daher,nacheinander getastet,denselben Klartext liefern. Mit Hilfe des Rostes erhielt man die Position der rechten Walze und hierauf ohne besondere Schwierigkeiten die Positionen der übrigen Walzen.Es stellte sich heraus,dass der Spruchinhalt nochmals mittels eines Satzbuches verschlüsselt war,desselben,der gleichzeitig auch ohne Maschinenverschlüsselung angewand wurde,und der bereits teilweise gelösst war;es war der schon erwähnte,die 18 Buchstaben ABEFGIKLMOPSTUWXYZ enthaltende vierstellige Code.Ausser diesem einen Zeitabschnitt wurden andere Zeitabschnitte nicht gelösst.Man stellte nur fest,dass die Walzenlage,Stellung der Umkehrwalze,Ringstellung und Spruchstellung (Grundstellung gab es bei diesem Verfahren nicht) in unregelmässigen Zeitabschnitten,die 3 - 15 Tage umfassten,verändert wurden.

Am 1.Januar 1927 wurde zwar nicht das Schlüsselverfahren,wohl aber das Satzbuch durch ein neues ersetzt.Man konnte jetzt die Schlüssel auf

folgende Weise finden:In einer ganzen Reihe von Sprüchen vermutete man am Ende stets eine und dieselbe Codegruppe,die "Fortsetzung folgt" bedäuten sollte.Da die Maschine die Eigenschaft besitzt,dass Klar- und verschlüsselte Buchstaben stets voneinander verschieden sind (mit Ausnahme von X ,das stets X ergibt),konnte man schliesslich diese Gruppe (unverschlüsselt) finden,und hierauf mittels des Kostverfahrens die Positionen der Walzen für einen Zeitabschnitt bestimmen.Es stellte sich heraus,dass das neue Satzbuch sämtliche 29 Buchstaben einschliesslich der Umlaute enthielt,es konnte jedoch aus Zeitmangel nicht gelöst werden.

Am 1.Januar 1929 trat eine Änderung,diesmal des Schlüsselverfahrens selbst ein.Sie beruhte darauf,dass jetzt jeder Spruch seine eigene Spruchstellung besass,die mittels der am Anfang und Ende jeden Spruches stehenden Kenngruppen auf eine uns näher nicht bekannte Weise angegeben wurden.

Am 1.Mai 1931 trat eine erneute Änderung des Schlüsselverfahrens ein, die darauf beruhte,dass jetzt der Spruchschlüssel ebenso geschlüsselt wurde wie im Heere.Gerade dadurch gelang es ja die Walzenschaltungen zu rekonstruieren.

Es kam jetzt noch darauf an,den Spruchinhalt selbst zu finden.Man vermutete zunächst als Inhalt Satzbuchgruppen.aber nach mehreren Monaten angestrengter vergeblicher Arbeit stellte es sich zufällig heraus,dass der Inhalt aus Klartext (ähnlich wie im Heere) bestand.

Das Schlüsselverfahren war,wie bereits erwähnt wurde,grundsätzlich dasselbe wie im Heere und in der Luftwaffe.Doch wurde die sogenannte "innere" Maschineneinstellung,d.h. Walzenlage,Stellung der Umkehrwalze, und Ringstellung so wie bisher in Unregelmässigen Zeitabständen geändert, während die Grundstellung täglich geändert wurde.

Die Spruchschlüssel wurden einem Verzeichnis entnommen. Sei es,dass dies Verzeichnis nicht sehr umfassend war oder sei es,dass die Schlüssler vorwiegend dieselben Spruchschlüssel aus dem Verzeichnis wählten,jedenfalls wiederholten sich dieselben oft,sodass eine Statistik angefertigt werden konnte, die es erlaubte aus den Substitutionen A_1A_4, A_2A_5, A_3A_6 die (unverschlüsselten) Spruchschlüssel selbst zu finden,wobei auch das Nichtvorkommen der Umlaute in den Spruchschlüsseln behilflich war.

Das Zyklometer konnte nicht angewandt werden,denn die Kataloge zu diesem müssten

$$60 \times 28^4 = 36\,879\,360$$

Positionen umfassen,was wohl kaum ausführbar wäre.So wurde denn die Position der rechten Walze mittels des Rosten festgestellt, was mühlos geschah,da keine Steckerverbindungen vorhanden waren,während die Position der übrigen Walzen mit Hilfe einer Kartothek,ähnlich der Katalogen F im Heere und in der Luftflotte,bestimmt wurde,nur war diese Kartothek umfangreicher,denn sie enthielt

$$28^3 = 21\,952$$

Positionen.

Der Spruchinhalt selbst war so kurz wie möglich gefasst. Es kamen in ihm Wortkürzungen aller Art vor;Die zweiten und weiteren Teile eines mehrteiligen Spruches begannen stets mit

den Buchstaben FORT (Abkürzung für Fortsetzung). Um Grundstellung und Ringstellung gesondert zu finden, ging man von diesen Buchstaben FORT aus, so wie man im Heer und in der Luftflotte von den Buchstaben AN und im S.D.-Netz von den Buchstaben QY ausging.

56. Die Anwendung in der deutschen Kriegsmarine der Enigma-Chiffriermaschine mit 26 Tasten.

Vom 1. Oktober 1934 ab wurde in der deutschen Kriegsmarine dieselbe Enigma-Chiffriermaschine wie im Heere angewandt. Das Chiffrierverfahren blieb dasselbe wie bisher, mit dem Unterschied, dass jetzt die Steckerverbindungen (stets 6 Paar) hinzutraten, die gleich der Grundstellung täglich geändert wurden. In der Zeit bis zum 15. November 1936 wurden ausserdem in der deutschen Kriegsmarine zwei zusätzliche Chiffrierwalzen angewandt, so dass im Ganzen fünf Chiffrierwalzen vorhanden waren, von denen drei gleichzeitig in die Maschine eingesetzt wurden.

Mit Hilfe der für das Heer hergestellten Kataloge zum Zyklometer konnte nur ein kleiner Teil (etwa ein Zehntel) der Tage bis zum 15. November 1936 gelöst worden. Dies genügte nicht, um ein Spruchschlüsselverzeichnis herstellen zu können. Erst als am 16. November 1936 die beiden Zusatzwalzen zurückgezogen wurden und nur die drei Walzen I, II, III übrig blieben, konnte ein entsprechendes Spruchschlüsselverzeichnis hergestellt werden, mit Hilfe dessen man nachträglich die Spruchschlüssel in den Tagen vor dem

16.November 1936 auffinden konnte.Hinterher mittels der Rostmethode wurden dann die Schaltungen der beiden Zusatzwalzen errechnet.Man nannte sie IV M und V M zum Unterschied von den später im Heer und in der Luftflotte gebrauchten Walzen IV und V.

Für wichtigere Sprüche gab es ausser dem allgemeinen noch einen Offiziers- und einen Stabs- (oder Admirals-) Schlüssel. Der Offiziersschlüssel wurde wie folgt angewandt:Zunächst wurde der gewählte Spruchschlüssel bei der Grundstellung "Allgemein" zweimal verschlüsselt und die beiden so erhaltenen dreistelligen Buchstabengruppen nach Voransetzung eines vierten Füllbuchstaben wie üblich als erste und letzte Gruppe in den Spruch eingesetzt.Hierauf jedoch wurde der gewählte Spruchschlüssel noch einmal bei der Grundstellung "Offizier" verschlüsselt und das Ergebnis (und nicht der Spruchschlüssel selbst) diente zur Schlüsselung des eigentlichen Spruchinhaltes.

Wie der Stabsschlüssel angewandt wurde ist nicht bekannt.

Am 1.Mai 1937 trat eine Änderung des Schlüsselverfahrens ein, die darauf beruhte,dass der Spruchschlüssel nicht mehr mittels der Maschine selbst,sondern auf eine andere,ziemlich komplizierte Weise verschlüsselt wurde.Die Einzelheiten des neuen Schlüsselverfahrens wurden erst bekannt,als es im Jahre 1940 den Engländern gelang,in einem versunkenen deutschen U-Boot die Schlüsselanleitung zu diesem Verfahren zu finden.Wir können dies Verfahren

hier nicht ausführlich beschreiben, sondern verweisen den Leser auf die photographische Abbildung der Schlüssel-anleitung.

Die Unkenntnis des neuen Schlüsselverfahrens hinderte uns nicht im Jahre 1937 eine Reihe von Ergebnissen zu erzielen, die hier mitgeteilt werden mögen.

Der Spruchschlüssel wird in jedem Spruch mittels der beiden ersten Gruppen angegeben, die zwecks Vermeidung von Fehlern am Ende des Spruches wiederholt werden. Der eigentliche Text also beginnt mit der dritten Gruppe. Mittels einer Methode die noch angegeben wird, gelang es den Textinhalt vieler Sprüche zwischen den 1. und 8. Mai 1937 zu finden und dadurch die Walzenlage, Steckerverbindungen, sowie teilweise auch die Ringstellung zu rekonstruieren. Ein Vergleich mit den gelössten Tagen von Ende April 1937 ergab, dass die innere Einstellung am 1. Mai 1937 keiner Änderung unterlag, und dass sie in der Zeit vom 27. April bis 8. Mai dieselbe geblieben ist.

Ein Vergleich der Spruchschlüssel der gelössten Sprüche mit den beiden ersten (oder letzten) Gruppen ergab folgendes:

Werden in sämtlichen gelössten Sprüchen eines Tages die beiden ersten Gruppen in vier nebeneinander stehende Buchstabenpaare geteilt und haben zwei Sprüche ein gemeinsames erstes, zweites oder drittes Buchstabenpaar, so haben sie auch einen gemeinsamen ersten, zweiten oder dritten Spruchschlüsselbuchstaben.

Die umgekehrte Behauptung ist nicht wahr.Gleichen Buchstaben können also sehr wohl verschiedene Buchstabenpaare entsprechen. Auch entsprechen gleichen Buchstabenpaaren an verschiedenen Stellen im Allgemeinen verschiedenen Spruchschlüsselbuchstaben.

Bei der Änderung des Verfahrens am 1.Mai 1937 wurde ausser der Beibehaltung der inneren Einstellung noch ein zweiter grober Fehler durch die Schlüsselstelle der deutschen Kriegsmarine begangen.Da ein Kriegsschiff nicht rechtzeitig mitder neuen Schlüsselmethode versehen werden konnte,verkehrte es noch während der drei ersten Maitage 1937 nach dem alten Verfahren.Auf diese Weise konnte man am 2. und 3.Mai 1937 die Grundstellungen "allgemein" und "Offizier" auffinden.

Von Seiten der Engländer wurde später noch folgendes festgestellt:

Werden die Spruchschlüssel der nach dem neuen Verfahren geschlüsselten Sprüche mittels der gefundenen Grundstellungen vom 2. und 3.Mai 1937 entschlüsselt,so entsprechen denselben Buchstabenpaaren dieselben Buchstaben der entschlüsselten Spruchschlüssel,selbst wenn sie an verschiedenen Stellen auftreten.

Der Inhalt der Sprüche in der Periode vom 1. bis 8.Mai 1937 wurde auf folgende Weise gefunden:Nehmen wir an wir hätten einen Spruch,der nach der Streichung der zwei ersten Gruppen folgendermassen beginnt:

VLPP WGKS WKUL QBOR

Weiterhin nehmen wir an,dass dieser Spruch die Fortsetzung eines anderen Spruches sei,der im Kopfe die Uhrzeit 1623 trägt.Nach

unseren Erfahrungen muss dann der Klartext dieses Spruches mit den Buchstaben

F O R T Y Q Z W E Y Y Q Z W E Y

beginnen (QZWE bedeutet 162).Wir kennen also ein aus 16 Buchstaben bestehendes Fragment des Textes vor und nach der Verschlüsselung.Da in der Marine stets nur 6 Paar Steckerverbindungen auftreten,muss ein Teil der Buchstaben unverändert bleiben.Man macht nun verschiedene Annahmen darüber,welche Buchstaben unverändert geblieben sind,und sucht diese Annahmen zu verifizieren, entweder direkt auf der Maschine,oder mittels des Rostes,oder mit Hilfe der Bogen Jeffreys,einer englischen Erfindung,die unseren Katalogen F entsprach.In allen Fällen ist die Arbeit sehr lang,so dass sie sich nur dann lohnt,wenn es wie in unserem Falle,darauf ankommt,ein neues Verfahren zu analysieren.

Den Engländern gelang es noch einige Sprüche vom Jahre 1938 zu lösen.Hieraus ging hervor,dass jetzt die Umkehrwalze B im Gebrauch ist.Wahrscheinlich wurde sie in derselben Zeit wie im Heer eingeführt.Die Zahl der Steckerverbindungen blieb weiterhin 6 Paar.

Im Jahre 1940 fanden die Engländer in einem gesunken deutschen U-Boot zwei Chiffrierwalzen,die die Bezeichnung VI und VII trugen Ob jetzt in der Marine die fünf Walzen I,II,III,VI und VII,oder ob sämtliche Walzen I bis VII angewandt werden,muss dahingestellt bleiben.

57. Chronologische Übersicht über die Anwendung von Enigma-Chiffriermaschinen in der deutschen Kriegsmarine.

| | | |

58. Teilnahme der drei Staaten an der Lösung der Enigma.

I. Polen

Zykelntheorie
Substitutionentheorie
Schaltungen der Walzen I - III
und der Umkehrwalze A
Methode zur Auffindung der
Eintrittswalze
Methode zur Auffindung der
Steckerverbindungen
Methode der charakteristischer
Schlüssel
Statistische Methode
Methode ungleicher Buchstaben
Bestimmung der rechten Walze
Der Rost und Katalog P
Zyklometer (Maschine und Katalog)
Auffindung des Textes
Schaltungen der Umkehrwalze B
Schaltungen der Walzen IV und V
Analyse des zweiten Schlüssel-
verfahrens
Die Bomben
Die Netze (Projekt)
Kataloge zu den Netzen (Projekt)
Analyse des dritten Schlüsselver-
fahrens
Das Funknetz S.D.
Die Marine-Enigma-Maschine mit
29 Tasten
Schaltungen der Walzen IV M und
V M
Analyse des Marine-Schlüsselver-
fahrens vom 1. Mai 1937

II. England

Die Netze (Ausführung)
Kataloge zu den Netzen
(Ausführung)
Methode Jeffreys
Methode Knox
Methode Herivel
Walzen VI und VII
(im U-Boot gefunden)

III. Frankreich

Lieferung zweier wichti-
ger Dokumente

Raport – fotokopia przekładu na język francuski

- TRADUCTION -

("ENIGMA" - Kurzgefasste Darstellung der Auflösungsmethoden)

3.- Zykelntheorie
5.- Substitutionentheorie
6.- Die Substitution E
7.- Die Substitution S
8.- Einige Ziffern
9.- Auffindung der Spruchschlüssel
11.- Die statistische Methode
12.- Methode ungleicher Buchstaben
13.- Bestimmung der rechten Walze
14.- Der Rost
15.- Der Katalog F
16.- Der Zyklometer
17.- Grundstellung und Ringstellung
18.- Einige Bemerkungen
23.- Auffindung der Walzenlage
24.- Bomben
25.- Die Netze
28.- Methode KNOX
29.- Kataloge zu den Netzen
30.- Methode HERIVEL
31.- Drittes Schlüsselverfahren
32.- (simplement, traduction du verbe "tauschen" au sens technique qui lui est donné)

- - - - - - - -

(Au point de vue linguistique, toutes questions pourront être posées à M. BARSAC) .

3. Théorie des cycles

Une analyse détaillée des six premières lettres de chaque message conduisit au résultat que ces lettres constituent la clef du message. Plus précisément, il fut constaté ce qu'il suit: On impose d'avance une certaine position des roues, la même à tous les chiffres pour une journée donnée. Ensuite chaque chiffreur choisit arbitrairement une clef de trois lettres qu'il chiffre deux fois consécutivement sortant de la position imposée des roues. De cette façon il obtient six lettres qu'il place à l'entrée avant le texte propre.

Or, comme la première et la quatrième, resp. la deuxième et la cinquième, resp. la troisième et la sixième lettres sont le résultat de chiffrement d'une même lettre, il est clair qu'il existe des rapports entre ces lettres. Il était possible de former certaines expressions avec les six premières lettres des divers messages d'une même journée que l'on appelle cycles, et qui permettent à énoncer ces rapports sous forme de théorèmes suivants:

1). Le nombre des cycles d'une même longueur est toujours pair

2). Les lettres ~~se~~ qui se trouvent dans un certain cycle sont provoquées par des lettres qui se trouvent dans un autre cycle de la même longueur.

3). Si une lettre X fut provoquée par une lettre Y, alors la lettre qui se trouve du côté droit de X fut provoquée par la lettre qui se trouve du côté gauche de Y.

L'ensemble de ces trois théorèmes ~~forme ce que l'on appelle la théorie des~~ avec ses conséquences forme ce que l'on appelle la théorie des cycles. Par cette théorie on s'est approché au problème de la reconstruction des clefs individuelles des messages, c'est à dire des clefs choisies arbitrairement par les chiffreurs. La résolution complète de ce ~~théorème~~ problème était déjà possible, mais les travaux cryptologiques furent dans ce temps-là dirigés dans une autre direction.

5. Théorie des substitutions

On aborda maintenant le problème le plus important, c'est à dire la recherche des connexions des roues. A cette effet on se servait d'une méthode mathématique, mais le chemin à parcourir était long et il fallait surmonter une série de difficultés sérieuses. Une exposition de la méthode mathématique appliquée dépasserait considérablement les cadres de cette esquisse. Pour son étude nous renvoyons le lecteur à un des oeuvres suivants:

1). J. A. Serret: Cours d'Algèbre supérieure, Tome II.
2). E. Netto. Substitutionentheorie
3). Burnside: Theory of groups of finit order.
4). Bianchi: Lezioni sulla teoria dei gruppi di sostituzioni.

Ici nous devons nous borner à donner une idée du chemin parcourue:

Le chiffre Enigma est une substitution, cela veut dire que la machine change les lettres de l'alphabet dans des autres lettres pour chaque position des roues.

Désignons par A_1 la substitution effectuée sur les lettres de l'alphabet quand les roues se trouvent dans la position initiale (Grundstellung) fixée pour la journée donnée, par A_2 la position suivante, et ainsi de suite jusqu'à A_6.

Si nous disposons d'un nombre suffisant de messages (en moyen il en faut environ 80) ce que nous voulons admettre, nous pouvons former les produits A_1A_4, A_2A_5, A_3A_6. On peut donc regarder ces produits comme connus.

Désignons ensuite par

S la substitution effectuée par les Steckverbindung
C_α " " " " la roue de droit
C_β " " " " " " " milieu
C_γ " " " " " " " gauche
U " " " " " " miroir
E " " " " " " d'entrée, c'est à dire par la succession dans laquelle le courant électrique coule des touches à la roue C_γ.

Q la substitution (1,2,3,4, ... 24,25,26)

Si pendant le chiffrement de la clef du message la roue de milieu ne fournie pas ce qui est assez probable et que nous voulons admettre dans la suite, alors on peut exprimer les substitutions $A_1, A_2, A_3 \ldots A_6$ de la façon suivante:

$$A_1 = SEC_\gamma C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1} C_\gamma^{-1} E^{-1} S^{-1}$$
$$A_2 = SEQC_\gamma Q^{-1} C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1} Q C_\gamma^{-1} Q^{-1} E^{-1} S^{-1}$$
$$A_3 = SEQ^2 C_\gamma Q^{-2} C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1} Q^2 C_\gamma^{-1} Q^{-2} E^{-1} S^{-1}$$
$$- - - - - - - - - - - - - - - - - - - -$$
$$A_6 = SEQ^5 C_\gamma Q^{-5} C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1} Q^5 C_\gamma^{-1} Q^{-5} E^{-1} S^{-1}$$

Il faudrait donc, pour trouver les connexions des roues, résoudre ce système d'équations qui, bien entendu, ne sont pas des équations ordinaires mais des équations de substitution.

La première difficulté que nous rencontrons ici en ce que non seulement les membres droits, mais aussi les membres gauches des équations sont inconnus. Ce qui est connu, ce sont seulement les produits A_1A_4, A_2A_5, A_3A_6. Mais la théorie des cycles nous apprend qu'il n'existe, en général, plus que quelques dizaines de désignations pour la substitution A_1 et que chaque désignation de A_1 détermine en même temps une seule désignation pour la substitution A_4. La même observation s'applique aussi aux substitutions A_2 et A_5, et A_3 et A_6. On peu

donc s'imaginer que l'on a écrit toutes les désignations possibles pour les substitutions $A_1, A_2, \ldots A_6$. De telle façon on peut surmonter cette première difficulté en augmentant en même temps, il est vrai, le travail à exécuter bien de fois, car dans les opérations à suivre il faut mettre successivement toutes les désignations possibles pour $A_1, A_2, \ldots A_6$.

La deuxième difficulté était encore beaucoup plus grave. Elle consistait dans la substitution S qui était inconnu. On a encore étudié ce problème profondément quand les connexions des roues étaient déjà trouvées par d'autres voies, et on est venu à la conviction que pratiquement, sans connaissance de la substitution S, notre système d'équations était irrésoluble. Théoriquement on a élaboré une méthode, mais elle exigeait beaucoup de temps, beaucoup de matériel, la connaissance de la substitution E, et la connaissance des substitutions $A_1, A_2, A_3 \ldots A_6$ séparément.

Le troisième obstacle était le manque de connaissance de la substitution E, et il semble que c'est à cause de cet obstacle que les recherches des cryptologues anglais sont échouées. Dans le bureau polonais des chiffres on supposait d'abord que la substitution E avait la même forme comme dans la machine à chiffrer commerciale, c'est à dire

$$E = \begin{pmatrix} A & W & E & R & T & Z & U & I & O & A & S & D & F & G & H & J & K & P & Y & X & C & V & B & N & M & L \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 & 26 \end{pmatrix}$$

Les recherches postérieures conduisaient au résultat qu'il était possible de trouver la substitution E par un chemin déductif mais seulement avec la connaissance antérieure de la substitution S.

En résumé on peut donc dire qu'il était possible, au moins théoriquement, de trouver les connexions des roues sans aucun autre aide, seul à l'aide des matériaux d'écoute, mais à condition que l'on devine la substitution E. Mais si l'on veut éliminer tout moment de devination, il faut supposer qu'on bien la substitution E ou la substitution S soient connues. Et nous répétons: si l'inconnu est S, il faut un matériel qui s'étend sur un intervalle de

temps bien long.

En réalité notre système d'équations fut résolu grace au document français qui donnait la substitution S pour une période de deux mois, et grace à la heureuse derivation de la substitution E.

Pour orienter le lecteur nous communiquons qu'il faut pour trouver les connexions des roues, amener nos équations à la forme suivante:

$$E^{-1}S^{-1}A_1SEQ^{-3}E^{-1}S^{-1}A_4SEQ^3 = C_\delta[C_\beta C_\alpha U C_\alpha^{-1}C_\beta^{-1}Q^{-3}C_\beta C_\alpha U C_\alpha^{-1}C_\beta^{-1}Q^3]C_\delta^{-1}$$
$$Q^{-1}E^{-1}S^{-1}A_2SEQ^{-3}E^{-1}S^{-1}A_5SEQ^4 = C_\delta Q^{-1}[C_\beta C_\alpha U C_\alpha^{-1}C_\beta^{-1}Q^{-3}C_\beta C_\alpha U C_\alpha^{-1}C_\beta^{-1}Q^3]QC_\delta^{-1}$$
$$Q^{-2}E^{-1}S^{-1}A_3SEQ^{-3}E^{-1}S^{-1}A_6SEQ^5 = C_\delta Q^{-2}[C_\beta C_\alpha U C_\alpha^{-1}C_\beta^{-1}Q^{-3}C_\beta C_\alpha U C_\alpha^{-1}C_\beta^{-1}Q^3]Q^2C_\delta^{-1}$$

Ces équations malgré leur longueur ne sont pas très compliquées. Les membres gauches sont connus, et les membres droits ont la partie du milieu commune. Par élimination de cette partie on reçoit $C_\delta Q C_\delta^{-1}$ ce qui donne immédiatement C_δ, c'est à dire connexions de la roue droit.

Il fallait encore trouver les connexions de la roue du milieu, du gauche, de la roue miroir, et déterminer les positions pour lesquelles les roues tournent, mais nous n'insisterons pas sur ces questions, parceque méthodiquement elles n'apportent rien de nouveau.

Il vaut uniquement mentionner que les Allemands en plaçant dans leur „Gebrauchsanweisung" un exemple authentique de chiffrement, ont allégé le travail considérablement.

6. La substitution E

Nous voulons esquisser en quelques mots, comment on pourrait trouver la substitution E aussi par une voie déductive.

Comme nous sommes en possession des defs journalières pour deux mois, il est aisé à trouver deux journées pour lesquelles non seulement l'ordre des roues, mais aussi la position ~~des roues du droit~~ (c'est à dire la différence entre Grundstellung et Ringstellung) des roues du droit sont les mêmes. Pour une pair de telles journées nous formons nos deux systèmes d'équations A_1 jusqu'à A_6 et obtiendrons

$$A_1 = SEC_\delta FC_\delta^{-1}E^{-1}S^{-1}$$
$$A_2 = SEQC_\delta Q^{-1}FQC_\delta^{-1}Q^{-1}E^{-1}S^{-1}$$
$$A_3 = SEQ^2C_\delta Q^{-2}FQ^2C_\delta^{-1}Q^{-2}E^{-1}S^{-1}$$
$$\cdots\cdots\cdots\cdots$$
$$A_6 = SEQ^5C_\delta Q^{-5}FQ^5C_\delta^{-1}Q^{-5}E^{-1}S^{-1}$$

$$\underline{A_1} = \underline{S}\underline{E}\underline{C_\delta}\underline{F}\underline{C_\delta^{-1}}\underline{E^{-1}}\underline{S^{-1}}$$
$$\underline{A_2} = \underline{S}\underline{E}\underline{Q}\underline{C_\delta}\underline{Q^{-1}}\underline{F}\underline{Q}\underline{C_\delta^{-1}}\underline{Q^{-1}}\underline{E^{-1}}\underline{S^{-1}}$$
$$\underline{A_3} = \underline{S}\underline{E}\underline{Q^2}\underline{C_\delta}\underline{Q^{-2}}\underline{F}\underline{Q^2}\underline{C_\delta^{-1}}\underline{Q^{-2}}\underline{E^{-1}}\underline{S^{-1}}$$
$$\cdots\cdots\cdots\cdots$$
$$\underline{A_6} = \underline{S}\underline{E}\underline{Q^5}\underline{C_\delta}\underline{Q^{-5}}\underline{F}\underline{Q^5}\underline{C_\delta^{-1}}\underline{Q^{-5}}\underline{E^{-1}}\underline{S^{-1}}$$

Dans ~~les~~ équations nous avons posé pour abréviation $F = C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1}$, $\underline{F} = \underline{C_\beta}\,\underline{C_\alpha}\,U\,\underline{C_\alpha^{-1}}\,\underline{C_\beta^{-1}}$. Les lettres soulignées signifient les grandeurs qui se rapportent à la deuxième journée.

Nous transformons nos équations de façon à obtenir six nouvelles équations dans lesquelles les membres du côté gauche sont connus:

$$S^{-1}A_1 S\underline{S^{-1}}\underline{A_1}\underline{S} = EC_\delta F\underline{F}C_\delta^{-1}E^{-1}$$
$$S^{-1}A_2 S\underline{S^{-1}}\underline{A_2}\underline{S} = EQC_\delta Q^{-1}F\underline{F}QC_\delta^{-1}Q^{-1}E^{-1}$$
$$\cdots\cdots\cdots\cdots$$
$$S^{-1}A_6 S\underline{S^{-1}}\underline{A_6}\underline{S} = EQ^5C_\delta Q^{-5}F\underline{F}Q^5C_\delta^{-1}Q^{-5}E^{-1}$$

Par élimination de $F\underline{F}$ nous obtenons les expressions

$$E(QC_\delta Q^{-1} C_\delta^{-1})E^{-1}$$
$$EQ(QC_\delta Q^{-1} C_\delta^{-1})Q^{-1}E^{-1}$$
$$EQ^2(QC_\delta Q^{-1} C_\delta^{-1})Q^{-1}E^{-1}$$
$$\cdots\cdots\cdots\cdots$$
$$EQ^4(QC_\delta Q^{-1} C_\delta^{-1})Q^{-4}E^{-1}$$

et de là, par élimination de $(QC_\delta Q^{-1} C_\delta^{-1})$ nous obtenons $EQ^{-1}E^{-1}$ et enfin E.

Le chemin qui nous mène au résultat est bien long, surtout quand les substitutions $A_1 A_2 \ldots A_6$ ne sont pas connues séparément, seulement les produits A_1A_4, A_2A_5, A_3A_6, et l'exécution effective des opérations ébauchées ici absorberait certainement une personne pour quelques mois. Mais en tout cas nous constatons qu'on arriverait toujours d'une ou d'autre manière au résultat pourvu que les Stechzeverbindungen sont connues.

7. La substitution S

Nous voulons enfin montrer une méthode qui conduirait probablement au bout même si l'on ne possédait pas les deux pour deux mots. Mais alors il faut admettre que la substitution E est connue, ou au moins que l'on peut la deviner ce qui est, du reste, arrivé en réalité. Ensuite il faut supposer que les substitutions $A_1, A_2, \ldots A_6$ sont connues séparément, et non seulement les produits A_1A_4, A_2A_5, A_3A_6. Et enfin il faut que nous disposions d'un matériel tellement étendu, qu'il soit possible de former les substitution A_1, $A_2, \ldots A_6$ pour quelques centaines de journées. Quand toutes ces hypothèses sont accomplies, on peut espérer que l'on trouve deux journées, pour lesquelles l'ordre des roues est le même, la position des roues du gauche et du milieu est la même, et pour lesquelles la position des roues du droit ne diffère plus que de trois unité. Un tel cas, s'il arrive, est facile à découvrir. Car admettons par exemple, pour fixer les idées, que les positions des roues du droit diffèrent de 3, de telle façon que les substitutions A_1 et A_4 naissent dans la même position. Alors il est facile à démontrer que les produits A_1A_2 et A_4A_5 sont semblable, et aussi les produits A_2A_3 et A_5A_6. Il suffit pour cela écrire les quatre

équations correspondantes:

$A_1A_2 = S(EGQGQ^{-1}E^{-1})S^{-1}$ $\quad$ $\underline{A_4}\underline{A_5} = \underline{S}(EGQGQ^{-1}E^{-1})\underline{S}^{-1}$

$A_2A_3 = S(EQGQGQ^{-2}E^{-1})S^{-1}$ $\quad$ $\underline{A_5}\underline{A_6} = \underline{S}(EQGQGQ^{-2}E^{-1})\underline{S}^{-1}$

dans lesquelles, pour abréviation, on a posé $G = C_\alpha C_\beta C_\gamma U C_\delta^{-1} C_\beta^{-1} C_\alpha^{-1}$.

Ensuite on peut calculer le produit $S\underline{S}$ une fois à l'aide des équations A_1A_2 et $\underline{A_4}\underline{A_5}$, et une autre fois à l'aide des équations A_2A_3 et $\underline{A_5}\underline{A_6}$.

Les résultats ~~doivent~~ doivent être naturellement dans les deux cas les mêmes. Et enfin le produit $S\underline{S}$ doit se composer d'au moins 14 cycles.

La difficulté essentielle consiste en ce que l'on obtient de telle façon seulement le produit $S\underline{S}$ et non les 2 substitutions S et $\underline{S}$ séparément. Mais on peut montrer qu'en général les substitutions S et $\underline{S}$ n'admettent plus que quelques centaines de valeurs. Il faut donc poser toutes ces valeurs successivement dans nos équations et chercher à parvenir à un résultat. C'est un très grand travail qui serait purement inexécutable si encore les substitutions $A_1, A_2, \ldots A_6$ n'étaient pas connue séparément, mais seulement les produits A_1A_4, A_2A_5, A_3A_6.

8. Quelques chiffres.

Une description détaillée de la machine Enigma dépasserait les cadres de ~~cette esquisse~~ cette esquisse. Aussi nous ~~nous~~ voulons nous contenter de donner quelques chiffres pour montrer la puissance du point de vue cryptologique de la machine Enigma pourvu que l'on s'en serve avec prudence.

Le nombre de différents ordres de roues est

$$3 \cdot 2 \cdot 1 = 6$$

quand on utilise 3 roues, et

$$5 \cdot 4 \cdot 3 = 60$$

quand on utilise 5 roues.

Il y a

$$26^3 = 17576$$

différentes positions fondamentales (Grundstellung) et autant ~~positions~~ différentes positions des anneaux (Ringstellung).

Il existe donc (avec les différents ordres des roues) pour trois roues

$$105.456$$

différents positions et pour cinq roues

$$1.054.560$$

différents positions

Le nombre des différents Steckerverbindung est pour 6 paires

$$\frac{26!}{2^6 \cdot 6! 14!} = 100\,391\,791\,500$$

et pour 10 paires

$$\frac{26!}{2^{10} \cdot 10! \cdot 6!} = 150\,738\,274\,937\,250$$

Le nombre de différents connexions possibles ~~pour~~ est pour la roue mince

$$\frac{26!}{13! 2^{13}} = 7\,905\,853\,580\,625$$

et pour les autres roues

$$26! = 403\,291\,587\,620\,262\,925\,584\,000\,000$$

9. La reconstruction des clefs individuelles.

Jusqu'ici on a résolu le problème suivant: Connaissant les clefs pour deux mois trouver les connexions des roues. Maintenant il s'agit du problème inverse: Connaissant les connexions des roues trouver les clefs.

Avant tout la machine Enigma du type commerciale fut modifiée dans le bureau technique du bureau polonais des chiffres tellement qu'elle pouvait servir pour la lecture des télégrammes militaires. Ensuite on lisait tout le matériel de deux mois pour lesquels on possédait les clefs. A cette occasion on découvrit une série des fautes commises par les chiffreur et on en tira naturellement tout le profit possible. Ces fautes servaient surtout à la reconstruction des clefs individuelles, c'est à dire des clefs que les chiffreurs choisissaient arbitrairement, chiffraient deux fois et ensuite mettaient au commencement du message. Dans le courant de temps les Allemands réussirent à dresser leur personel de telle façon qu'il commirent des fautes de moins en moins. Mais le développement dans cette direction avançait assez lentement pour que l'on put toujours réussir dans l'entretemps réussir à inventer des méthodes de plus en plus raffinées, qui quand même parvenaient à trouver les clefs individuelles.

11. La méthode statistique

Nous apercûmes, que les lettres d'alphabet n'entraient pas dans les clefs avec la même fréquence. Par exemple ~~les lettres A et Q paraîtraient~~ comme première lettres paraîtraient dans les clefs surtout les lettres A et Q, comme deuxièmes lettres toutes les voyelles, comme troisièmes lettres ~~toute~~ les lettres L et O. Il y avait aussi des lettres comme J et Y, qui se présentaient très rarement. On fabriquait donc une statistique des lettres pour les trois places et puis on ~~s'efforçait~~ s'efforça à subordonner les cycles l'un à l'autre de ~~telle~~ façon à obtenir une concordance la meilleur possible avec la statistique.

La fréquence des lettres changeait du reste un peu avec le temps, et il fallait la changer à plusieurs reprises. ~~Outre cela~~ En outre la fréquence des lettres dans l'armée différait considérablement de celle dans l'aviation. Et dans le „Sicherheitsdienst" on divisait les lettres avec tant de attention que toutes les lettres apparaissaient avec la même fréquence et l'application de la méthode statistique était dans ce cas impossible.

12. Méthode des lettres différentes

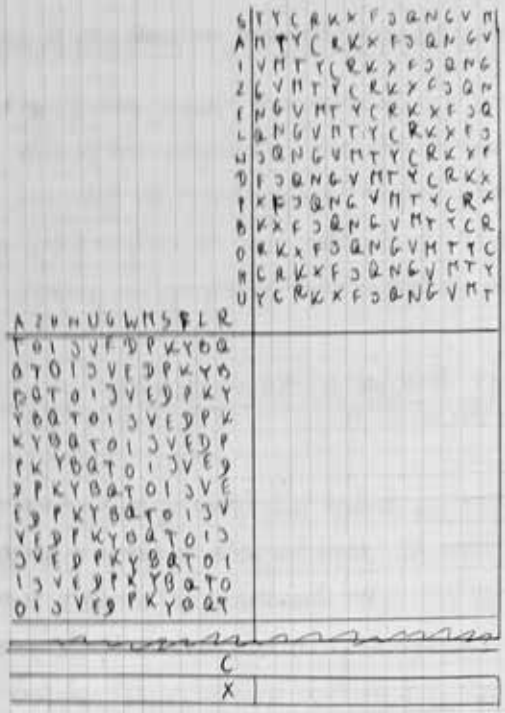
Les différences

Après l'interdiction de choisir trois lettres égales comme clefs, ~~les différences~~ évitaient même telles clefs dans lesquelles entraient ~~se~~ deux lettres égales comme AAB ou FVF. Cette ~~caractéristique~~ marque était la plus courante et c'est conservée jusqu'aujourd'hui. La méthode basée sur cette marque a cet avantage qu'on peut parfois agir tout à fait mécaniquement.

Supposons par exemple que, pour la journée donnée, on a ~~obtenu~~ des cycles de la forme suivante:

(SAIZELWDPBOHU)(YCRKXFJQNGVMT)
(AZHNUGWMSFLR)(QBYKPDEVJIOT)(C)(X)
(AZCSYBVMFJPDO)(NUGTIRHQKXEWL)

Il faut alors dessiner la figure ci-dessous et deux figures analogues et puis biffer dans les rectangles vides les caractères qui ~~correspondraient~~ à entraîneraient ~~la~~ l'identité de deux lettres. Quand on dispose d'un matériel assez nombreux, il ne restera à la fin qu'un seul cas.



13. La détermination de la ~~gauche~~ droite

On avait donc dans la plupart des cas la possibilité de reconstruire les clefs individuelles. Maintenant on passa à la découverte des clefs du jour, c'est à dire ~~position~~ ordre des roues, „Stecherverbindung", position des anneaux, position fondamentale. On commença par la détermination de l'ordre des roues.

Quand on écrit l'une ~~sous~~ l'autre deux ~~phrases~~ phrases allemandes ~~quelconques~~ chacune composée de 100 lettres, alors on ~~écrit~~ écrivent en moyenne 8 colonnes qui contiennent chacune deux lettres égales. Cette marque subsistera même quand on chiffrera les deux phrases d'après le même procédé.

Si par contre on prends deux textes ~~pour~~ dépourvus de sens dans lesquels les lettres paraîssent avec la même fréquence (à peu près), alors on devra en moyenne ~~seulement~~ sur 100 lettres seulement 4 colonnes composés de deux lettres égales.

On se sert de cette marque pour déterminer la roue ~~g~~droite. Car si l'on dispose d'un matériel assez nombreux, on trouvera un ~~nombre~~ de paire de télégrammes telles que dans chaque paire les premières lettres et aussi les deuxième lettres sont identiques pendant que les troisièmes lettres sont différentes. On écrit alors les deux télégrammes d'une paire l'une sous l'autre de telle façon que les lettres qui furent chiffrées dans la même position se trouvent verticalement l'une sous l'autre. Mais (a priori) il y a deux positions possibles, ~~elle dépend~~ elle dépend du moment dans lequel la roue de milieu tourne. ~~On~~ Il faut donc compter dans les deux positions le nombre de colonnes avec les lettres égales et on obtiendra dans la vraie position, en général, à peu près deux fois plus de colonnes que dans l'autre position. On apprendra donc, dans quel intervalle la roue de milieu tourne, et ~~si l'on dispose~~ nous procéderons de la même façons avec toutes les paires, il sera possible de resserer l'intervalle pour qu'on puisse déterminer la roue ~~de~~ droite qui, comme on ~~sait~~ sait, produit le tournement de la roue du milieu. Les autres roues seront déterminées plus tard par une autre voie.

14. Le gril

La phase ~~sui~~ prochaine du travail consistait dans la découverte des "Steckerverbindung". C'était un problème assez difficile, mais ~~enfin~~ on trouva enfin une méthode qui était basée sur le fait que la roue du milieu tourne en moyen une fois pour cinq et que les „Steckerverbindung" ne changent pas toutes les lettres.

~~Pour rendre notre méthode clair~~ Imaginons, pour rendre notre méthode clair, que les „Steckerverbindung" n'existent pas. On peut alors amener les six équations pour les Substitutions $A_1, A_2, \ldots A_6$ à la forme suivante :

$$Q^x C_\beta^{-1} Q^x E^{-1} A_1 E Q^x C_\beta Q^{-x} = F$$
$$Q^{x+1} C_\beta^{-1} Q^{-x-1} E^{-1} A_2 E Q^{x+1} C_\beta Q^{-x-1} = F$$
$$- \quad - \quad - \quad - \quad - \quad - \quad - \quad - \quad -$$
$$Q^{x+5} C_\beta^{-1} Q^{-x-5} E^{-1} A_6 E Q^{x+5} C_\beta Q^{-x-5} = F$$

Tout est connu dans ces équations à l'exception de $F = C_\beta C_\alpha \ldots C_\alpha^{-1} C_\beta^{-1}$ et de l'exposant X. Car quoiqu'on connaît, grâce à la méthode précédente, quelle est la rose du côté droit, on ne sait pas, quelle est la position de cette rose.

Nous procédons donc de la manière suivante: On pose pour x successivement les valeurs $0, 1, 2, \ldots 25$, et on calcule chaque fois les valeurs correspondantes de F dans les six équations. En général ces six valeurs seront différentes entre eux. Mais pour une certaine X tous les F deviendront égaux. De cette façon on obtient x, c'est à dire la position de la rose droite, et en même temps aussi la substitution F, dont nous nous servirons encore plus tard.

Dans la pratique on procède de telle façon, qu'on écrit sur une feuille de papier successivement les deuxièmes lignes des substitutions $C_\beta, QC_\beta Q^{-1}, \ldots \ldots Q^{25} C_\beta Q^{-25}$ (les premières lignes seraient toujours 1, 2, 3, ... 25, 26)

~~7 19 3 15 23~~ 7 19 3 15 23 11 20 4 16 25 10 14 22 2 17 6 25 9 1 21 12 18 5 24 13 8

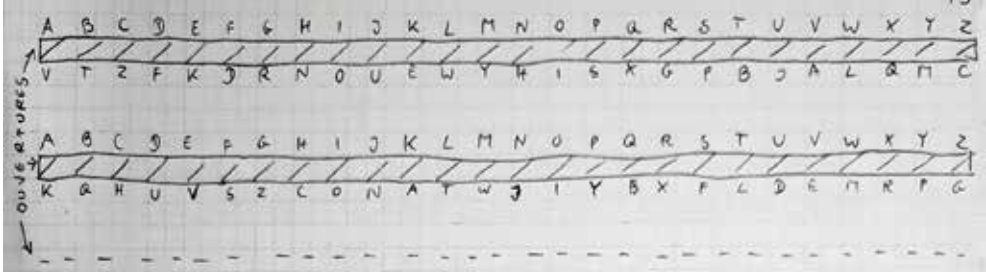
18 2 17 22 10 19 3 15 25 5 13 21 1 16 5 24 8 26 20 11 17 4 23 12 7 6

1 13 21 5 18 2 14 24 8 12 20 26 15 1 23 7 25 19 10 16 3 22 11 6 5 17

- -

(l'exemple est arbitraire)

Ensuite on écrit sur une deuxième feuille avec ~~des~~ ouvertures (d'où le nom grid) les six substitutions $A_1, A_2, \ldots A_6$ de la manière suivante:



Après ces préparations on pose le gril sur la ~~feuille~~ première feuille et on ~~déplace~~ le déplace du haut en bas jusqu'à ce que dans une certaine position toutes les substitutions F qui apparaissent dans les ouvertures deviendront identiques. Mais cela ne se produit seulement dans le cas où les „Steckerverbindung" manquent. Dans le cas contraire ~~l'image~~ l'image ~~se~~ change, mais comme les „Steckerverbindung" ne réintroduisent toutes les lettres, on remarquera dans une certaine position des analogies parmi ~~les~~ les 6 différentes substitutions F. Il faut alors tâcher à placer autrement les lettres dans les substitutions $A_1, A_{21} \ldots A_6$ (simultanément) pour que toutes les substitutions F deviendront identiques. Si l'on réussit, les déplacement des lettres donnent les „Steckerverbindung" cherchés, et en même temps on obtient la position de la roue droite et la substitution F.

15. Le catalogue F

Connaissant déjà la roue droite et leur position on pourrait déterminer les roues du milieu et gauche ~~et~~ et leurs positions par un simple tâtonnement de tous les cas possibles directement sur la machine. Mais pour éviter ce travail inutile, le même pour chaque jour, on a confectionné une fois pour toutes un catalogue contenant toutes les substitutions possibles F dont il existe

$$6 \cdot 26 \cdot 26 = 4056.$$

Maintenant il suffisait ~~pour~~ chercher la substitution F que l'on a trouvé en même temps ~~des~~ de les „Steckerverbindung" dans le catalogue pour apprendre ~~dans~~ tout de suite ordre et position des roue du milieu et du gauche.

16 Le cyclomètre

La méthode longue et incommode qu'on employait pour trouver les „Steckerverbindungen" n'amena pas toujours à la solution. Au surplus elle exigea ~~d'avance~~ la connaissance d'avance des clefs individuelles et les méthodes pour les trouver ~~faciles~~ étaient souvent onéreuses et ne ~~donnèrent~~ produisaient pas toujours au résultat.

On chercha donc alors une méthode, ~~laquelle plus vite et sûr~~ qui amènerait au but plus vite et plus sûr.

~~On tâcha~~ Sachant ~~obtenir le fait~~ que la longueur des cycles ~~dans les substitutions~~ $A_x A_L$ est indépendante des „Steckerverbindungen" et que la forme de cycles est rarement la même dans deux jours différents, ~~On~~ tomba sur l'idée de cataloguer tous les cycles dans toutes les positions possibles des roues, c'est à dire dans 105456 positions.

Afin d'effectuer ce travail on construit une machine speciale, le cyclomètre ~~qui~~ le cyclomètre contenait deux Enigmes ~~se trouvant~~ complètes telle qu'elle que dans chaque position s'allumèrent simultanement une certaine quantité des petites lampes ~~selon~~ conforme à la longueur des cycles.

Ce travail ~~coûtait~~ exigeait toute une année de travail, mais ~~à l'école de~~ le catalogue une fois faite on trouvait en quelques minutes l'ordre des roues, leur position ~~des roues~~ et les „Steckerverbindungen" du jour.

17. La position fondamentale et la position des anneaux

Par ~~la~~ position des roues (nous ~~en~~ comprendrons toujours) ~~exprime~~ la différence entre la position fondamentale et la position des anneaux.

Pour parvenir à la solution complète des clefs du jour, on doit trouver séparément la position fondamentale et la position des anneaux. Pour cela l'étude unique ~~les études~~ ~~sur~~ des clefs du message ne suffisant ~~pas~~, il faut ~~on doit~~ passer ~~s'adresser~~ aux textes des messages. ~~Quand on résolvait~~ ~~Après avoir résolu~~ le matériel du mois d'octobre et décembre 1931 dont les clefs étaient connues, on aperçut que le texte des plusieurs messages commençait par les lettres AN.

Afin de trouver séparément la position fondamentale et la position des anneaux, on prenait ~~le~~ un message quelconque, supposant qu'il commence par les lettres AN et on essayait dans toutes les positions de la machine si notre supposition était ~~possible~~ juste – un travail onéreux parce qu'on doit examiner $26^3 = 17576$ positions.

~~On était~~ plus tard ~~persuadé~~ on constata, que, si un message commençait par les lettre AN ~~les~~ quelques ~~inconnues~~ positions de la roue droite étaient a priori impossibles.

Lorsqu'on disposait ~~chaque~~ pour un jour d'un nombre ~~suffisant~~ ~~des~~ ~~les~~ messages, où on pouvait supposer AN ~~AN~~ au commencement, on parvenait presque toujours à l'aide d'un simple calcul à fixer la position exacte de la roue droite.

18. Quelques observations

Décrivant
~~Pendant la description~~ de gril et de cylindre on a supposé que la roue de milieu ne tourne pas pendant le chiffrement de la clef individuelle. En réalité cette supposition n'est pas indispensable, au contraire la détermination de la position fondamentale et de la position des anneaux est ~~particulièrement~~ plus facile ~~quand~~ justement quand ~~la~~ ~~cette roue~~ la roue de milieu tourne. Nous nous rapportons au lecteur d'examiner les détails du travail dans ces conditions.

On a remarqué que, pour une journée donnée, les six nombres formant la position fondamentale et la position des anneaux étaient toujours différents entre eux. Cette constatation conduisait dans certains cas non seulement à une considérable simplification du travail, mais elle permettait aussi dans des années ultérieures à appliquer convenablement la méthode Herivel dont on parlera encore plus tard. Il y avait aussi des périodes où tous les 24 nombres qui, dans 4 journées successives formaient les positions fondamentales et les positions des anneaux étaient différents entre eux.

On a fait de pareilles observations à des temps divers aussi avec les „Steckerverbindung".

23. La détermination de la position des roues

Chez le nouveau procédé de chiffrement on ~~ne~~ chiffrait ~~plutôt~~ les clefs individuelles ~~toutes de la même~~ sortant de ~~position~~ différentes positions des roues. Il s'ensuit que la théorie des cycles et toutes les méthodes basées sur cette théorie, c'est à dire les méthodes ~~des~~ de détermination des clefs individuelles, ~~tout~~ le gril, ~~et~~ le cylindre, n'étaient plus valables.

~~Mais~~ On ne demeurait pas les bras croisés mais on se mettait à ~~la~~ l'examen du nouveau procédé. On établira avant tout ce qu'il suit:

Si le matériel était assez étendu, on trouvait de temps en temps de paires de télégrammes pour lesquelles les premières et ~~la~~ deuxième ~~lettre~~ de la position fondamentale, et aussi les deuxièmes lettres de la position fondamentale étaient identiques et pour lesquelles les troisièmes lettres se trouvaient dans l'alphabet côte à côte ou presque côte à côte comme par exemple TKP et TKR. Si alors par hasard ~~dans~~ aussi dans les clefs individuelles paraissent deux lettres ~~égales~~ identiques sur des places correspondantes, on peut parfois conclure quelle roue se trouve à la droite ou au milieu. Nous voulons expliquer les différentes possibilités par quelques exemples

1). Supposons que nous avons trouver deux ~~messages~~ avec des clefs suivantes

Position fondamentale	Clef individuelle
TKP	ANV CKB
TKR	VTS JQM

Dans ce cas il est sûr que entre les lettres P et R, la roue de milieu tourne, c'est à dire qu'à droit se trouve la roue T parceque cette roue et seulement cette roue provoque un avancement entre les lettres K

Dans le cas contraire ~~correspondraient~~ correspondraient au deux lettres égales V aussi deux lettres égales R (ou J).

2)

Position fondamentale	Clef individuelle
TKP	ANV CKB
TKR	VTS BQM

Dans ce cas il est peu probable qu'il y ait un tournoyement entre P et R, c'est à dire que la roue droite soit la roue I.

3). Les positions fondamentales avec deux lettres différentes du milieu peuvent aussi donner parfois des informations sur l'ordre des roues, comme démontre l'exemple suivant:

Position fondamentale	Clef individuelle
TKP	ANV CKB
TLR	VTS JQM

Dans ce cas un tournoyement de la roue de milieu entre P et R est impossible, la roue de droite est donc différente de la roue I.

4). Même les positions fondamentales ~~avec deux lettres pareil~~ dont les lettres premières sont différentes, peuvent donner des renseignements sur l'ordre des roues

Position fondamentale	Clef individuelle
TJG	CMS PKR
UKG	CWT PLJ

Dans ce cas il est probable, qu'il y avait un tournoyement entre J et K, de la roue de gauche, c'est à dire que la roue de milieu est la roue IV.

~~Dans~~ On peut tirer de pareilles conclusions dans des autres cas.

24. Les „bombes"

Déjà quelques jours après l'introduction du nouveau procédé de chiffrement on a pris un projet comment on pourrait enlever les nouvelles difficultés. Notre marche des idées était la suivante:

Prenons un certain nombre de messages et écrivons leurs positions fondamentales et leurs positions des clefs individuelles:

1.	KTL	WOC	DRB	7	GRA	FDR	YWD
2	SVW	KKM	IYS	8	MDO	OTW	YZW
3	JOT	IWA	BWN	9	KJC	FSW	RSE
4	EDC	DSP	LJC	10	SGF	TEY	ASR
5	GKD	WAV	WHA	11	AGH	MDF	RHF
6	BWK	TCA	TOC	12	JBR	WLT	SOQ

Dirigeons maintenant notre attention sur les message Nr. 3. Dans sa clef individuelle la lettre W se présente deux fois dans un intervalle de 3 lettres. Cela signifie que dans une certaine position de la machine la lettre W donnerait une lettre pour nous inconnue disons X, et trois positions plus tard la même lettre W donnerait encore une fois la même lettre X. Nous faisons encore l'hypothèse que la lettre W ne fut pas modifiée par les „Steckerverbindung" ce qui (avec 5 – 8 Steckerverbindg) arrive dans 50% des cas.

On pourrait alors rechercher la juste position des roues en touchant la lettre W en même temps dans deux machines dont les positions des roues diffèrent de trois lettres et que l'on fait tourner synchroniquement. Chaque fois où la même lettre s'allume simultanément dans les deux machines, nous avons devant nous un cas qui peut être juste et qu'il faut donc examiner à part.

Mais de tels cas il y aurait trop souvent à ~~examiner~~ On prend donc au lieu de un message trois message dans lesquels la lettre W paraisse deux fois dans un intervalle de trois lettres. Dans notre exemple ce seraient les messages Nr 3, 5, et 8. Mais alors il faut se servir successivement au lieu de deux de six machines. ~~Car~~ En réalité, ce serait excessivement inopportun s'il on voulait vraiment manipuler avec six machines isolées. ~~On inventa plus~~ C'est pourquoi on inventa une machine, appellée bombe, qui correspondait à 6 ~~Enigma~~ machines "Enigma", procédait une impulsion électrique, et s'arrêtait ~~la~~ à chaque cas favorable automatiquement. Dans le bureau polonais des chiffres on fabriqua 6 bombes correspondant aux 6 ordres des roues (les roues IV et V ~~n'existaient pas encore~~) n'étaient pas encore en emploi). Chaque bombe venait à bout des 17576 cas possibles dans une heure et demie.

25. Les filets

La construction des bombes n'était pas encore finie quand il y avait déjà des nouveaux changements. Le 15 décembre 1938 les roues IV et V furent introduites, c'est à dire le nombre des ordres des roues décuplé. ~~et~~ Deux semaines plus tard on augmenta le nombre de „Steckverbindungen" à 7-10. Les bombes ~~perdaient~~ perdaient pratiquement ~~la~~ une grande partie de leur importance par ces changements, parceque la solution d'une journée exigeait maintenant beaucoup de temps. On réussissait parfois, par la méthode décrivée plus haut, à déterminer ~~pas~~ en partie l'ordre des roues, mais seulement quand on avait beaucoup de matériel ~~ce qui n'arrivait pas très souvent~~, mais cela n'arrivait pas souvent. Au surplus l'application des bombes était limitée par les „Steckverbindung".

On créa donc déjà bientôt une nouvelle méthode qui était indépendante ~~de la~~ du nombre des „Steckverbindung".

Pour expliquer la nouvelle méthode nous devons ~~nous~~ avant tout introduire une nouvelle notion, celle des positions masculines et féminines. Retournons encore une fois aux messages donnés sur la page (21)

1.	KTL	WOC DRB	7.	GRA	FDR YWD
2.	SVW	KKM IYS	8.	MDO	OTW YZW
3.	JOT	IWA BWN	9.	KJC	FSW RSE
4.	EDC	DSP LJC	10.	SGF	TEY ASR
5.	GKD	WAV WHA	11.	AGH	MDF RHF
6.	BWK	TCA TOC	12.	JBR	WLT SOQ

Un cas comme ~~dans~~ la clef N°.3 qu'une lettre (dans l'exemple la lettre W) ~~paraisse~~ deux fois ~~dans~~ à une distance de trois lettres, ne peut se produire dans toutes les positions. Par des calculs on peut montrer que cela n'arrive que dans 40% ~~des~~ de toutes les cas (plus précis le rapport est égal à $1 - \frac{1}{\sqrt{e}}$, e étant la base des logarythmes naturelles). Nous appelons ces positions positions féminines, les autres positions masculines.

~~D~~Dans notre exemple ~~les~~ messages 3, 5, 6, 8, 9, 11 appartiennent sûrement aux positions féminines, quant au reste on ne peut rien dire. Les „Steckerverbindung" ont naturellement une influence sur les lettres des clefs mais non sur le sexe des positions.

On pourrait donc faire un catalogue avec toutes les positions féminines et chercher dans ce catalogue si l'on ne trouve pas six positions féminines dont la distance est la même ~~comme~~ que la distance des positions fondamentales JOU, GKD, BWK, MDR, KJD, AGK. (Il faut aussi tenir compte à des tournoyements possibles de la roue du milieu et du gauche).

Mais comme cela serait en pratique inexecutable on inventa les ainsi nommés filets: Pour chaque ordre des roues on ~~fait~~ inscrit ~~enregistrer~~ toutes les positions féminines sur 26 feuilles de papier, ~~une chaqunne~~ dont chacune contient 26 × 26 cases, et cela ~~en~~ en quadruple exémplaire. ~~Il~~ Les diverses

feuilles correspondent aux 26 positions de la roue gauche, les 26 × 26 cases de chaque feuille aux 26 × 26 positions de la roue de milieu et de droite. On expliquera la cause de la quadruple exécution plus bas. On perfore les cases correspondant à des positions féminines (d'où le nom filet).

Maintenant on pose, pour revenir à notre exemple, 6 feuilles parmi les 26 feuilles ~~dans une succession et une position qui correspond~~ l'une sur l'autre dans une succession et une position qui correspondent aux distances mutuelles des positions fondamentales. Si simultanément sur toutes les feuilles à la même place paraît un ~~trou~~ trou, alors nous avons affaire à un cas qui peut être favorable et que l'on faut examiner séparément. Pour épuiser tous les cas possibles il faut échanger ~~cycliq~~ les feuilles cycliquement. Sur chaque feuille se trouvent les 26 × 26 cases dans une quadruple exécution parce qu'on ne pose pas les feuilles directement l'une sur l'autre, mais décalées l'une envers l'autre.

Le résultat dépend d'une mise extrêmement soignée des feuilles l'une sur l'autre dans la juste position et c'est pourquoi on confectionne toujours avant le travail une petite fiche, appelée ~~[illegible]~~ le nom, sur laquelle était inscrit la succession et la position mutuelle des feuilles.

La connaissance, quelles positions ~~sont~~ ~~étaient~~ sont masculines et quelles féminines, fut prise aux catalogues pour le cyclomètre. Car il est clair que les positions féminines correspondent aux substitutions ~~dans~~ qui ~~des~~ cycles constituent composés d'une seule lettre.

L'examen des cas ~~possibles~~ favorables fut aussi exécuté à l'aide du cyclomètre. Mais comme cela ~~était~~ exigeait beaucoup de temps, on voulait confectionner des catalogues spéciaux, dans lesquelles entrent nous seulement ~~les positions féminines~~ toutes les positions féminines, mais aussi les lettres qui se présentent dans tous les cycles composés d'une seule lettre. Mais cette idée ~~fut~~ ne fut réalisée que plus tard, par le bureau anglais des chiffres.

28. La Méthode Knox

Le cryptologue anglais avait remarqué que les chiffreurs allemands choisissent souvent comme position fondamentale les lettres qui paraissent dans les fenêtres de la machine après avoir terminé le chiffrement du message précédent. Celà arrivait surtout dans les messages composés de plusieurs parties. Il suffisait donc dans ces cas soustraire de la position fondamentale la longueur du message précédent pour obtenir la clef individuelle (en clair) du message précédent. Quand on obtenait alors des clefs caractéristiques comme ASD, WER, OKL, dans plusieurs parties d'un même message, on était sûr que le chiffreur a commis une telle faute. Comme il fallait pendant la soustraction tenir compte des tournoyements possibles de la roue de milieu et de gauche, il était possible de déterminer en partie l'ordre des roue et réduire dans le cas favorable le nombre des ordres possibles de 60 à 3. Il était aussi très important que par cette méthode on connaissait les clefs (en clair) de quelques messages.

Cette méthode fournissait de services précieuses surtout pendant la campagne norvégienne, où on résolvait jour par jour chaque journée obtenant ainsi du matériel extrêmement important d'une extrême importance.

29. Les catalogues pour les filets

Dans l'entretemps les Anglais ont réalisé encore une autre idée des cryptologues polonais. On a déjà mentionné que la vérification des cas possibles obtenus par les filets était exigeait beaucoup de travail et de temps. Il fallait chaque fois chercher à l'aide du cyclomètre les lettres qui déterminaient le caractère féminin de la position, et comparer avec les lettres qui entraient dans la clef individuelle correspondante. Déjà en Pologne on a voulu fabriquer des catalogues qui contiendraient toutes les lettres en question de toutes les positions féminines, mais des difficultés techniques empêchaient l'exécution de cette idée. Maintenant

elle fut réalisée par les Anglais à l'aide de la même machine qui servait à la fabrication des filets, encore un exemple brillant de la fécondité de la coopération polonais-français-anglaise. Grâce aux possibilités financières et organisatoires de nos collègues anglais on réalisait nos plans, qui autrement ne verraient probablement jamais le jour, furent réalisés sans égard aux frais et difficultés.

30. La Méthode Herivel

Un autre cryptologue fit la découverte suivante: Quand les chiffreurs allemands mettaient à après minuit ou le matin la machine à chiffrer au point pour le jour donné, il arrivait qu'ils ne tiraient pas les roues et, après la mise au point des anneaux, ne les tournaient pas, et qu'ils choisissaient pour le premier message les lettres qu'ils voyaient dans les fenêtres de la machine. Ainsi il passait que la position fondamentale du premier message ne différait pas beaucoup de la position des anneaux établi pour cette journée.

Comparant les positions fondamentales des messages chiffrés par des divers chiffreurs après minuit ou au grand matin, il était possible à déterminer souvent possible à déterminer précisément ou avec une grande approximation la position des anneaux pour la journée donné. Grâce à cette découverte il était possible à ét. Par cette découverte le temps exigé pour la résolution fut par cette découverte abrégé prodigieusement de telle façon que les Anglais possédait souvent la clef pour toute la journée déjà tôt au matin.

A l'occasion de cette méthode nous voulons ajouter à l'observation suivante: Quand on trouva les connexions de la roue IV et V, il n'était pas possible à fixer la position des anneau d'une manière définitive. Il existaient 26 positions différents, parmi lesquelles on choisit une par hasard. Après la résolution d'un nombre de journées (avant la découverte d'Herivel) on se rappela, qu'autrefois les trois lettres formant la position des anneaux

étaient toujours différents entre eux. Pour que cette marque subsistait aussi maintenant, il fallait corriger la position des anneau sur les roues IV et V. On trouva cette correction et ~~tout de suite communiqué~~ la communiqua tout de suite aux Anglais. Seulement après cette correction la méthode Herivel fut véritablement applicable.

31. Le troisième procédé de chiffrement

Le 1. Mai 1940, avant l'offensive allemande contre la Belgique et la Hollande, le ~~de~~ système de chiffrement fut changé encore une fois. On ne chiffrait plus la ~~clef~~ clef individuelle deux fois, mais seulement une fois. Dans la tête de chaque message figuraient maintenant 6 lettres, les trois premières signifiaient la position fondamentale, les trois dernières la clef chiffrée individuelle. ~~La~~ Cette situation se clarifia, parceque les chiffreurs allemands commirent ~~la~~ comme déjà une fois, ~~la~~ l'imprudence de chiffrer une suite des message d'après le nouveau procédé déjà la veille de ~~l'introduction~~ son introduction. Cette journée, le 30 Avril 1940 fut résolu, du reste par des cryptologues ~~anglais~~ polonais, et de telle façon on apprit, en quoi consistait le nouveau procédé.

C'était un coup très dur. Les filets et les catalogues pour les filets devinrent tout à fait inutilisable, seulement les méthodes Knox et Herivel restaient valables. Les cryptologues polonais, qui à titre passager furent transposés de Vignolles à Paris, cherchaient à l'aide de ces méthodes résoudre une journée, mais vainement.

Les Anglais ont eu plus de succès. Ils disposaient d'un matériel ~~pp~~ beaucoup plus volumineux, et ainsi ils reussirent, après une pause de trois semaines, à résoudre de nouveau une journée, le 20. Mai 1940, et bientôt presque toutes les journées suivantes. Ils envoyaient les clefs régulièrement et de nouveau les spécialistes polonais étaient arrivés aux deux machines d'origine de Varsovie pour aider à ~~déchiffrer~~ lire les matériel extrêmement important. Après l'évacuation de Paris le [illegible]

fut continué à La Ferté-St. Aubin et il ne fut interrompu qu'immédiatement avant l'armistice. La dernière journée pour laquelle les Anglais envoyèrent la clef, était le 16. Juin 1940.

32.

„Steckerverbindungen tauschen sechs Paar Buchstaben" veut dire:

La „Steckerverbindung" est composée de six paire ~~de~~ de lettres.

Chaque paire de lettres effectue une substitution additionelle ~~dans le texte chiffré et dans le clair du message~~ de telle façon que les deux lettres d'une paire sont ~~remplacées~~ l'une par l'autre aussi bien dans le clair que dans le chiffre de chaque texte.

Transkrypt oryginału w języku niemieckim

Inhaltsverzeichnis

1. Einleitung 147
2. Die Anfänge 148
3. Zykelntheorie 148
4. Zwei wichtige Schriftstücke 149
5. Substitutionentheorie 149
6. Substitution E 152
7. Die Substitution S 153
8. Einige Ziffern 153
9. Auffindung der Spruchschlüssel 154
10. Methode der charakteristischen Schlüssel 155
11. Die statistische Methode 155
12. Bestimmung der rechten Walze 155
13. Bestimmung der rechten Walze 156
14. Der Rost 157
15. Der Katalog F 158
16. Der Zyklometer 159
17. Grundstellung und Ringstellung 159
18. Einige Bemerkungen 159
19. Neue Netze. Beständige Änderungen 160
20. Umkehrwalze B 160
21. Neue Chiffrierwalzen 160

22. Änderung des Chiffriersystems 161

23. Auffindung der Walzenlage 161

24. Bomben. 162

25. Die Netze 163

26. Die Warschauer Konferenz 164

27. Kriegsaufbruch. Vignolles 165

28. Methode Knox. 166

29. Kataloge zu den Netzen. 166

30. Methode Herivel. 167

31. Drittes Schlüsselverfahren. 167

32. Chronologische Übersicht über die Änderungen des Schlüsselverfahrens im Heer und in der Luftwaffe 168

33. Das Funknetz des Sicherheitsdienstes 169

34. Die Schlüsselverfahren der deutschen Kriegsmarine vor Einführung der Enigma 169

35. Die Marine-Chiffriermaschine mit 29 Tasten 170

36. Die Anwendung in der deutschen Kriegsmarine der Enigma--Chiffriermaschine mit 26 Tasten 172

37. Chronologische Übersicht über die Anwendung von Enigma--Chiffriermaschinen in der deutschen Kriegsmarine 175

38. Teilnahme der drei Staaten an der Lösung der Enigma 176

1. Einleitung

Bereits wenige Jahre nach Beendigung des Weltkrieges begann die deutsche Wehrmacht zur Verschlüsselung von Nachrichten, die auf dem Funkwege übersandt werden sollten, sich der „Enigma-Chiffriermaschine“ zu bedienen.

Als erste führte, wie es scheint, die deutsche Kriegsmarine dieses Schlüsselverfahren bei sich ein. Jedenfalls ist gewiss, dass sie es bereits im Jahre 1926 benutzte, während seine Anwendung im deutschen Heer erst ab 15. Juli 1928 festgestellt wurde.

Am 1. August 1935 folgte dann mit der Einführung der Enigma die deutsche Luftflotte, vom September 1937 ab bediente sich ihrer der Sicherheitsdienst, auch von der Polizei wurde sie benutzt. Während sich so der Gebrauch der Enigma in der deutschen Wehrmacht immer mehr verbreitete, begannen andere Schlüsselmethoden, wie z.B. Doppelwürfelverfahren, allmählich zu verschwinden, sodass bereits eine gewisse Zeit vor Beginn des Deutsch-Polnischen Krieges 1939 beinahe alles, was von der deutschen Institutionen militärischen oder halbmilitärischen Charakters dem Funkwege anvertraut wurde, mit der Enigma-Maschine verschlüsselt war. Die Lösung dieses Schlüsselverfahrens bildete daher für die Generalstäbe Polens, Frankreichs und Grossbritanien ein Problem von erstklassiger Bedeutung. Im Laufe der Jahre wurde der Typ der Maschine mehrfach geändert. Vor Einführung der Enigma „M“ mit Steckerverbindung, die noch heute im Gebrauch ist, benutzte das deutsche Heer in der Zeit vom 15. Juli bis 31. Mai 1930 die Enigma „G“ mit Stöpselstellung. Bei den Wehrkreiskommandos bediente man sich eine Zeit lang einer selbstschreibenden Maschine, der sogenannten „Enigma II“, die jedoch anscheinend als unpraktisch bald aus dem Verkehr gezogen wurde. Die deutsche Kriegsmarine wiederum wandte bis September 1934 einen Maschinentyp mit 29 statt mit 26 Tasten an und ging erst ab Oktober 1934 zum Gebrauch derselben Maschine wie die deutsche Heer über. Übrigens bewahrte die deutsche Kriegsmarine auch späterhin eine gewisse Selbstständigkeit, indem sie in gewissen Zeiträumen eine grössere Anzahl von Schlüsselwalzen benutzte als die übrigen Formationen. Grundsätzlich kann man jedoch sagen, das ab Oktober 1934 bis heute nur ein Maschinentyp gebraucht wird, derselbe, dessen sich das deutsche Heer seit 1. Juli 1930 bedient.

Im folgendem wird skizziert, auf welche Weise dem Schlüsseldienst des polnischen Generalstabes gelang, den oben angeführten Typ der Enigma wiederherzustellen und welche Verfahren weiterhin ausgedacht wurden, um das eingehende Chiffriermaterial fast stets laufend zu lösen, trotz sämtlicher Veränderungen und Verbesserungen, die andauernd vom deutschen Schlüsseldient eingeführt wurden, um das Verfahren absolut unlösbar zu machen. Es wird auch dargestellt werden, von wie grosser Trägheit die Zusammenarbeit der Generalstäbe Polens, Frankreichs und Grossbritannien sich in dieser Hinsicht erwies.

2. Die Anfänge

Noch mehrere Jahre nach Gründung des polnischen Schlüsseldienstes konnte aus Personalmangel dem einlaufenden Schlüsselmaterial der deutschen Kriegsmarine keine Beachtung geschenkt werden. Daher wurde das Erscheinen der Enigma erst in dem Augenblick bemerkt, als sich ihrer das deutsche Heer zu bedienen begann, d.h. im Jahre 1928.

Unter den einlaufenden Sprüchen, die von deutschen Militärfunkstationen aufgegeben wurden, zeigten sich damals neben solchen, die wie bisher nach dem Doppelwürfelverfahren geschlüsselt waren, auch andere, die zweifellos den Charakter eines Substitutionverfahrens aufwiesen. Man begann sich mit ihnen zu beschäftigen und stellte leicht fest, dass die sechs ersten Buchstaben eines jeden Spruches eine besondere Bedeutung hatten und wahrscheinlich den Schlüssel des gegebenen Spruches darstellten. Gleichzeitig gelang es dem polnischen Nachrichtendienste, in dem Besitz mehrerer kleiner Schriftstücke zu kommen, aus denen hervorging, dass vom 15. Juli 1928 ab im deutschen Heer neben den bisherigen Schlüsselverfahren als neues das „Maschinenschlüsselverfahren Enigma G" in Kraft trat, dass bei der Enigma eine Stöpselstellung (während bei dem späteren Typ eine Steckerverbindung) vorhanden war, und dass jede Dienststelle in gewissen Zeitabständen eine Anzahl von Schlüsseln zugeteilt bekommt, von denen aus drei Zahlen nicht grösser als 26 besteht.

Es war nunmehr klar, dass das neue Schlüsselverfahren, das man entdeckt hatte, identisch mit dem Enigmaschlüsselverfahren war. Um das Studium dieses Verfahrens zu erleichtern, wurde vom polnischen Generalstab eine Enigma vom Handelstypus angekauft, bei der selbstverständlich die Walzen ganz andere Schaltungen hatten., als bei der Dienste des Heeres stehende Maschine, die sich aber auch sonst noch, wie sich später herausstellte, in mehrerer Hinsicht stark von der letzteren unterschied. Die Untersuchungen dieses Schlüsselverfahrens wollten jedoch nicht recht von der Stelle rücken und wurden nach einiger Zeit abgebrochen.

3. Zykelntheorie

Die Wiederaufnahme der Arbeiten erfolgte im Jahre 1932. Man unterzog die ersten 6 Buchstaben der Sprüche einer erneuten Untersuchung und stellte dabei folgendes fest: Für jeden Tag wird eine gewisse Stellung der Walzen, eine und dieselbe für sämtliche Schlüssler, festgesetzt. Daraufhin wählt sich jeder Schlüssler drei beliebige Buchstaben, schlüsselt sie zweimal hintereinander ausgehend von der für diesen Tag festgesetzten Stellung der Walzen und setzt die so erhaltenen 6 Buchstaben in den Anfang des Spruches ein.

Auf diese Weise entstehen zwischen dem 1. und 4., bezw. 2. und 5., bezw. 3. und 6. Buchstaben der Sprüche gewisse Beziehungen, die eine rein mathematische Behandlungsweise gestatteten und die Grundlage der Späteren Wiederherstellung der Enigma bildeten.

Man verfährt folgendermassen: Man nimmt irgendeinen Spruch, schreibt dessen ersten Buchstaben und rechts davon vierten Buchstaben auf. Dann sucht man einen Spruch, in dem der zuletzt aufgeschriebene Buchstabe als erster Buchstabe auftritt und schreibt recht vom dessen vierten Buchstabe auf. So verfährt man weiter, bis man zum ersten Buchstabe zurückkehrt. Das erhaltene Ergebnis nennt man einen Zyklus. Man kann folgende Sätze beweisen:

1. Zykeln derselben Länge treten stets in gerader Zahl auf.

2. Buchstaben eines Zyklus werden durch Buchstaben hervorgerufen, die in einem anderen, gleichlangen Zyklus auftreten.
3. Wird eine Buchstabe X durch einen Buchstaben Y hervorgerufen, so wird der rechts von X stehende Buchstabe durch den links von Y stehenden Buchstabe hervorgerufen.

Diese drei Sätze lösten teilweise die Aufgabe, die Spruchschlüssel zu rekonstruieren, und bestimmt hätte man schon damals dieses Problem vollständig gelöst, wenn nicht gerade in diesem Augenblick Hilfsmittel zur Verfügung gestellt worden wären, die Arbeiten in andere Bahnen lenkten.

4. Zwei wichtige Schriftstücke

In dieser Zeit gelangte nämlich die polnische Schlüsselstelle in den Besitz zweier Schriftstücke von ausserordentlicher Bedeutung. Das erste dieser beiden Schriftstücke trug die Überschrift: „Anleitung zum Maschinenschlüsselverfahren“, während das andere die sogenannten Tagesschlüssel zur Enigma für die Monate Oktober und Dezember 1931 enthielt. Diese Schriftstücke erhielt die polnische Schlüsselstelle vom französischen Generalstab, der in ihren Besitz durch seinen Nachrichtendienst gelang war. Es muss betont werden, dass der Besitz dieser Schriftstücke und zwar besonders der Tagesschlüssel entscheidend den Fortgang der Arbeiten beeinflusst hat. Ohne diese Dokumente wäre die Lösung des Enigmaschlüsselverfahrens zumindest um Jahre verzögert worden. Andererseits mag jedoch auch festgestellt werden, dass es weder der französischen noch der englischen Schlüsselstelle gelungen war, das Verfahren zu lösen, trotzdem beide Stellen im Besitz dieser Schriftstücke waren. Übrigens wird weiter unten eine Methode angegeben werden, die eventuell auch ohne den genannten Schriftstücken zum Ziele geführt haben würde.

Aus dem ersten der gennannten Dokument ging hervor, dass ab 1. Juni 1930 an Stelle der bisherigen Enigma mit Stöpselstellung eine neue Enigma mit Steckerverbindung trat. Weiter erfuhr man noch folgendes:

1) Die Maschine enthält 3 Schlüsselwalzen, deren Lage verändert werden kann. Änderung der Walzenlage erfolgt alle drei Monate.
2) Die Umkehrwalze ist fest (im Gegensatz zur Enigma-Handelsmaschine).
3) Die Schlüsselwalzen sind mit einem Zahlen-, bezw. Buchstabenring versehen. Änderung der Ringstellung erfolgt täglich.
4) Die Steckerverbindung vertauscht 6 Paar Buchstaben. Änderung der Steckerverbindung erfolgt täglich.
5) Die Stellung, von der aus der Spruchschlüssel geschlüsselt wird, heisst Grundstellung. Änderung der Grundstellung erfolgt täglich.

Das zweite Dokument enthielt, wie bereits bemerkt wurde, die Tagesschlüssel, d.h. Walzenlage, Grundstellung, Ringstellung, Steckerverbindung, für die Dauer von zwei Monaten.

5. Substitutionentheorie

Man schritt nun zur Bewältigung des Hauptproblems, d.h. zur Rekonstruktion der Walzenschaltungen. Man bediente sich hierbei einer mathematischen Theorie,

der so genannten Substitutionentheorie, die selbstverständlich hier nicht auseinandergesetzt werden kann, sondern vielmehr als bekannt vorausgesetzt wird. Man muss sich aber natürlich nicht vorstellen, dass es einfach genügte, bekannte Sätze der Substitutionentheorie anzuwenden, um das Ergebnis zu erhalten. Im Gegenteil war auf dem Wege zum Endziele eine ganze Reihe überaus schwieriger Hindernisse zu überwinden. Im Folgenden geben wir kurz den eingeschlagenen Gedankengang an. Das Schlüsselverfahren Enigma ist ein Substitutionverfahren, d.h. die Maschine setzt in jeder Position der Walzen für die Buchstabe des Alphabets andere Buchstaben ein. Wir bezeichnen mit A_1 die Substitution, der die Buchstaben des Alphabets unterworfen sind, wenn sich die Walzen in der für gegebenen Tag festgesetzten Grundstellung befinden, mit A_2 die Substitution in der nächstfolgenden Stellung der Walzen u.s.w. bis A_6.

Wenn man über genügende Anzahl von Sprüchen verfügt (im Durchschnitt etwa 80), so wird man mit Hilfe der Zykelntheorie zunächst die Produkte A_1A_4, A_2A_5, A_3A_6 bilden können, die daher als bekannt vorausgesetzt werden können. Wir bezeichnen nun weiter durch

S die Substitution hervorgerufen durch die Steckerverbindungen
C_γ » » » » » rechte Schlüsselwalze
C_β » » » » » mittlere »
C_α » » » » » linke »
U » » » » » Umkehrwalze
E » » » » » Eintrittswalze
Q = (1, 2, 3, 4, 5, 6, ..., 24, 25, 26)

Wenn während des Chiffrierens des Spruchschlüssels die mittlere Walze sich nicht fortbewegt, was ziemlich wahrscheinlich ist, und was wir im Folgenden voraussetzen wollen, so können die Substitutionen A_1 bis A_6 auf folgende Weise dargestellt werden:

$$A_1 = \quad S\ E\ C\gamma C_\beta\ C_\alpha\ U\ C_\alpha^{-1}\ C_\beta^{-1}\ C\gamma^{-1}E^{-1}\ S^{-1}$$
$$A_2 = S\ E\ Q\ C\gamma Q^{-1} C_\beta\ C_\alpha\ U\ C_\alpha^{-1}\ C_\beta^{-1}\ Q\ C\gamma^{-1}\ Q^{-1}\ E^{-1}\ S^{-1}$$
$$A_3 = S\ E\ Q^2\ C\gamma Q^{-2} C_\beta\ C_\alpha\ U\ C_\alpha^{-1}\ C_\beta^{-1}\ Q^2\ C\gamma^{-1}\ Q^{-2}\ E^{-1}\ S^{-1}$$
. . . . . .
$$A_6 = S\ E\ Q^5\ C\gamma Q^{-5} C_\beta\ C_\alpha\ U\ C_\alpha^{-1}\ C_\beta^{-1}\ Q^5\ C\gamma^{-1}\ Q^{-5}\ E^{-1}\ S^{-1}$$

Die erste Schwierigkeit, die zu überwinden war, bestand darin, dass nicht nur die rechten, sondern auch die linken Seiten der Gleichungen unbekannt sind, bekannt sind nur die Produkte A_1A_4, A_2A_5, A_3A_6. Die Zyklentheorie lehrt uns jedoch, dass die Substitution A_1 in den meisten Fällen nicht mehr als etwa hundert Bezeichnungen annehmen kann und dass gleichzeitig jede Bezeichnung von A_1 eindeutig die Substitution A_4 festsetzt. Dasselbe gilt von A_2 und A_5, bezw. A_3 und A_6. Man kann sich also vorstellen, dass sämtliche Bezeichnungen von A_1 bis A_6 aufgeschrieben sind. Auf diese Weise kann man die erste Schwierigkeit als überwunden betrachten, auf Kosten allerdings einer vielfachen Vergrösserung der Arbeitszeit, denn bei den weiteren Operationen müssen sämtliche möglichen Bezeichnungen für A_1 bis A_6 der Reihe nach eingesetzt werden.

Die zweite Schwierigkeit ist noch viel ernster. Trotz grösster Bemühungen nämlich, die noch jahrelang aus theoretischen Gründen fortgesetzt wurden, nachdem die

Walzenschaltungen schon längst gefunden waren, liessen sich die oben angeführten Gleichungen auf keine Weise lösen, das grösste Hindernis stellte stets die Substitution S, d.h. die Steckerverbindung dar. Man hat schliesslich eine Methode gefunden, die vielleicht zum Ziele geführt hätte, sie setzte jedoch die Kenntnis der Substitutionen A_1 bis A_6 (und nicht Bloss der Produkte A_1A_4, A_2A_5, A_3A_6), die Kenntnis der Substitution E, und ferner recht umfangreiches Material voraus.

So wurde denn die zweite und Hauptschwierigkeit auf dem Wege der Lösung der Enigma vor allem durch das vom französischen Generalstab zur Verfügung gestellte Schriftstuck, das die Steckerverbindungen für zwei Monate enthielt, überwunden.

Die dritte Schwierigkeit beruhte auf der Unkenntnis der Substitution E. Es scheint, dass dies das Hindernis war, am dem die Bemühungen der englischen Kryptologen gescheitert sind. Spätere Untersuchungen in der polnischen Schlüsselstelle ergaben, dass man die Substitution E auf dem deduktiven Wege hätte finden können (vorausgesetzt, dass S bekannt ist), in Wirklichkeit jedoch fand man E durch Probieren. Man nahm zunähst an, die Substitution E sei dieselbe wie in der Enigma-maschine vom Handelstypus, d.h.:

Q	W	E	R	T	Z	U	I	O	A	S	D	F	G	H	J	K	P	Y	X	C	V	B	N	M	L
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Als man mit dieser Annahme kein Resultat erzielte, glaubte man anfangs, das am gewählten Tage während der Chiffrierung des Tageschlüssel eine Verschiebung der mittleren Walze stattfände. Man wiederholte also die ganzen Operationen noch einmal auf dem Material eines anderen Tages und, als man wieder kein Ergebnis erzielte, nahm man einen dritten und vierten und fünften Tag.

Die Arbeiten, die bereits Monate dauerten, sollten schon abgebrochen werden, als man noch einen Versuch machte und zwar unter der Annahme

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Diesmal hatte man Glück, die Annahme stellte sich als richtig heraus und führte zur Lösung der Aufgabe.

Zur Orientierung des Lesers wird mitgeteilt, dass zur Auffindung der Schaltungen der rechten Walze unser oben angeführtes System von 6 Gleichungen zunächst auf folgende Form gebracht werden muss.

$$E^{-1}S^{-1}A_1SEQ^{-3}E^{-1}S^{-1}A_4SEQ^{3} = C_\gamma \quad [C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1} Q^{-3} C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1} Q^{3}]\, C_\gamma^{-1}$$
$$Q^{-1}E^{-1}S^{-1}A_2SEQ^{-3}E^{-1}S^{-1}A_5SEQ^{4} = C_\gamma Q^{-1} [C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1} Q^{-3} C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1} Q^{3}]\, QC_\gamma^{-1}$$
$$Q^{-2}E^{-1}S^{-1}A_3SEQ^{-3}E^{-1}S^{-1}A_6SEQ^{5} = C_\gamma Q^{-2} [C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1} Q^{-3} C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1} Q^{3}]\, Q^2C_\gamma^{-1}$$

Die Gleichungen sind trotz ihrer Länge nicht besonders kompliziert. Alle Ausdrücke auf der linken Seite sind bekannt, all Ausdrücke auf der rechten Seite haben einen gemeinsamen Mittelteil. Durch Elimination dieses Teiles erhält man $C_\gamma QC_\gamma^{-1}$, und hierdurch unmittelbar C_γ, d.h. die Schaltungen der rechten Walze.

Man musste selbstverständlich noch die Schaltungen der linken, mittleren und Umkehrwalze auffinden sowie di Positionen, bei denen die Walzen sich drehten, da man jedoch hierbei keine grundsätzlich neuen Methoden anwandte, so mögen die diesbezüglichen Arbeiten übergangen werden.

6. Substitution E

Wir wollen kurz skizzieren, wie man die Substitution E auch deduktiv hätte finden können.

Da wir im Besitz der Tageschlüssel für zwei Monate sind, können wir leicht zwei solche Tage finden, in denen sowohl die Walzenlage als auch Position der rechten Walzen, d.h. die Differenz zwischen Grund- und Ringstellung der rechten Walze dieselbe ist. Wir stellen für diese beiden Tage die zwei Gleichungssysteme A_1 bis A_6 auf, und erhalten, wenn wir zur Abkürzung

$$F = C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1}$$

setzen und die Buchstaben, die sich auf zweiten Tag beziehen, unterstreichen:

$$\begin{array}{ll}
A_1 = S\ E\ C_\gamma\ F\ C_\gamma^{-1} E^{-1}\ S^{-1} & \underline{A_1} = C_\gamma \underline{F}\ C_\gamma^{-1} E^{-1} \underline{S}^{-1} \\
A_2 = SE\,Q C_\gamma Q^{-1} F\ Q\ C_\gamma^{-1} Q^{-1} E^{-1} S^{-1} & \underline{A_2} = \underline{S}E\,Q\,C_\gamma Q^{-1} \underline{F}\ Q\,C_\gamma^{-1} Q^{-1} E^{-1} \underline{S}^{-1} \\
A_3 = SE\,Q^2 C_\gamma Q^{-2} F\ Q^2 C_\gamma^{-1} Q^{-2} E^{-1} S^{-1} & \underline{A_3} = \underline{S}E\,Q^2 C_\gamma Q^{-2} \underline{F}\ Q^2 C_\gamma^{-1} Q^{-2} E^{-1} \underline{S}^{-1} \\
\vdots\ \vdots\ \vdots\vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots & \vdots\ \vdots\ \vdots\vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots \\
A_6 = SE\,Q^5 C_\gamma Q^{-5} F\ Q^5 C_\gamma^{-1} Q^{-5} E^{-1} S^{-1} & \underline{A_6} = \underline{S}E\,Q^5 C_\gamma Q^{-5} \underline{F}\ Q^5 C_\gamma^{-1} Q^{-5} E^{-1} \underline{S}^{-1}
\end{array}$$

Hieraus bilden wir folgende Gleichungen, in denen die rechten Seiten bekannt sind:

$$\begin{array}{l}
S^{-1} A_1 S \underline{S}^{-1} \underline{A_1} \underline{S} = E C_\gamma F\ \underline{F}\ C_\gamma^{-1} E^{-1} \\
S^{-1} A_2 S \underline{S}^{-1} \underline{A_2} \underline{S} = E Q C_\gamma Q^{-1} F\ \underline{F} Q\,C_\gamma^{-1} Q^{-1} E^{-1} \\
\vdots\ \vdots\ \vdots\vdots\ \vdots\ \vdots\vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\vdots\ \vdots\ \vdots \\
S^{-1} A_6 S \underline{S}^{-1} \underline{A_6} \underline{S} = E Q^5 C_\gamma Q^{-5} F\ \underline{F} Q^5 C_\gamma^{-1} Q^{-5} E^{-1}
\end{array}$$

Durch Elimination von $F\underline{F}$ erhalten wir die Ausdrücke:

$$\begin{array}{l}
E\ (Q C_\gamma Q^{-1} C_\gamma^{-1})\ E^{-1} \\
E\,Q\ (Q C_\gamma Q^{-1} C_\gamma^{-1})\ Q^{-1} E^{-1} \\
E\,Q^2\ (Q C_\gamma Q^{-1} C_\gamma^{-1})\ Q^{-2} E^{-1} \\
\vdots\ \vdots\ \ \vdots\ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots \\
E\,Q^4\ (Q C_\gamma Q^{-1} C_\gamma^{-1})\ Q^{-4} E^{-1}
\end{array}$$

Und hieraus durch Elimination von $QC_\gamma Q^{-1} C_\gamma^{-1}$ zunächst $EQ^{-1}E^{-1}$, und hieraus unmittelbar E.

Der Weg zum Ergebnis ist recht lang, besonders wenn die Substitutionen A_1 bis A_6 selbst nicht, sondern nur die Produkte A_1A_4, A_2A_5, A_3A_6 bekannt sind, und die tatsächliche Ausführung der hier skizzierten Operationen wurde eine Person sicherlich mehrere Monate lang in Anspruch nehmen. Jedenfalls aber möge festgestellt werden, dass, wenn nur die Steckerverbindungen bekannt sind, man stets auf diese oder andere Weise zum Ziel gelangt wäre.

7. Die Substitution S

Wir wollen endlich noch einen Weg zeigen, wie man wahrscheinlich auch zum Ziele gelangt wäre, wenn man nicht im Besitze der Schlüssel für zwei Monate befunden hätte. Es muss hierbei allerdings vorausgesetzt werden, dass die Substitution E bekannt ist oder wenigstens erraten wie es in Wirklichkeit geschehen ist. Ferner muss angenommen werden, dass die Substitutionen A_1 bis A_6 selbst und nicht Bloss die Produkte A_1A_4, A_2A_5, A_3A_6 bekannt sind. Auch das hätte man sicherlich erzielt. Und endlich müssen wir über so umfangreiches Material verfügen, dass wir in mehreren hundert Tagen die Substitutionen A_1 bis A_6 bilden können. Wenn alle diese Voraussetzungen erfüllt sind so ist es zu erwarten, dass man zwei Tage findet, in denen die Walzenlage dieselbe ist, die Differenz zwischen Grund- und Ringstellung der linken und mittleren Walze dieselbe ist, und die Differenz zwischen Grund- und Ringstellung der rechten Walze sich um nicht mehr als 3 unterscheidet. Tritt ein solcher Fall ein, so ist er leicht aufzudecken. Denn nehmen wir etwa an, die Positionen der rechten Walzen unterscheiden sich in den beiden Tagen um 3, so dass etwa die Substitutionen A_1 und $\underline{A}_4$ in derselben Position entstehen. Dann müssen zunächst einmal die Produkte A_1A_2 und $\underline{A}_4\underline{A}_5$ einerseits und die Produkte A_2A_3 und $\underline{A}_5\underline{A}_6$ anderseits ähnlich sein, wie man leicht überzeugt, wenn man die betreffenden Gleichungen aufschreibt:

$$A_1A_2=S(EGQGQ^{-1}E^{-1})S^{-1} \qquad \underline{A}_4\underline{A}_5=\underline{S}(EGQGQ^{-1}E^{-1})\underline{S}^{-1}$$
$$A_2A_3=S(EGQGQ^{-2}E^{-1})S^{-1} \qquad \underline{A}_5\underline{A}_6=\underline{S}(EGQGQ^{-2}E^{-1})\underline{S}^{-1}$$

wobei man zur Abkürzung $C_\alpha C_\beta C_\gamma U C_\gamma^{-1} C_\beta^{-1} C_\alpha^{-1} = G$ gesetzt hat.

Ferner kann man aus den Gleichungen A_1A_2 und $\underline{A}_4\underline{A}_5$ und aus den Gleichungen A_2A_3 und $\underline{A}_5\underline{A}_6$ andererseits das Produkt $S\underline{S}$ errechnen und dies Produkt muss in beiden Fällen gleich sein. Und schliesslich muss das Produkt $S\underline{S}$ aus mindestens 14 Zykeln bestehen.

Die Hauptschwierigkeit besteht nun darin, dass auf diese Weise nur das Produkt $S\underline{S}$ und nicht die Substitutionen S und $\underline{S}$ einzeln erhält. Es zeigt sich aber, dass im Allgemeinen S und $\underline{S}$ nur mehrere hundert verschiede Werte annehmen werden. Wir müssen also diese Werte der Reihe nach in unseren Gleichungen einsetzen und versuchen, zu einem Ergebnis zu gelangen. Eine sehr grosse Arbeit, die sicherlich unausführbar wäre, wenn auch noch die Substitutionen A_1 bis A_6 nicht einzeln, sondern nur ihre Produkte zu zweien bekannt wären.

8. Einige Ziffern

Eine vollständige Beschreibung der Maschine Enigma würde den Rahmen dieser Skizze weit überschreiten. So wollen wir uns denn begnügen einige Zahlen anzugeben, um zu zeigen, wie ein starkes Instrument vom kryptologischen Standpunkt aus die Enigma darstellt, vorausgesetzt natürlich, dass sie richtig angewandt wird.

Die Anzahl verschiedener Walzenlagen beträgt bei den drei Walzen

$$3\times2\times1 = 6$$

und bei fünf Walzen

$$5\times4\times3 = 60$$

Die Zahl der verschiedenen Grundstellungen und Ringstellungen beträgt je

$$26^3 = 17\,576$$

Die Zahl verschiedener Positionen der Walzen beträgt mithin (zusammen mit den Walzenlagen) bei drei Walzen

105 456

und bei fünf Walzen

1 054 560

Die Zahl verschiedener Steckerverbindungen beträgt bei 6 Paaren

$$(26!)/(2^6 \times 6! \times 14!) = 100\,391\,791\,500$$

Und bei zehn Paaren

$$(26!)/(2^{10} \times 10! \times 6!) = 150\,738\,274\,937\,250$$

Die Zahl verschiedener Schaltungen für die Umkehrwalze beträgt

$$(26!)/(13! \times 2^{13}) = 7\,905\,853\,580\,625$$

Und für die übrigen Walzen

$$26! = 403\,291\,587\,620\,262\,925\,584\,000\,000$$

Die letzte Zahl kann man sich folgendermassen veranschaulichen: Wenn sämtliche die Erdkugel bewohnenden Menschen in jeder Sekunde je eine Schaltung ausführen würden, so würden sie ihre Arbeit erst nach sechs Milliarden Jahren beenden (wobei nebenbei bemerkt werden möge, dass angeblich die Welt erst seit 2 Milliarden Jahren existierte).

9. Auffindung der Spruchschlüssel

Folgendes Problem ist bisher gelöst worden: Bei Kenntnis der Schlüssel für zwei Monate die Walzenschaltungen auffinden. Damit ist jedoch die Aufgabe nicht beendet. Es handelt sich vielmehr jetzt um die Lösung des umgekehrten Problems: Bei bekannten Walzenschaltungen die Schlüssel finden.

Zunächst wurde im technischen Büro der polnischen Schlüsselstelle die Enigma vom Handeltyp so umgeändert, dass sie zum Lesen von Militärsprüchen dienen konnte. Daraufhin wurde das Spruchmaterial für zwei Monate, für die Schlüssel vorhanden waren, gelöst und hierbei eine Reihe von Fehlern, die von den Schlüsslern begangen wurden, entdeckt und natürlich ausgenutzt. Diese Fehler dienten vor allem zur Auffindung der Spruchschlüssel d.h. der Schlüssel, die von Chiffranten willkürlich gewählt, zweimal geschlüsselt und daraufhin am Anfang des Spruches

eingesetzt werden. Im Laufe der Jahre gelang es zwar den Deutschen, ihr Schlüsselpersonal so zu schulen, dass immer weniger Fehler begangen wurden, die Entwicklung in dieser Richtung ging jedoch genügend langsam von statten, so dass es stets gelang, in der Zwischenzeit immer raffiniertere Methoden auszusinnen, um trotz allem die Spruchschlüssel auffinden zu können.

10. Methode der charakteristischen Schlüssel

In der ersten Zeit nach Einführung der Enigma wählten die Schlüssler mit Vorliebe solche Schlüssel, die aus 3 gleichen Buchstaben bestanden wie AAA, BBB, u.s.w. Die Methode der charakteristischen Schlüssel beruhte nun darauf, mit Hilfe der Zyklentheorie die einzelnen Zykeln so einander zuzuordnen, um möglichst viele aus drei gleichen Buchstaben bestehenden Schlüssel zu erhalten. Bald jedoch wurde den Schlüsslern die Wahl dreier gleicher Buchstaben verboten. Daraufhin begannen sie, sich solche Buchstaben zu wählen, die sich auf dem Glühlampenfeld der Maschine

Q W E R T Z U I O
A S D F G H J K
P Y X C V B N M L

quer oder waagerecht nebeneinander befinden, wie ASD, QAY, QWE, u.s.w. Es genügte jetzt die Zykeln so einander zuzuordnen, dass möglichst viele Schlüssel wie ASD u.s.w. entstanden.

11. Die statistische Methode

Bald aber wurde auch das verboten. Inzwischen bemerkte man jedoch, dass die Buchstaben des Alphabets in den Schlüsseln nicht mit gleicher Häufigkeit auftraten. So zum Beispiel traten auf als erste Buchstaben in den Schlüsseln vor allem Buchstaben A und Q, als zweite Buchstaben sämtliche Vokale, als dritte Buchstaben die Buchstaben L und O. Andere Buchstaben dagegen wie J oder Y kamen nur selten vor. Man verfertigte also eine Statistik der Buchstabenfrequenzen und bemühte sich dann, die Zykeln so einander zuzuordnen, um eine möglichst gute Übereinstimmung mit der Statistik zu erzielen. Die Buchstabenfrequenzen schwankten übrigens im Laufe der Zeit, so dass ab und zu die Statistik verändert werden musste. Auch waren die Buchstabenfrequenzen andere im Heer und andere in der Luftwaffe. Im Sicherheitsdienst wurden die Schlüssel so sorgfältig gewählt, dass sämtliche Buchstaben mit derselben Frequenz auftraten und die statistische Methode also nicht angewandt werden konnte.

12. Methode ungleicher Buchstaben

Nach dem Verbot, drei gleiche Buchstaben als Schlüssel zu wählen, vermieden die Schlüssler aufs sorgfältigste selbst solche Schlüssel, in denen auch nur zwei gleiche Buchstaben auftraten, wie AAB, oder FVF. Dieses Merkmal war das beständigste von allen und hat sich zum heutigen Tage erhalten. Die auf diesem Merkmal aufgebaute Methode hatte den Vorteil, dass man oft ganz mechanisch vorgehen konnte.

Nehmen wir etwa an, am gegebenen Tage hätten wir Zykeln von folgender Gestalt:

(SAIZELWDPBOHU) (YCRKXFJQNGVMT)
(AZHNUGWMSFLR) (QBYKPDEVJIOT) (C) (X)
(AZCSYBVMFJPDO) (NUGTIRHQKXEWL)

Wir haben dann nebenstehende Figur und zwei analoge Figuren aufzuzeichnen und hierauf in den leeren Rechtecken diejenigen Zuordnungen von Zykeln zu streichen, die Gleichheit zweier Buchstaben nach sich ziehen würden.

S	TYCRKXFJQNGVM
A	MTYCRKXFJQNGV
I	VMTYCRKXFJQNG
Z	GVMTYCRKXFJQN
E	NGVMTYCRKXFJQ
L	QNGVMTYCRKXFJ
W	JQNGVMTYCRKXF
D	FJQNGVMTYCRKX
P	XFJQNGVMTYCRK
B	KXFJQNGVMTYCR
O	RKXFJQNGVMTYC
H	CRKXFJQNGVMTY
U	YCRKXFJQNGVMT
AZHNUGWMSFLR	

TOIJVEDPKYBQ	
QTOIJVEDPKYB	
BQTOIJVEDPKY	
YBQTOIJVEDPK	
KYBQTOIJVEDP	
PKYBQTOIJVED	
DPKYBQTOIJVE	
EDPKYBQTOIJV	
VEDPKYBQTOIJ	
JVEDPKYBQTOI	
IJVEDPKYBQTO	
OIJVEDPKYBQT	
C	
X	

Wenn man über genügende Anzahl von Sprüchen verfügt, wird schliesslich nur ein Fall übrig bleiben.

13. Bestimmung der rechten Walze

Nachdem man so in den meisten Fällen in der Lage war, die Spruchschlüssel wiederherzustellen, trat man jetzt zur Auffindung der Tagesschlüssel, d.h. Walzen-

lage, Steckerverbindung, Ringstellung, Grundstellung. Man begann mit der Bestimmung der Walzenlage.

Wenn man zwei beliebige deutsche Sätze, jeder hundert Buchstaben lang, untereinander schreibt, so werden durchschnittlich in 8 Kolonnen je zwei gleiche Buchstaben auftreten. Diese Eigenschaft bleibt auch dann bestehen, wenn man beide Sätze nach einem und demselben Verfahren verschlüsselt. Nimmt man dagegen zwei sinnlose Texte, zu je 100 Buchstaben, in denen sämtliche Buchstaben mit etwa derselben Frequenz auftreten und schreibt sie untereinander, so wird man im Durchschnitt nur 4 Kolonnen mit je zwei gleichen Buchstaben antreffen. Diese Eigenschaft benutzt man, um die rechte Walze zu bestimmen. Wenn man nämlich über genügendes Spruchmaterial verfügt, so wird man eine Anzahl Paare von Sprüchen finden, derart, dass in jeder Paar die ersten sowie die zweiten Buchstaben der Schlüssel einander gleich, die dritten Buchstaben dagegen voneinander verschieden sind. Man schreibt nun die beiden Sprüche eines Paares so untereinander, dass Buchstaben, die bei der gleichen Position der Walzen geschlüsselt wurden, senkrecht untereinander zu stehen kommen. A priori sind jedoch zwei Fälle möglich, je nachdem, wann die Drehung der mittleren Walze erfolgt. Man zählt also nach, wieviel Kolonnen mit gleichen Buchstaben in beiden Fällen vorkommen und muss im richtigen Falle, im Allgemeinen wenigstens, etwa zweimal so viel Kolonnen erhalten als im falschen Fall. Man erfährt hierdurch, in welchem Intervall die mittlere Walze sich dreht, und, wenn man so mit sämtlichen Paaren verfährt, wird man fast stets das Intervall so einengen können, dass hierdurch die rechte Walze, die ja die Drehung der mittleren Walze bewirkt, eindeutig bestimmt wird. Die übrigen Walzen bestimmt man später auf andere Weise.

14. Der Rost

Die nächste Arbeitsphase bestand in der Auffindung der Steckerverbindungen. Es war dies ein ziemlich schwieriges Problem, doch schliesslich ersann man eine Methode, die davon ausging, dass erstens während des Schlüsselns des Spruchschlüssels eine Drehung der mittleren Walze nur etwa in 5 Fällen eintritt, und dass zweitens die Steckerverbindung eine Anzahl Buchstaben unverändert lässt.

Zur Veranschaulichung der Methode stellen wir uns zunächst einmal vor, die Steckerverbindung sei nicht vorhanden. Dann kann man die sechs Gleichungen für die Substitutionen A_1 bis A_6 auf folgende Gestalt bringen:

$$
\begin{aligned}
&Q^{X}\ C_{\gamma}^{-1}Q^{-X}\ E^{-1}A_1EQ^{X}\ C_{\gamma}Q^{-X} = F\\
&Q^{X+1}C_{\gamma}^{-1}Q^{-X-1}E^{-1}A_2EQ^{X+1}C_{\gamma}Q^{-X-1} = F\\
&\vdots\quad\vdots\quad\vdots\quad\vdots\quad\vdots\quad\vdots\quad\vdots\quad\vdots\quad\vdots\quad\vdots\quad\vdots\\
&Q^{X+5}C_{\gamma}^{-1}Q^{-X-5}E^{-1}A_6EQ^{X+5}C_{\gamma}Q^{-X-5} = F
\end{aligned}
$$

In diesen Gleichungen ist alles bekannt mit Ausnahme von $F = C_{\beta}C_{\alpha}UC_{\alpha}^{-1}C_{\beta}^{-1}$ und des Exponenten X. Denn wenn wir auch dank der vorliegenden Methode wissen, welche Walze sich auf der rechten Seite befindet, so wissen wir doch nicht, welches ihre Position ist.

Wir verfahren also auf die Weise, dass wir für X der Reihe nach die Werte von 0 bis 25 einsetzen und jedesmal F aus jeder der sechs Gleichungen errechnen. Die sechs Substitutionen F werden jedesmal untereinander verschieden seines mit Aus-

nahme einzigen Falles, wo sie sämtlich denselben Wert annehmen. Auf diese Weise erhalten wir X, d.h. die Position der rechten Walze und zugleich auch die Substitution F, die wir noch später benötigen werden.

In der Praxis geht man in der Weise vor, dass man auf einem Bogen Papier der Reihe nach die zweiten Zeilen der Substitutionen C_γ, $QC_\gamma Q^{-1}$,… , $Q^{25}C_\gamma Q^{-25}$ folgendermassen aufschreibt: (die ersten Zeilen der Substitutionen würden stets lauten 1 2 3 4 … 26)

19	3	15	23	11	20	4	16	26	10	14	22	2	17	6	25	9	1	21	12	18	5	24	13	8
2	14	22	10	19	3	15	25	9	13	21	1	16	5	24	8	26	20	11	17	4	23	12	7	6
13	21	9	18	2	14	24	8	12	20	26	15	4	23	7	25	19	10	16	3	22	11	6	5	17

(das Beispiel ist willkürlich)

Hierauf schreib man auf einem zweiten Bogen mit Öffnungen (daher der Name Rost) die 6 Substitutionen A_1 bis A_6 in folgender Form auf:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

V T Z F K D R N O U E W Y H I S X G P B J A L Q M C

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

K Q H U V S Z C O N A T W J I Y B X F L D E M R P G

Nach diesen Vorbereitungen legt man den Rost auf den ersten Bogen und verschiebt ihn so lange von oben nach unten, bis in einer bestimmten Lage die in Öffnungen erscheinenden Substitutionen F sämtlich identisch sind. Das trifft natürlich nur dann ein, wenn keine Steckerverbindungen vorhanden sind. Im entgegengesetzten Fall ändert sich das Bild, da jedoch die Steckerverbindungen nicht sämtliche Buchstaben vertauschen, wird man in einer bestimmten Lage gewisse Analogien zwischen den 6 verschiedenen Substitutionen F bemerken. Man muss nun versuchen, die Buchstaben der Substitutionen A_1 bis A_6 so umzustellen, dass alle F identisch werden. Gelingt dies, so ergeben die Umstellungen der Buchstaben die gesuchten Steckerverbindungen, und zugleich erhält man die Position der rechten Walze sowie die Substitution F.

15. Der Katalog F

Nachdem so die rechte Walze und ihre Position bereits bekannt war, hätte man die linke und mittlere Walze und ihre Positionen einfach so bestimmen können, dass man direkt auf der Maschine sämtliche möglichen Fälle probierte. Um sich jedoch dieselbe unnütze Arbeit zu ersparen, verfertigte man ein- für allemal einen Katalog, der sämtliche möglichen Substitutionen F, deren es

$$6 \times 26 \times 26 = 4056$$

gibt, enthielt. Es genügte jetzt die Substitution F, die man beim Suchen der Steckerverbindungen erhalten hatte, im Kataloge nachzuschlagen, um sofort Lage und Stellung der linken und mittleren Walze zu erfahren.

16. Der Zyklometer

Die Methode, die man anwandte, um die Steckerverbindungen zu finden, war nicht nur lang und umständlich, sondern sie führte auch nicht immer zum Ergebnis. Übrigens setzte sie die Kenntnis des Spruchschlüssel voraus, und die Methoden, diese Schlüssel zu finden, waren ebenfalls zeitraubend und nicht immer vom Erfolg gekrönt. So sah man sich denn nach anderen Methoden um, die schneller und sicherer zum Ziele führen könnten. Man verfiel darauf, dass die Gestalt der Zykeln erstens invariant gegenüber den durch die Steckerverbindungen verursachten Substitutionen sei, und zweitens ein Charakteristikum des betreffenden Tages bildete, in dem Sinne nämlich, dass zwei Tage deren Zykeln die gleiche Gestalt hatten, verhältnismässig selten vorkommen konnten. So kam man denn auf den Gedanken, die Zykeln in sämtlichen möglichen Positionen der Walzen, deren es bei drei Walzen, wie bereits gesagt,

105 456

gab, zu katalogisieren. Um diese Arbeit zu bewältigen, baute man eine besondere Maschine, den Zyklometer, der aus zwei Enigmen bestand, die so gekoppelt waren, dass in jeder Position eine grössere oder kleinere Anzahl der Glühlampen gleichzeitig aufleuchtete, je nach der Länge des entsprechenden Zyklus. Mehr als ein Jahr verging, ehe die Arbeit beendet war, dann aber fand man in der Regel schon nach wenigen Minuten Walzenlage, Position der Walzen und Steckerverbindungen des betreffenden Tages.

17. Grundstellung und Ringstellung

Unter Position der Walzen verstehen wir stets die Differenz zwischen Grund- und Ringstellung. Um also den völligen Besitz des Tagesschlüssels zu gelangen, mussten noch die beiden letzten Elemente des Tagesschlüssels, d.h. Grund- und Ringstellung gefunden werden. Dazu genügt es offenbar nicht, sich auf das Studium der Spruchschlüssel zu beschränken, vielmehr muss auf den Inhalt der Sprüche zurückgegriffen werden.

Als man das Material von Oktober und Dezember 1931, für das Schlüssel vorhanden war, löste, bemerkte man, dass der Text sehr vieler Sprüche mit Buchstaben AN begann.

Um also Grund- und Ringstellung gesondert zu erhalten, nahm man irgendeinen Spruch, von dem man vermutete, dass er mit Buchstaben AN begann und probierte in sämtlichen Positionen der Maschine, ob diese Annahme möglich ist. Eine langwierige Arbeit, wenn man bedenkt, dass dabei $26^3 = 17\,576$ Positionen untersucht werden müssen.

Später überzeugte man sich, dass, wenn ein Spruch mit den Buchstaben AN begann, a priori gewisse Positionen der rechten Walze unmöglich waren. Und da man täglich über eine ganze Anzahl von Sprüchen verfügte, in denen man ein AN am Anfang erhofft durfte, so gelang es meistens rein rechnerisch die richtige Position der rechten Walze zu erhalten.

18. Einige Bemerkungen

Bei der Beschreibung des Rostes und des Zyklometers wurde vorausgesetzt, dass während des Schlüsselns des Spruchschlüssels die mittlere Walze sich nicht

drehte. In Wirklichkeit ist diese Voraussetzung nicht bedingt erforderlich, ja die Auffindung von Grund- und Ringstellung ist sogar besonders leicht gerade dann, wenn eine Drehung der mittleren Walze eintritt. Wir überlassen es dem Leser zu ermitteln, wie sich in solchen Fällen die Verhältnisse gestalten.

Man hat bemerkt, dass innerhalb eines Tages die sechs Grund und Ringstellung bildenden Zahlen bzw. Buchstaben stets voneinander verschieden waren. Diese Feststellung führte nicht nur in gewissen Fällen zu bedeutender Vereinfachung der Arbeit, sondern sie erlaubte es auch in späteren Jahren die Methode Herivel, von der noch die Rede sein wird, zweckmässig anzuwenden. Es gab übrigens auch Zeiträume, wo gar stets in vier aufeinander folgenden Tagen alle 24, die Grund- und Ringstellungen bildenden Zahlen bezw. Buchstaben voneinander verschieden waren.

Ähnliche Entdeckungen hat man zu verschiedenen Zeiten auch mit den Steckerverbindungen gemacht.

19. Neue Netze. Beständige Änderungen

Im Masse wie sich die deutsche Wehrmacht entwickelte, wurde auch die Zahl der Heeresfunkstellen immer mehr vergrössert. Dabei wurde allmählich ebenfalls die Zahl der Funknetze, die sich alle derselben Enigma, jedoch mit anderen Tagesschlüssel bedienten, vermehrt. So bildete z.B. die neugegründete deutsche Luftflotte mit dem 1. August 1935 ihr eigenes Funknetz mit eigenem Tagesschlüssel.

Um die Unauflösbarkeit des Enigmaverfahrens sicherzustellen, wurden verschiedene Neuerungen eingeführt. Ab 1. Februar 1936 wurde die Walzenlage monatlich, und ab 1. Oktober 1936 sogar täglich geändert. Gleichzeitig wurde die Zahl der Steckerverbindungen geändert, sie betrug nicht mehr als 6, wie bisher, sondern 5 bis 8. Und schliesslich wurde noch am 2. November 1937 die bisherige Umkehrwalze aus dem Verkehr genommen und durch eine neue, die sogenannte Umkehrwalze B, ersetzt.

20. Umkehrwalze B

Von Seiten der deutschen Schlüssler wurde die Unvorsichtigkeit begangen, in den Funksprüchen vom September 1937 von der bevorstehenden Änderung der Umkehrwalze zu reden. So war man denn in der polnischen Schlüsselstelle auf die Änderung vorbereitet und wunderte sich nicht, als die Gestalt der Zykeln vom 2. November 1937 im Kataloge nicht aufzufinden war. Dagegen konnte man natürlich nach wie vor mit Hilfe des Rostes die Steckerverbindungen sowie die rechte Walze und ihre Position bestimmen.

Unbekannt blieben nur die linke und mittlere Walze sowie ihre Positionen. Das ergab $2 \times 26 \times 26 = 1352$ mögliche Fälle und jeder dieser Fälle bestimmte eine Umkehrwalze.

Durch Vergleich dieser 1352 Umkehrwalzen in zwei verschiedenen Tagen konnte leicht die richtige Umkehrwalze ermittelt werden.

21. Neue Chiffrierwalzen

Im September 1937 bildete sich ein neues Funknetz, nämlich das Funknetz des Sicherheitsdienstes, einer politischen Organisation, von der noch später die Rede sein wird. Das Schlüsselverfahren war in diesem Netze im Grossen und Ganzen das-

selbe, wie in der Armee, jedoch wurden gewisse Neuerungen nicht gleichzeitig, sondern mit einer bestimmten Verspätung eingeführt. So z.B. wurde am 15 September 1938 das Schlüsselverfahren im Heere und in der Luftwaffe vollständig umgeschaltet, dagegen blieb es im Sicherheitsdienst noch mehrere Monate lang unverändert, ein grober Fehler, der sich sofort rächen sollte. Denn bereits drei Monate später wurden, diesmal gleichzeitig in allen Netzen, zwei neue Chiffrierwalzen, die Walzen IV und V eingeführt. Da in diesem Augenblicke das Netz des Sicherheitsdienstes sich noch des alten Verfahrens bediente, konnten die Schaltungen dieser Walzen in ähnlicher Weise gefunden werden, wie die Schaltungen der Umkehrwalze B. Es erübrigt sich wohl, in Einzelheiten einzugehen, es möge nur angedeutet werden, dass man sich hierbei zweier Tage, in denen Drehung der mittleren Walze eintrat, bediente. Wäre im Sicherheitsdienst das neue Chiffrierverfahren früher eingeführt werden, so hätte man wohl kaum die Schaltungen der Walzen IV und V auf kryptologischem Wege erhalten.

22. Änderung des Chiffriersystems

Dank der beschriebenen Methoden konnten bis September 1938 tagtäglich sämtliche Netze d.h. Heer, Luftwaffe, Sicherheitsdienst, Marine (von der noch weiter unten die Rede sein wird) in oft unglaublich kurzer Zeit gelöst werden.

Die Sachlage änderte sich jedoch vollkommen, als am 15. September 1938 ein neues Chiffrierverfahren eingeführt wurde und hierdurch die bisherigen Errungenschaften polnischer Kryptologen auf diesem Gebiete ernsthaft bedroht wurden.

Das neue Schlüsselverfahren beruhte darauf, dass die Grundstellung nicht mehr eine und dieselbe war für sämtliche Sprüche eines Tages, sondern von Spruch zu Spruch wechselte.

Wir wollen das neue Schlüsselverfahren an einem Beispiele erläutern. Der Schlüssler wählt sich zwei Buchstabentripel, z.B. SKR WTC, stellt die Maschine auf SKR ein und schlüsselt die Buchstaben WTC zweimal hintereinander (wie bisher), wobei etwa die sechs Buchstaben KFDLSF erhalten möge.

Die Grundstellung SKR wird unverschlüsselt in den Kopf des Spruches, die sechs Buchstaben KFD LSF am Anfang des Spruches eingesetzt, und der Spruch selbst wird von der Stellung WTC aus verschlüsselt (also so wie bisher). Dass das neue Verfahren gerade so, wie beschrieben, und nicht anders war, erfuhr man dadurch, dass bereits am Vortage der Systemänderung einige Schlüssler sich des neuen Verfahrens bedienten, was natürlich ein grober Fehler war.

23. Auffindung der Walzenlage

Da bei dem neuen System die Spruchschlüssel nicht mehr von ein- und derselben Position aus verschlüsselt werden, so wurde die Zykelntheorie und die darauf aufgebauten Methoden der Spruchschlüssels, des Rostes und des Zyklometers hinfällig.

Man liess jedoch die Arme nicht hängen, sondern schritt zur Untersuchung des neuen Verfahrens. Als erstes stellte man fest, dass wenn das Spruchmaterial innerhalb eines Tages und eines Netzes genugend umfangreich war, man von Zeit zu Zeit auf Paare von Grundstellungen traf, deren erste und zweite Buchstabe identisch, und deren dritte Buchstaben im Alphabet nebeneinander oder fast nebeneinander

standen, wie etwa TKP und TKR. Wenn dann zufälligerweise auch in den Spruchschlüsseln gleiche Buchstaben an entsprechenden Stellen auftraten, so konnte man hieraus bisweilen schlussfolgern, welche Walzen sich recht oder in der Mitte befinden. Wir wollen die verschiedenen Möglichkeiten an einigen Beispiele klarmachen.

1) Angenommen, wir hätten zwei Sprüche mit folgenden Schlüsseln gefunden:

Grundstellung	Spruchschlüssel
TKP	ANV CKB
TKR	VTS JQM

In diesem Fall ist sicher, dass zwischen Buchstaben P und R eine Drehung der mittleren Walze stattfindet, d.h. dass rechts sich die Walze I befindet, da diese und nur diese eine Drehung zwischen Q und R hervorruft. Im entgegengesetzten Falle würden den gleichen Buchstaben V auch gleiche Buchstaben B (oder J) entsprechen.

2)

Grundstellung	Spruchschlüssel
TKP	ANV CKB
TKR	VTS BQM

In diesem Falle ist es wenig wahrscheinlich, dass eine Drehung zwischen P und R eintritt, dass also rechts sich die Walze I befindet.

3) Auch Grundstellungen mit verschiedenen mittleren Buchstaben können Aufschlüsse über die Walzenlage bieten, wie folgendes Beispiel zeigt:

Grundstellung	Spruchstellung
TKP	ANV CKB
TLR	VTS JQM

Zwischen P und R kann keine Verschiebung der mittleren Walze eintreten, also ist die rechte Walze sicher verschieden von der Walze I.

4) Ja sogar aus Grundstellungen mit verschiedenen ersten Buchstaben lassen sich bisweilen Schlüsse über Walzenlage ziehen.

Grundstellung	Spruchschlüssel
TJG	CWS PKR
UKG	CWT PLJ

In diesem Falle ist es wahrscheinlich, dass zwischen J und K sich die linke Walze gedreht hat, dass also in der Mitte sich die Walze IV befindet.

In anderen Fällen lassen sich ähnliche Schlüsse ziehen.

24. Bomben

Bereits wenige Tage nach Einführung des neuen Schlüsselverfahrens hatte man einen Plan gefasst, wie man die entstandenen Schwierigkeiten aus dem Wege schaffen könnte. Unser Ideengang war folgender:

Nehmen wir eine Anzahl von Sprüchen und schreiben deren Grundstellungen und Spruchschlüssel auf.

1.	K T L	WOC	D R B	7. G R A	F D R	YWD
2.	S V W	KKM	I Y S	8. MDO	OTW	YZW
3.	J O T	IWA	BWN	9. K J C	F S W	R S E
4.	E D C	D S P	L J C	10. S G F	T E Y	A S R
5.	G D K	WAV	WHA	11. A G H	M D F	R H F
6.	B W K	T C A	T O C	12. J B R	W L T	S O Q

Richten wir jetzt unsere Aufmerksamkeit auf den Spruch Nr. 3. In dessen Spruchschlüssel kommt der Buchstabe W zweimal im Abstande von 3 Buchstaben vor. Das bedeutet, dass in einer ganz bestimmten Position der Maschine der Buchstabe W einen uns unbekannten Buchstaben, sagen wir etwa X, ergeben und drei Positionen später derselbe Buchstabe W wieder denselben Buchstabe X ergeben würde. Nehmen wir nun noch an, der Buchstabe W werde durch Steckerverbindungen nicht berührt, eine Annahme, die bei 5 bis 8 Steckerverbindungen in 50% aller Fälle zutreffend ist.

Dann könnte man die richtige Position der Walzen ermitteln, dass in zwei Maschinen, deren Positionen sich um 3 unterscheiden, der Buchstabe W gleichzeitig getastet und daraufhin in beiden Maschinen die Walzen synchronisch gedreht werden. Jedesmal, wenn in beiden Maschinen gleichzeitig derselbe Buchstabe aufleuchtet, haben wir es mit einem Fall zu tun, der möglicherweise richtig ist und daher besonders untersucht werden muss.

Da jedoch solche Fälle allzu häufig auftreten würden, hilft man sich in der Weise, dass man nicht einen, sondern drei Sprüche, in deren Spruchschlüssel der Buchstabe W zweimal im Abstande von 3 Buchstaben vorkommt, benutzt. In unserem Beispiel wären es Sprüche Nr. 3, 5 und 8. Nur muss man sich natürlich nicht zweier, sondern sechs Maschinen bedienen. Es wäre aber in Wirklichkeit höchst umständlich und unzweckmässig, wollte man wirklich mit sechs einzelnen Maschinen manipulieren. Vielmehr man eine Maschine, Bombe genannt, die 6 Enigmen entsprach, elektrisch angetrieben wurde und jedesmal automatisch anhielt, wenn ein günstiger Fall vorlag. Es wurden in der polnischen Schlüsselstelle sechs solche Bomben montiert, für jede Walzenlage eine (denn die Walzen IV und V wurden erst später eingeführt), wobei jede Bombe alle möglichen 17 576 Fälle in 1½ Stunde bewältigte.

25. Die Netze

Die Bomben befanden sich noch im Bau, als bereits neue Änderungen eintraten. Am 15. Dezember 1938 wurden die Walzen IV und V eingeführt, die Anzahl der möglichen Walzenlagen also verzehnfacht, und zwei Wochen später die Zahl der Steckerverbindungen auf 7–10 erhöht. Durch diese Änderungen verloren die Bomben praktisch den grössten Teil ihrer Bedeutung, da die Lösung eines Tages zu viel Zeit beanspruchen würde. Es gelang zwar bisweilen, dank der früher angegebenen Methode die Walzenlage teilweise zu bestimmen, aber nur dann, wenn umfangreiches Material vorhanden war, was verhältnismässig selten eintrat. Auch war die Anwendbarkeit der Bomben durch die Steckerverbindungen eingeschränkt.

Man schuf daher bereits sehr früh eine neue Methode, die von der Zahl der Steckerverbindungen unabhängig war.

Zur Darlegung dieser neuen Methode müssen wir zunächst einen neuen Begriff, den der männlichen und weiblichen Positionen, einführen. Kehren wir noch einmal zu den auf Seite 106 angegebenen Sprüche zurück:

1.	K T L	W O C	D R B	7.	G R A	F D R	Y W D
2.	S V W	K K M	I Y S	8.	M D O	O T W	Y Z W
3.	J O T	I W A	B W N	9.	K J C	F S W	R S E
4.	E D C	D S P	L J C	10.	S G F	T E Y	A S R
5.	G D K	W A V	W H A	11.	A G H	M D F	R H F
6.	B W K	T C A	T O C	12.	J B R	W L T	S O Q

Ein Fall, wie im Spruchschlüssel Nr. 3, dass derselbe Buchstabe (in unserem Beispiel W) zweimal im Abstand von drei Buchstaben vorkommt, kann nicht in sämtlichen Positionen der Maschine eintreten. Vielmehr haben Rechnungen ergeben, dass solche Fälle in etwa 40% aller Positionen eintreten (genau genommen beträgt das Verhältnis 1 - (1/√e), wobei e die Basis der naturellen Logarithmen ist). Diese Positionen nennen wir weibliche Positionen, die übrigen heissen männliche Positionen. In unserem Beispiel gehören die sechs Spruche Nr. 3, 5, 6, 8, 9, 11 bestimmt weiblichen Positionen an, während von den übrigen Sprüchen nichts ausgesagt werden kann. Die Steckerverbindungen haben natürlich Einfluss auf die in den Spruchschlüsseln auftretenden Buchstaben, nicht aber auf das Geschlecht der Position (ob weiblich oder männlich).

Man konnte daher einen Katalog mit sämtlichen weiblichen Positionen anfertigen, und in diesem Kataloge nachsuchen, ob man nicht sechs weibliche Positionen findet, die in denselben Abständen auftreten, wie die Grundstellungen: JOU, GKD, BWK, MDR, KJD, AGK (dabei müssen auch eventuell Drehungen der mittleren wie auch linken Walze berücksichtigt werden).

Da dies jedoch praktisch unausführbar wäre, so ging man anders vor; man stellte die sogenannte Netze her: Für jede Walzenlage werden sämtliche weibliche Positionen auf 26 Bogen Papier, von denen jeder 26x26 Felder, und zwar in vierfacher Ausführung enthält, eingetragen. Die verschiedenen Bogen entsprechen den 26 Positionen der linken Chiffrierwalze, die 26x26 Felder der mittleren und rechten Walze. Der Grund der vierfachen Ausführung wird unten erklärt werden. Die Felder die den weiblichen Positionen entsprechen, werden durchlocht (daher der Name Netz).

Nun werden, um auf unseres Beispiel zurückzugehen, sechs von den 26 Bogen in einer Reihenfolge und in einer Lage, die den gegenseitigen Entfernungen der Grundstellungen entspricht, aufeinander gelegt. Wenn gleichzeitig in allen sechs Bogen an derselben Stelle ein Loch erscheint, so haben wir es mit einem möglicherweise richtigen Falle zu tun, der besonders geprüft werden muss. Um alle möglichen Fälle zu erschöpfen, müssen die Bogen der Reihe nach zyklisch vertauscht werden. Auf jedem Bogen befinden sich die 26x26 Felder in vierfacher Ausführung, weil die Bogen nicht direkt, sondern gegenseitig verschoben aufeinander gelegt werden. Die Erzielung des Ergebnisses ist von einem überaus sorgfältigen Aufeinanderlegen der Bogen in der richtigen Lage abhängig. Deshalb wurde stets vor Beginn der Arbeit auf einem besonderen Zettel, dem sogenanntem Menu, die Reihenfolge und gegenseitige Lage der Bogen festgelegt.

Die Kenntnis, welche Positionen weiblich und welche männlich sind, wurde den Katalogen zum Zyklometer entnommen, denn offenbar entsprechende weibliche Positionen denjenigen Substitutionen, in denen Zykeln vorkommen, die aus einem Buchstabe bestehen.

Das Prüfen der richtigen Fälle geschah auch mit Hilfe des Zyklometers. Da dies ziemlich zeitraubend war, trug man sich mit dem Gedanken, besondere Kataloge herzustellen, in denen nicht nur die weibliche Positionen, sondern auch alle Buchstaben, die in den eingliedrigen Zykeln vorkommen, eingetragen wären. Aber dieser Gedanke wurde erst später, und zwar von der englischen Schlüsselstelle, verwirklicht.

26. Die Warschauer Konferenz

In der Polnischen Schlüsselstelle wurden zwei Sätze von je 26 Netzen für zwei Walzenlagen mit der Hand angefertigt, und man überzeugte sich dass die Idee der Netze vollkommen brauchbar ist. Ganz anders jedoch stellte sich die Ausführung dieser Idee dar.

Während die weiblichen Positionen für die Walzenlagen I II III, I III II, …, III II I direkt von den Katalogen entnommen werden konnten, müsste man für die übrigen 54 Walzenlagen die weibliche Positionen erst ermitteln, entweder mittels des Zyklometers, was mehrere Jahre beansprucht hätte, oder mit Hilfe einer neuen kostspieligen Maschine, woran man zunächst noch nicht denken wollte. Ferner war das handmässige Perforieren bereits der beiden ersten Sätze von je 26 Netzen recht mühsam gewesen, so dass man für den Rest der Arbeit ebenfalls besondere Apparate benötigt haben wäre. Und schliesslich wäre, wenn schon alles fertig wäre, das Manipulieren mit den 60 Sätzen von Netzen, um die einzelnen Tage zu lösen, ein zahlreiches Hilfspersonal erfordern.

Da die polnische Schlüsselstelle nicht in der Lage war, all diese Schwierigkeiten selbst zu bewältigen, entschloss man sich, das Geheimnis der Enigma, das bisher sorgsam gehütet war, auch der französischen und englischen Schlüsselstellen anzuvertrauen.

Am 26. Juli trat in Warschau eine dreitägige Konferenz unter Teilnahme von Vertretern der französischen und englischen Schlüsselstelle in Sachen der Enigma zusammen. Es stellte sich heraus, dass weder unsere französischen noch englischen Fachgenossen die ersten Schwierigkeiten haben überwinden können. Die Walzenschaltungen waren ihnen unbekannt, mithin auch etwaige Auflösungsmethoden. Wir legten ihnen die Ergebnisse unserer siebenjährigen Arbeit, sowie die Schwierigkeiten, auf die wir zuletzt gestossen waren, vor. Von Seiten der Engländer wurde bereitwilligst Hilfe in der Ausführung der Netze für die 60 Walzenlagen versprochen.

27. Kriegsaufbruch. Vignolles

Ein Monat später brach der deutsch-polnische Krieg aus. Es gelang noch, den 25. August 1939, den Tag der allgemeinen Mobilmachung in Deutschland, zu lösen, als bereit die Evakuation begann. Die Bomben, Zyklometer, Enigmen, Netze, sämtliche Akten und Aufzeichnungen wurden mitgenommen, aber auf dem Wege zur rumänischen Grenze vernichtet. Einzig und allein zwei Enigmen wurden gerettet. In Bukarest nahm sich der drei Spezialisten von der Enigma die französische Botschaft an und schickte sie sofort nach Paris, wo sie gastfreundlich aufgenommen wurden. Einige Wochen später schuf der französische Generalstab in Vignolles, einem Schlösschen unweit Gretz, 30 km von der Hauptstadt entfernt, ein Büro, wo polnische Kryptologen samt Hilfspersonal unter Leitung von Oberstleutnant Langer versuchten, die in Polen unterbrochene Arbeit wiederaufzunehmen. Man begann wieder mühselig, wie bereits schon einmal in Warschau, die Netze mit der Hand zu fabrizieren, eine Arbeit, die wohl erst nach Jahren beendet worden wäre.

Jetzt aber begann die Warschauer Konferenz Früchte zu tragen. Es stellte sich heraus, dass in der Zwischenzeit die Engländer eine Maschine konstruiert hatten, die ihnen ermöglichte, die Netze für sämtliche 60 Walzenlagen in wenigen Wochen herzustellen. Aber Proben, die mit diesen Netzen in England angestellt wurden, gaben kein Ergebnis. Da glücklicherweise die Netze in zwei Exemplaren hergestellt waren, konnten uns die Engländer ein Exemplar zur Verfügung stellen, was sie auch freundlichst taten. Sobald diese Netze in Vignolles ankamen, begann eine angestrengte Arbeit, und bald waren zwei Tage, der 28.10.1939 und der 6.1.1940 gelöst werden würde.

Die Engländer haben ihre Arbeit glänzend organisiert. Sie verfügten über umfangreiches Spruchmaterial und zahlreiches Personal. Die Mehrzahl der gelösten Tage stammte von ihnen.

Auch in Vignolles wurde fieberhaft gearbeitet. Da es aber darauf ankam, möglichst viel Spruchmaterial zu lösen und zu lesen, um es im Generalstab auszuwerten, so sassen denn polnische Kryptologen tagaus tagein an den Enigmen und tasteten die Sprüche ab oder manipulierten mit den Netzen, um von Zeit zu Zeit auch einen Tag zu lösen und sich nicht ganz von den Engländer distanzieren zu lassen. Alles mechanische Arbeiten, wozu sicherlich Spezialisten nicht nötig waren. So ist es denn nicht zu verwundern, dass von polnischen Kryptologen keine wesentlichen Ergebnisse mehr erzielt wurden, sondern, dass der Schwerpunkt kryptologischer Untersuchungen sich nach London übertrug.

28. Methode Knox

Der englische Kryptolog Knox hatte bemerkt, dass die deutschen Schlüssler oft als Grundstellung diejenigen Buchstaben wählten, die nach Beendigung des Schlüsselns des vorhergehenden Spruches in den Fenstern der Maschine erscheinen. Besonders häufig trat dies in vielteiligen Sprüchen auf. Es genügte also in solchen Fällen von der Grundstellung die Länge des vorhergehenden Spruches zu subtrahieren, um den Spruchschlüssel des vorhergehenden Spruches (unverschlüsselt) zu erhalten. Erhielt man dabei charakteristische Schlüssel wie ASD, WER, OKL, … in mehreren Teilen eines vielteiligen Spruches, so war man sicher, dass der Schlüssler einen solchen Fehler begangen hat. Da bei der Subtraktion der Spruchlänge von der Grundstellung eventuelle Drehungen der mittleren und linken Walzen berücksichtigt werden müssen, so konnte man auf diese Weise teilweise die Walzenlage bestimmen und dadurch im glücklichen Falle die Arbeit des Auflösens von 60 auf 3 Walzenlagen herabsetzen. Wichtig war auch, dass mit Hilfe der Methode Knox die (unverschlüsselten) Spruchschlüssel einiger Sprüche bekannt waren.

Diese Methode hatte besonders während des norwegischen Feldzuges wertvolle Dienste geleistet, wo Tag auf Tag gelöst wurde, wobei sich überaus wichtiges und interessantes Material ergab.

29. Kataloge zu den Netzen

Inzwischen verwirklichten die Engländer noch eine Idee polnischer Kryptologen. Es wurde bereits erwähnt, dass das Verifizieren der mittels Netze erhaltenen möglichen Fälle mit Hilfe des Zyklometers ziemlich zeitraubend war. Mann musste jedesmal, wenn ein günstiger Fall vorlag, die Buchstaben, die den weiblichen Charakter der Position bestimmten, mit Hilfe des Zyklometers aufsuchen, und mit den Buchstaben der betreffenden Spruchschlüssel vergleichen. Man trug sich bereits in Polen mit dem Gedanken, Kataloge herzustellen, die die in Frage kommenden Buchstaben sämtlicher weiblicher Positionen enthalten sollten, jedoch technische Schwierigkeiten verhinderten die Ausführung dieser Idee. Jetzt wurde sie von den Engländer mit Hilfe derselben Maschine, die die Netze angefertigt hat, ein weiteres glänzendes Beispiel, wie fruchtbar sich die polnisch-französisch-englische Zusammenarbeit erwies. Dank der finanziellen und organisatorischen Möglichkeiten unseren Londoner Fachgenossen wurden unsere Pläne, die sonst wohl nie das Licht der Welt erblick hätten, ohne Rücksicht auf die Kosten und Schwierigkeiten in Wirklichkeit umgesetzt.

30. Methode Herivel

Ein anderer englischer Kryptolog machte die Entdeckung, dass einige von deutschen Schlüssler, wenn nach Mitternacht oder am Morgen die Enigma für betreffenden Tag einstellten, die Walzen zur Ringstellung nicht herausnahmen und nicht drehten, und die Grundstellung für den ersten Spruch des Tages die Buchstaben wählten, die sie in Fenstern der Maschine erblickten. Infolgedessen unterschied sich die Grundstellung dieses ersten Spruches nicht viel von der für diesen Tag festgestellten Ringstellung.

Durch Vergleich der Grundstellungen von Sprüchen, die von verschiedenen Schlüssler nachts oder in der frühen Morgenstunden chiffriert wurden, konnte man oft die Ringstellung genau oder mit grosser Annäherung ausfindig machen. Dank dieser Feststellung wurde die zur Lösung erforderliche Arbeit ganz ausserordentlich abgekürzt, sodass oft am frühen Morgen die Engländer bereits im Besitze des Schlüssels für den ganzen Tag waren.

Zu dieser Methode möge noch folgendes hinzugefügt werden. Als die Schaltungen der Walzen IV und V gefunden worden, konnte die Lage des Buchstabenringes für diese Walzen nicht eindeutig festgestellt werden. Es gab je 26 verschiedene Lagen, von denen die ersten besten ausgewählt wurden. Man war sich jedoch darüber im Klaren, dass diese Lagen mit den originalen Lagen in den Walzen nicht identisch waren. Nachdem eine grössere Anzahl von Tagen (vor der Entdeckung Herivels) gelöst war, erinnerte man sich daran, dass früher die drei die Ringstellung bildenden Buchstaben stets voneinander verschieden waren. Wenn dieses Merkmal auch jetzt bestehen sollte (was sehr wahrscheinlich war), es mussten die Lagen der Buchstabenringe in den Walzen IV und V einer gewissen Korrektur unterzogen werden. Diese Korrektur wurde gefunden und den Engländer sofort mitgeteilt. Erst durch diese Korrektur konnte das Verfahren Herivel richtig angewandt werden.

31. Drittes Schlüsselverfahren

Am 1. Mai 1940, vor Beginn der deutschen Offensive gegen Belgien und Holland wurde das Schlüsselverfahren nochmals geändert. Der Spruchschlüssel wurde nicht mehr zweimal, sondern nur einmal verschlüsselt. Im Kopf des Spruches werden jetzt sechs Buchstaben angegeben, die drei erste bedeuteten die Grundstellung, die drei folgenden den chiffrierten Spruchschlüssel.

Der Sachverhalt wurde dadurch geklärt, dass die deutschen Schlüssler wieder, wie schon einmal, die Unvorsichtigkeit begingen, bereits am Vorabend der Neueinführung eine Anzahl von Sprüchen nach dem neuen Verfahren zu schlüsseln. Dieser Tag, der 30. April 1940, wurde gelöst, nebenbei bemerkt von polnischen Kryptologen, und so stellte sich denn heraus, worauf das neue Verfahren beruhte.

Es war wieder ein sehr harter Schlag. Die Netze und die Kataloge zu den Netzen wurden völlig unbrauchbar, es blieben nur noch die Methoden Knox und Herivel bestehen. Mit Hilfe dieser Methoden versuchten die polnische Kryptologen, die vorübergehend von Vignolles nach Paris versetzt waren, wenigstens einen Tag zu lösen, jedoch vergeblich.

Die Engländer hatten mehr Erfolg. Sie verfügten über bedeutend umfangreicheres Material, und so gelang es ihnen, nach einer dreiwöchentlichen Pause wieder einen Tag, den 20. Mai 1940, zu lösen, und bald darauf fast sämtliche folgenden Tage.

Sie übersandten regelmässig die Schlüssel, und so sassen wieder Tag und Nacht die polnischen Spezialisten an den beiden aus Warschau stammenden Enigmen, um das überaus wertvolle Spruchmaterial lesen zu helfen. Nach der Evakuation von Paris wurde die Arbeit in La Ferté-St. Aubin fortgesetzt, wo ebenfalls Tag und Nacht gearbeitet wurde und erst unmittelbar vor dem Waffenstillstand wurde sie abgebrochen. Der letzte Tag, für die Engländer die Schlüssel übersandten, war der 16. Juni 1940.

32. Chronologische Übersicht über die Änderungen des Schlüsselverfahrens im Heer und in der Luftwaffe

<table>
<tr><td>15. Jul. 1928
1929
31. Mai 1930</td><td colspan="6">Enigma G mit Stöpselstellung</td></tr>
<tr><td>1. Jun. 1930
1931
1932
1933
1934
1935
31. Jan. 1936</td><td rowspan="9">Enigma M mit Steckerbrettverbindungen</td><td>Walzenlage ändert sich alle drei Monate.</td><td>Steckerverbindungen tauschen sechs Paar Buchstaben.</td><td rowspan="2">Umkehrwalze A</td><td rowspan="3">Walzen I–III</td><td>Erstes Schlüsselverfahren. Grundstellung dieselbe für alle Sprüche. Spruchschlüssel zweimal verschlüsselt.</td></tr>
<tr><td>1. Feb. 1936
30. Sep. 1936</td><td>Walzenlage ändert sich jeden Monat.</td><td rowspan="3">Steckerverbindungen tauschen 5–8 Paar Buchstaben.</td></tr>
<tr><td>1. Okt. 1936
1. Nov. 1937</td><td>Walzenlage ändert sich täglich.</td></tr>
<tr><td>2. Nov. 1937
14. Sep. 1938</td><td rowspan="6">Umkehrwalze B</td></tr>
<tr><td>15. Sep. 1938
14. Dez. 1938</td><td rowspan="4">Walzen IV–V</td><td rowspan="3">Zweites Schlüsselverfahren. Grundstellung wechselt von Spruch zu Spruch. Spruchschlüssel zweimal verschlüsselt.</td></tr>
<tr><td>15. Dez. 1938
31. Dez. 1938</td><td rowspan="2">Steckerverbindungen tauschen 7–10 Paar Buchstaben.</td></tr>
<tr><td>1. Jan. 1939
31. Dez. 1939</td></tr>
<tr><td>1. Jan. 1940
30. Apr. 1940</td><td rowspan="2">Steckerverbindungen tauschen zehn Paar Buchstaben.</td></tr>
<tr><td>1. Mai 1940</td><td>Drittes Schlüsselverfahren. Grundstellung wechselt von Spruch zu Spruch. Spruchschlüssel einmal verschlüsselt.</td></tr>
</table>

33. Das Funknetz des Sicherheitsdienstes

Das Funknetz des Sicherheitsdienstes wurde bereits auf Seite 104 1erwähnt. Da dieses Netz, abgekürzt S.D. genannt, sich eines Schlüsselverfahrens bedient, dass in Einzelheiten von demjenigen des Heeres und der Luftwaffe abwich, so möge es hier etwas genauer beschrieben werden.

Bis 1. August 1939 bestand der Hauptunterschied zwischen dem Verfahren S.D. und den übrigen Verfahren darin, dass der Text der Sprüche mit dreistelligen Satzbuchgruppen vermischt war. Das Satzbuch diente anscheinend vor allem dazu, den Inhalt der Sprüche abzukürzen. Es war nicht besonders schwer, dieses Satzbuch zu lösen, doch wurde es alle paar Monate geändert und durch ein umfangreicheres ersetzt, sodass man die Arbeit stets aufs Neue beginnen musste.

Der Spruchschlüssel wurde wie im Heer und in der Luftflotte zweimal verschlüsselt, doch wurde er nicht immer an Anfang, sondern bisweilen auch an anderen Stellen eingesetzt. Ausserdem wurden während der Dauer von mehreren Monaten die Buchstaben der Spruchschlüssel noch mittels eines Tauschalphabets überschlüsselt. Die Gültigkeit eines Tauschalphabets betrug jeweils einen Monat.

Die Spruchschlüsselwurden sehr sorgfältig gewählt, sodass nur die Methode ungleicher Buchstaben und der Zyklometer angewandt werden konnten.

Sprüche, die mit den Buchstaben AN begannen, kamen nicht vor. Um also Grund- und Ringstellung gesondert zu finden, musste man von anderen charakteristischen Eigenschaften des Spruchinhalts ausgehen. Es stellte sich heraus, dass in sehr vielen Sprüche der vierte und fünfte oder der fünfte und sechste Buchstabe QY lautete, und man also mit diesen Buchstaben ebenso vorgehen konnte, wie im Heer mit den Buchstaben AN.

Ihrem Inhalt nach waren die Sprüche von grosser Wichtigkeit. Es waren sehr oft Berichte von ausserhalb Deutschland sich befindenden Agenten des Sicherheitsdienstes, und man konnte sich mit ihrer Hilfe ein Bild über die weit verzweigte Organisation des deutschen Spionagedienstes machen.

Das am 15. September 1938 im Heer und in der Luftflotte eingeführte zweite Schlüsselverfahren wurde im S.D. Netz nicht beachtet. Es wurde nach wie vor nach dem alten System geschlüsselt, nur wurde durch Einsetzen in den Kopf der Sprüche einer dreistelligen Buchstabengruppe das neue System vorgetäuscht. Dagegen trat am 1. August 1939 eine völlige Änderung des Verfahrens ein, dass man nicht enträtseln konnte. Seit dieser Zeit blieben die Sprüche des S.D. Netzes unauflösbar. Der letzte gelöste Tag war der 31. Juni 1939.

Aus Mangel an Unterlagen kann eine chronologische Zusammenstellung der in S.D. Funknetz eingetretenen Veränderungen der verschiedenen Schlüsselmittel wie Satzbücher, Tauschalphabete, Einsatzstellen für Spruchschlüssel, usw. nicht angegeben werden.

34. Die Schlüsselverfahren der deutschen Kriegsmarine vor Einführung der Enigma

Die Schlüsselverfahren, die Deutsche Kriegsmarine anwandte, unterschieden sich, obwohl seit dem Jahre 1934 auch dort dieselbe Enigma wie im Heere benutzt wurde, sehr wesentlich von denen des Heeres und der Luftwaffe. Es wäre daher unzweckmässig gewesen, wollte man die Ergebnisse, die auf diesem Gebiet erzielt wurden, chronologisch zwischen die übrigen Arbeiten einflechten. Sie mögen jetzt am Ende dieser Skizze zusammengestellt werden.

Die im Funkverkehr der deutschen Kriegsmarine vorkommenden Spruche werden stets verschlüsselt in zwei-, drei- oder vierstelligen Buchstabengruppen angegeben, wobei Teilgruppen (z.B. am Ende des Spruches) nicht vorkommen. Hauptsächlich wurde die vierstellige Chiffre benutzt und nur dieser wurde in der polnischen Schlüsselstelle bearbeitet.

Die in den Jahren 1926–1927 angewandten vierstelligen Chiffres waren stets überschlüsselte Satzbücher. Die erste und letzte Gruppe eines jeden Spruches waren Blind- oder Kenngruppen. Die übrigen Gruppen waren verschlüsselte Codegruppen. Weder die Überschlüsselung noch die Satzbücher konnten gelöst werden.

In den Jahren 1926–1927 wurden zwei vierstellige Chiffres angewandt. Einer von ihnen war ein gewöhnliches Satzbuch ohne weitere Überschlüsselung. Dieses Satzbuch wurde im Jahre 1933 gelösst. Die Codegruppen bestanden ausschliesslich aus 18 Buchstaben:

A B E F G I K L N O P S T U W X Y Z

Das Satzbuch war sehr umfangreich und besass wahrscheinlich über 90 000 Codegruppen, von denen für ungefähr 10 000 die Bedeutungen gefunden worden konnten[1].

35. Die Marine-Chiffriermaschine mit 29 Tasten

In der Zeit vom Januar 1926 bis September 1934 wurde von der deutschen Kriegsmarine eine Chiffriermaschine zum Verschlüsseln von Funksprüchen benutzt. Die Maschine war eine Enigma-Chiffriermaschine, die sich jedoch in folgenden Einzelheiten von der im Heere gebrauchten Enigma-Chiffriermaschine unterschied:

1) Die Maschine besass 29 Tasten und ebensoviel Glühlampen für die 29 Buchstaben des deutschen Alphabets mit den Umlauten.
2) Beim Niederdrücken der Taste X leuchtete stets die Glühlampe X auf.
3) Weder Stöpselstellungen noch Steckerverbindungen waren vorhanden.
4) Die Schaltung der Eintrittswalze war folgende:

A	Ä	B	C	D	E	F	G	H	I	J	K	L	M	N	O	Ö	P	Q	R	S	T	U	Ü	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

5) Die Zahl der Chiffrierwalzen betrug fünf, von denen gleichzeitig drei in die Maschine eingesetzt wurden.
6) Die Zähne der Chiffrierwalzen waren nicht mit den Ringen, sondern mit der Walzeneinfassung verbunden.
7) Die Umkehrwalze war beweglich; man konnte sie wie jede Chiffrierwalze einstellen.
8) Die Ringe besassen Zahlen von 1–28.

Obwohl diese Chiffriermaschine schon ab 1926 im Gebrauch war, gelang es sie erst an Hand der Sprüche aus den Jahren 1931–1934 zu rekonstruieren. In dieser Zeit wurden die Sprüche auf dieselbe Weise wie im Heere verschlüsselt, das

[1] Der Zweite der beiden vierstelligen Chiffres war, wie sich herausstellte, mittels einer Chiffriermaschine verschlüsselt. Er wird auf Seite 116 beschrieben.

heisst also, dass für jeden Tag eine Grundstellung festgestellt wurde, bei welcher der aus 3 Buchstaben bestehendes Spruchschlüssel zweimal verschlüsselt wurde. Die so erhaltenen zwei dreistellige Buchstabengruppen wurden durch Voransetzung je eines blinden Buchstabe in vierstellige Gruppen verwandelt, von denen die erste am Anfang und die zweite am Ende des Spruches eingesetzt wurde. Auf diese beiden Gruppen konnte auf dieselbe Weise wie im Heer die Zykelntheorie angewandt werden.

Das Bilden der Substitutionen A_1A_4, A_2A_5 und A_3A_6 war jedoch dadurch erschwert, dass das Spruchmaterial unzureichend war. Umso schwerer war es die Spruchschlüssel selbst zu erhalten. Erst im Jahre 1933 wurde dies erheblich leichter, als sich herausstellte, dass die Spruchschlüssel, die einem Verzeichnis entnommen wurden, keine Umlautbuchstaben enthielten. Man konnte jetzt die Zykeln so einander zu ordnen, dass Buchstaben die in ersten Gruppe der verschlüsselten Spruchschlüssel nicht vorkamen, auf Umlaute fielen.

Eine weitere Schwierigkeit beruhte in der Unkenntnis der Schalung der Eintrittswalze. Sie wurde jedoch glücklich erraten ebenso wie dies bei der Heeresmaschine geschehen war. Man setzte dabei voraus, dass keine Steckerverbindungen vorhanden sind, was sich als richtig ergab. Im entgegengesetzten Fall wäre die Rekonstruktion der Maschine wahrscheinlich gescheitert. Und so fand man denn, ebenso wie im Heer, die Walzenschaltungen.

Jetzt kehrte man zu den Sprüchen aus früheren Jahren zurück. Im Jahre 1936 wurden innerhalb von Zeitabschnitten, die mehrere Tage umfassten, sämtliche Sprüche von ein- und derselben Position der Walzen ausgehend (also andere wie im Heere) verschlüsselt. Um den Spruchinhalt in einem dieser Zeitabschnitte zu finden, ging man folgendermassen vor:

Man fand zwei Sprüche, die allem Anschein nach denselben Spruchinhalt besassen, wobei jedoch in einem Fall vom Schlüssler ein Buchstabe ausgelassen worden war. Die entsprechenden Buchstaben beider Sprüche mussten daher, nacheinander getastet, denselben Klartext liefern. Mit Hilfe des Rostes erhielt man die Position der rechten Walze und hierauf ohne besondere Schwierigkeiten die Positionen der übrigen Walzen. Es stellte sich heraus, dass Spruchinhalt nochmals mittels eines Satzbuches verschlüsselt war, desselben, der gleichzeitig auch ohne Maschinenverschlüsselung angewandt wurde, und der bereits teilweise gelöst war; es war der schon erwähnte, die 18 Buchstaben ABEFGIKLNOPSTUWXYZ enthaltende vierstellige Code. Ausser diesem einen Zeitabschnitt wurden andere Zeitabschnitte nicht gelöst. Man stellte nur fest, dass die Walzenlage, Stellung der Umkehrwalze, Ringstellung und Spruchstellung (Grundstellung gab es bei diesem Verfahren nicht) in unregelmässigen Zeitabschnitten, die 3–15 Tage umfassten, verändert wurden.

Am 1. Januar 1927 wurde zwar nicht das Schlüsselvefahren, wohl aber das Satzbuch durch ein neues ersetzt. Man konnte jetzt die Schlüssel auf folgende Weise finden: In einer ganzen Reihe von Sprüchen vermutete man am Ende stets eine und dieselbe Codegruppe, die „Fortsetzung folgt" bedeuten sollte. Da die Maschine die Eigenschaft besitzt, dass Klar- und (mit Ausnahme von X, das stets X ergibt), verschlüsselte Buchstaben stets voneinander verschieden sind, konnte man schliesslich diese Gruppe (unverschlüsselt) finden, und hierauf mittels des Rostverfahrens die Positionen der Walzen für einen Zeitabschnitt bestimmen. Es stellte sich heraus, dass das neue Satzbuch sämtliche 29 Buchstaben einschliesslich der Umlaute enthielt, es konnte jedoch aus Zeitmangel nicht gelöst werden.

Am 1. Januar 1929 trat eine Änderung, diesmal des Schlüsselverfahrens selbst ein. Sie beruhte darauf, dass jetzt jeder Spruch seine eigene Spruchstellung besass, die mittels der am Anfang und Ende jeden Spruches stehenden Kenngruppen auf eine uns nicht näher bekannte Weise angegeben wurde.

Am 1. Mai 1931 trat eine erneute Änderung des Schlüsselverfahrens ein, die darauf beruhte, dass jetzt der Spruchschlüssel ebenso geschlüsselt wurde wie im Heere. Gerade dadurch gelang es ja die Walzenschaltungen zu rekonstruieren.

Es kam jetzt noch darauf an, den Spruchinhalt selbst zu finden. Man vermutete zunächst als Inhalt Satzbuchgruppen, aber nach mehreren Monaten angestrengter vergeblicher Arbeit stellte es sich zufällig heraus, dass der Inhalt aus Klartext (ähnlich wie im Heere) bestand. Das Schlüsselverfahren war, wie bereits erwähnt wurde, grundsätzlich dasselbe wie im Heere und in der Luftwaffe. Doch wurde die sogenannte „innere" Maschinenstellung, d.h. Walzenlage, Stellung der Umkehrwalze, und Ringstellung so wie bisher in unregelmässigen Zeitabständen geändert, während die Grundstellung täglich geändert wurde.

Die Spruchschlüssel wurden einem Verzeichnis entnommen. Sei es, dass dies Verzeichnis nicht sehr umfassend war oder sei es, dass die Schlüssler vorwiegend dieselben Spruchschlüssel aus dem Verzeichnis wählten, jedenfalls wiederholten sich dieselben oft, sodass eine Statistik angefertigt werden konnte die es erlaubte aus den Substitutionen A_1A_4, A_2A_5, A_3A_6 die (unverschlüsselten) Spruchschlüssel selbst zu finden, wobei auch das Nichtvorkommen der Umlaute in den Spruchschlüssel behilflich war.

Das Zyklometer konnte nicht angewandt werden, denn die Kataloge zu diesem müssten

$$60 \times 28^4 = 36\,879\,360$$

Positionen umfassen, was wohl kaum ausführbar wäre. So wurde denn die Position der rechten Walze mittels des Rostes festgestellt, was mühelos geschah, da keine Steckerverbindungen vorhanden waren, während die Position der übrigen Walzen mit Hilfe einer Kartothek, ähnlich der Katalogen F im Heere und in der Luftflotte, bestimmt wurde, nur war diese Kartothek umfangreicher, denn sie enthielt

$$28^3 = 21\,952$$

Positionen.

Der Spruchinhalt selbst war so kurz wie möglich gefasst. Es kamen in ihm Wortkürzungen aller Art vor. Die zweiten und weiteren Teile eines mehrteiligen Spruches begannen stets mit den Buchstaben FORT (Abkürzung für Fortsetzung). Um Grundstellung und Ringstellung gesondert zu finden, ging man von diesen Buchstaben FORT aus, so wie man im Heer und in der Luftflotte von den Buchstaben AN und im S.D. von den Buchstaben QY ausging.

36. Die Anwendung in der deutschen Kriegsmarine der Enigma-Chiffriermaschine mit 26 Tasten.

Vom 1. Oktober 1934 ab wurde in der deutschen Kriegsmarine dieselbe Enigma-Chiffriermaschine wie im Heere angewandt. Das Chiffrierverfahren blieb dasselbe wie bisher, mit dem Unterschied, dass jetzt die Steckerverbindungen (stets

6 Paar) hinzutraten, die gleich der Grundstellung täglich geändert wurden. In der Zeit bis zum 15. November 1936 wurden ausserdem in der deutschen Kriegsmarine zwei zusätzliche Chiffrierwalzen vorhanden waren, von denen drei gleichzeitig in die Maschine eingesetzt wurden.

Mit Hilfe der für das Heer hergestellten Kataloge zum Zyklometer konnte nur ein kleiner Teil (etwa ein Zehntel) der Tage bis zum 15. November 1936 gelöst werden. Dies genügte nicht um ein Spruchschlüsselverzeichnis herstellen zu können. Erst als am 16. November 1936 die beiden Zusatzwalzen zurückgezogen wurden und nur die drei Walzen I, II, III übrig blieben, konnte ein entsprechendes Spruchschlüsselverzeichnis hergestellt werden, mit Hilfe dessen man nachträglich die Spruchschlüssel in den Tagen vor dem 16. November auffinden konnte. Hinterher mittels der Rostmethode wurden dann die Schaltungen der beiden Zusatzwalzen errechnet. Man nannte sie IVM und VM zum Unterschied von den später im Heer und in der Luftflotte gebrauchten Walzen IV und V.

Für wichtigere Sprüche gab es ausser dem allgemeinen noch einen Offiziers- und einen Stabs- (oder Admirals-) Schlüssel. Der Offizierschlüssel wurde wie folgt angewandt: Zunächst wurde der gewählte Spruchschlüssel bei der Grundstellung „Allgemein" zweimal verschlüsselt und die beiden so erhaltenen dreistellige Buchstabengruppen nach Voransetzung eines vierten Füllbuchstaben wie üblich als erste und letzte Gruppe in den Spruch eingesetzt. Hierauf jedoch wurde der gewählte Spruchschlüssel noch einmal bei der Grundstellung „Offizier" verschlüsselt und das Ergebnis (und nicht der Spruchschlüssel selbst) diente zur Schlüsselung des eigentlichen Spruchinhaltes.

Wie der Stabsschlüssel angewandt wurde ist nicht bekannt. Am 1. Mai 1937 trat eine Änderung des Schlüsselverfahrens ein, die darauf beruhte, dass der Spruchschlüssel nicht mehr mittels der Maschine selbst, sondern auf eine andere, ziemlich komplizierte Weise verschlüsselt wurde. Die Einzelheiten des neuen Schlüsselverfahrens wurden erst bekannt, als es in Jahre 1940 den Engländern gelang, in einem versunkenen deutschen U-Boot die Schlüsseleinleitung zu diesem Verfahren zu finden. Wir können dies Verfahren hier nicht ausführlicher beschreiben, sondern verweisen den Leser auf die photographische Abbildung der Schlüssel-anleitung.

Die Unkenntnis des neuen Schlüsselverfahrens hinderte uns nicht im Jahre 1937 eine Reihe von Ergebnissen zu erzielen, die hier mitgeteilt werden mögen.

Der Spruchschlüssel wird in jedem Spruch mittels der beiden ersten Gruppen angegeben, die zwecks Vermeidung von Fehlern am Ende des Spruches wiederholt werden. Der eigentliche Text also beginnt mit der dritten Gruppe. Mittels einer Methode die nach angegeben wird, gelang es den Textinhalt vieler Sprüche zwischen den 1. Mai und 8. Mai 1937 zu finden und dadurch die Walzenlage, Steckerverbindungen, sowie teilweise auch die Ringstellung zu rekonstruieren. Ein Vergleich mit den gelösten Tagen von Ende April 1937 ergab, dass die innere Einstellung am 1. Mai 1937 keiner Änderung unterlag, und dass sie in der Zeit vom 27. April bis 8. Mai dieselbe geblieben ist.

Ein Vergleich der Spruchschlüssel der gelösten Sprüche mit beiden ersten (oder letzten) Gruppen ergab folgendes:

Werden in sämtlichen gelösten Sprüchen eines Tages die beiden ersten Gruppen in vier nebeneinander stehende Buchstabenpaare geteilt und haben zwei Sprüche ein gemeinsames erstes, zweites oder drittes Buchstabenpaar, so haben sie auch einen gemeinsamen ersten, zweiten oder dritten Spruchschlüsselbuchstaben. Die umgekehrte Behauptung ist nicht wahr. Gleichen Buchstaben können also sehr wohl verschiedene

Buchstabenpaare entsprechen. Auch entsprechen gleichen Buchstabenpaaren an verschiedenen Stellen im Allgemeinen verschiedenen Spruchschlüsselbuchstaben.

Bei der Änderung des Verfahrens am 1. Mai 1937 wurde ausser der Beibehaltung der inneren Einstellung noch ein zweiter grober Fehler durch die Schlüsselstelle der deutschen Kriegsmarine begangen. Da ein Kriegsschiff nicht rechtzeitig mit der neuen Schlüsselmethode versehen werden konnte, verkehrte es noch während der drei ersten Maitage 1937 nach dem alten Verfahren. Auf diese Weise konnte man am 2. und 3. Mai 1937 die Grundstellungen „Allgemein" und „Offizier" auffinden.

Von Seiten der Engländer wurde später folgendes festgestellt:

Werden die Spruchschlüssel der nach neuen Verfahren geschlüsselten Sprüche mittels der gefundenen Grundstellungen vom 2. Und 3. Mai entschlüsselt, so entsprechen denselben Buchstabenpaaren dieselben Buchstaben der entschlüsselten Spruchschlüssel, selbst wenn sie an verschiedenen Stellen auftreten.

Der Inhalt der Sprüche in der Periode vom 1. Bis 8. Mai 1937 wurde auf folgende Weise gefunden: Nahmen wir an wir hätten einen Spruch, der nach der Streichung der zwei ersten Gruppen folgendermassen beginnt:

VLPP WGKS WKUL QBOR

Weiterhin nehmen wir an, dass dieser Spruch die Fortsetzung eines anderen Spruches sei, der im Kopfe die Uhrzeit 1623 trägt. Nach unseren Erfahrungen muss dann Klartext dieses Spruches mit den Buchstaben

F O R T Y Q Z W E Y Y Q Z W E Y

beginnen (QZWE bedeutet 1623). Wir kennen also ein aus 16 Buchstaben bestehendes Fragment des Textes vor und nach der Verschlüsselung. Da in der Marine stets nur 6 Paar Steckerverbindungen auftreten, muss ein Teil der Buchstaben unverändert bleiben. Man macht nun verschieden Annahmen darüber, welche Buchstaben unverändert geblieben sind, und sucht diese Annahmen zu verifizieren, entweder direkt auf der Maschine, oder mittels des Rostes, oder mit Hilfe der Bogen Jeffreys, einer englischen Erfindung, die unseren Katalogen F entsprach. In allen Fällen ist die Arbeit sehr lang, so dass sie sich nur dann lohnt, wenn es wie in unserem Falle, darauf ankommt, ein neues Verfahren zu analysieren.

Den Engländern geling es noch einige Sprüche vom Jahre 1938 zu lösen. Hieraus ging hervor, dass jetzt die Umkehrwalze B im Gebrauch ist. Wahrscheinlich wurde sie in derselben Zeit wie im Heer eingeführt. Die Zahl der Steckerverbindungen blieb weiterhin 6 Paar.

Im Jahre 1940 fanden die Engländer in einem gesunkenen deutschen U-Boot zwei Chiffrierwalzen, die die Bezeichnung VI und VII trugen. Ob jetzt in der Marine die fünf Walzen I, II, III, VI und VII, oder sämtliche Walzen I bis VII angewandt werden, muss dahingestellt bleiben.

37. Chronologische Übersicht über die Anwendung von Enigma-Chiffriermaschinen in der deutschen Kriegsmarine

<table>
<tr><td>1926
1927
1928
1929
1930
April 1931</td><td colspan="2">Marine-Chiffriermaschine „Enigma“ (29 Tasten)</td><td colspan="2">5 Chiffrierwalzen</td><td colspan="2">Innere Einstellung: Walzenlage, Einstellung der Umkehrwalze und Ringstellung</td><td colspan="2">Innere Einstellung ändert in unregelmässigen Zeitabschnitten (3–15 Tage)</td><td colspan="2">Grundstellung täglich geändert</td><td>Die Grundstellung ändert gleichzeitig mit der inneren Einstellung</td><td></td></tr>
<tr><td>Mai 1931
1932
1933
Sept. 1934</td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td>Spruchschlüssel = Grundstellung</td><td></td></tr>
<tr><td>Okt. 1934
1935
15. Nov. 1936</td><td colspan="2">Chiffriermaschine „Enigma“ (26 Tasten)</td><td colspan="2">Umkehrwalze A</td><td>5 Ch.-Walzen
I, II, III, IVM und VM</td><td colspan="2"></td><td colspan="2">Grundstellung und Steckerverbindung ändern täglich</td><td>Das erste Schlüsselverfahren</td><td>29-Buchstabem Code</td><td>18-Buchstaben Code</td></tr>
<tr><td>16. Nov. 1936
Apr. 1937</td><td colspan="2"></td><td>3 Ch.-Walzen
I, II, III</td><td></td><td colspan="2"></td><td colspan="2"></td><td colspan="2">Das zweite Schlüsselverfahren</td><td></td><td></td></tr>
<tr><td>Mai 1937
Okt. 1937</td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td></td><td></td></tr>
<tr><td>Nov. 1937
1938</td><td colspan="2"></td><td colspan="2">Umkehrwalze B</td><td>5 Ch.-Walzen
I, II, III, VI und VII</td><td colspan="2"></td><td colspan="2">Das dritte Schlüsselverfahren</td><td colspan="2">Klartext</td><td></td></tr>
<tr><td>1939
1940</td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td></td></tr>
</table>

38. Teilnahme der drei Staaten an der Lösung der Enigma

I. Polen
Zykelntheorie
Substitutionentheorie
Schaltungen der Walzen I–III
und der Umkehrwalze A
Methode zur Auffindung der Eintrittswalze
Methode zur Auffindung
der Steckerverbindungen
Methode der charakteristischen Schlüssel
Statistische Methode
Methode ungleicher Buchstaben
Bestimmung der rechten Walze
Der Rost und Katalog F
Zyklometer (Maschine und Katalog)
Auffindung des Textes
Schaltungen der Umkehrwalze B
Schaltungen der Walzen IV und V
Analyse des zweiten Schlüsselverfahrens
Die Bomben
Die Netze (Projekt)
Kataloge zu den Netzen (Projekt)
Analyse des dritten Schlüsselverfahrens
Das Funknetz S.D.
Die Marine-Enigma mit 29 Tasten
Schaltungen der Walzen IVM und VM
Analyse der Marine-Schlüsselverfahren
vom 1. Mai 1937

II. England
Die Netze (Ausführung)
Kataloge zu den Netzen
(Ausführung)
Methode Jeffreys
Methode Knox
Methode Herivel
Walzen VI und VII
(im U-Boot gefunden)

III. Frankreich
Lieferung zweier wichtigen
Dokumente

Przekład oryginału na język polski

Spis treści

1. Wprowadzenie 181
2. Początki 182
3. Teoria cykli. 182
4. Dwa ważne dokumenty. 183
5. Teoria podstawień 183
6. Podstawienie E 185
7. Podstawienie S 186
8. Kilka liczb 187
9. Odtwarzanie klucza depeszy 188
10. Metoda charakterystycznych kluczy 188
11. Metoda statystyczna. 188
12. Metoda nierównych liter 189
13. Określanie prawego wirnika. 190
14. Ruszt 191
15. Katalog F 192
16. Cyklometr 192
17. Pozycja bazowa i pozycja pierścieni 193
18. Kilka spostrzeżeń 193
19. Nowe sieci. Ciągłe zmiany. 193
20. Reflektor B 194
21. Nowe wirniki. 194

22. Zmiana procedury szyfrowania 194

23. Określanie kolejności wirników 195

24. Bomby. 196

25. Płachty Zygalskiego 197

26. Konferencja w Warszawie 198

27. Wybuch wojny. Vignolles.. 198

28. Metoda Knoxa 199

29. Katalogi do płacht Zygalskiego 200

30. Metoda Herivela 200

31. Trzecia procedura szyfrowa 200

32. Chronologiczny przegląd zmian procedur szyfrowych w wojskach lądowych i Luftwaffe 202

33. Sieć radiowa służby bezpieczeństwa 202

34. Procedura szyfrowa niemieckiej marynarki przed wprowadzeniem Enigmy 203

35. Maszyna szyfrująca marynarki z 29 klawiszami 204

36. Użycie przez niemiecką Kriegsmarine maszyny szyfrującej z 26 klawiszami 206

37. Chronologiczny przegląd zastosowania maszyny szyfrującej Enigma w niemieckiej marynarce 208

38. Udział trzech państw w złamaniu Enigmy 209

1. Wprowadzenie[1]

Już kilka lat po zakończeniu wojny światowej niemieckie siły zbrojne zaczęły wykorzystywać maszynę szyfrującą Enigma do szyfrowania depesz przekazywanych drogą radiową.

Wydaje się, że nową procedurę szyfrowania jako pierwsza wprowadziła do użytku marynarka. W każdym razie wiadomo, że używała jej już w 1926 roku, podczas gdy użycie procedury w armii lądowej jest potwierdzone od 15 lipca 1928 roku.

W dniu 1 sierpnia 1935 roku Enigmę wprowadzono do użytku w Luftwaffe, od września 1937 roku wykorzystywała ją S.D., maszynę wykorzystywano także w policji.

W miarę poszerzania zakresu użycia Enigmy w niemieckich siłach zbrojnych inne metody szyfrowania, np. podwójna kaseta, zaczęły zanikać, tak że na długo przed wybuchem niemiecko-polskiej wojny w 1939 roku niemal wszelkie depesze przesyłane drogą radiową przez niemieckie instytucje o wojskowym lub choćby półwojskowym charakterze były szyfrowane Enigmą. Rozwiązanie tego szyfru było zatem dla sztabów Polski, Francji i Wielkiej Brytanii problemem o pierwszorzędnym znaczeniu. Z upływem czasu maszyna ulegała kilkakrotnym modyfikacjom. Przed wprowadzeniem maszyny typu M z łącznicą, która pozostaje w użyciu do chwili obecnej, od 15 lipca 1926 roku do 31 maja 1930 roku używano w wojskach lądowych Enigmy G, z tzw. wtyczkami. W dowództwach okręgów wojskowych przez pewien czas używano samopiszącej maszyny, zwanej Enigma II, która jednak jako niepraktyczna szybko wyszła z użytku. Niemiecka marynarka do września 1934 roku używała maszyny z 29 klawiszami zamiast 26 i dopiero w 1934 roku wdrożyła ten sam typ maszyny, który był używany w wojskach lądowych. Marynarka także w późniejszym okresie zachowała pewien poziom autonomii, m.in. korzystając z większej liczby wirników niż pozostałe formacje. Można jednak stwierdzić, że od października 1934 roku do dzisiaj wszystkie niemieckie siły zbrojne używają tego samego modelu maszyny, który w wojskach lądowych wszedł do użytku 1 lipca 1930 roku.

Poniżej zaprezentowano zarys działań Biura Szyfrów polskiego Sztabu Głównego, w wyniku których udało się nie tylko zrekonstruować opisany wcześniej model maszyny Enigma, lecz także opracować metody pozwalające odczytywać napływający materiał szyfrowy prawie na bieżąco, mimo wszelkich zmian i ulepszeń wprowadzanych nieustannie przez niemieckie służby kryptologiczne w celu zabezpieczenia łączności. Przedstawiono także znaczenie współpracy w tym obszarze pomiędzy sztabami Polski, Francji i Wielkiej Brytanii.

[1] W tłumaczeniu na język polski tłumacz usiłował zachować w możliwym stopniu styl niemieckiego oryginału, włączając w to wszelkie niedoskonałości wynikające z użycia przez autorów obcego języka.

2. Początki

Jeszcze wiele lat po utworzeniu polskiego Biura Szyfrów brak kadr nie pozwalał poświęcać uwagi materiałowi szyfrowemu napływającemu z niemieckiej marynarki. Dlatego pojawienie się Enigmy zostało odnotowane po raz pierwszy, dopiero gdy w 1928 roku zaczęły ją wykorzystywać wojska lądowe.

Wśród depesz napływających z niemieckich wojskowych stacji nadawczych pojawiły się takie, które nie były zaszyfrowane używanym do tej pory szyfrem podwójnej kasety, lecz innym, noszącym niewątpliwie podstawieniowy charakter. Zaczęto je analizować i ustalono bez trudu, że pierwsza szóstka znaków każdej depeszy ma szczególne znaczenie i stanowi klucz depeszy. Jednocześnie polski wywiad zdobył dokumenty, z których wynikało, że od 15 lipca 1928 roku w niemieckich wojskach lądowych wszedł w życie obok dotychczasowych także nowy szyfr oznaczony jako „Maschinenschlüsselverfahren Enigma G"; że w maszynie Enigma występuje element określany jako połączenia wtyczkowe (w późniejszych modelach znany jako łącznica) oraz że każda stacja otrzymuje regularnie pewną liczbę kluczy do szyfru, w których skład wchodzi trójka liczb nie większych niż 26.

Było oczywiste, że nowo odkryty szyfr był identyczny z procedurą wykorzystującą Enigmę. Aby ułatwić jego zbadanie polski sztab zakupił Enigmę typu handlowego, w której połączenia wirników były oczywiście odmienne od maszyny wykorzystywanej przez wojska lądowe. W toku późniejszych studiów okazało się, że różni się ona od wojskowego odpowiednika także pod wieloma innymi względami. Badania nowego szyfru nie posuwały się naprzód i po jakimś czasie zostały zarzucone.

3. Teoria cykli

Powrót do prac nastąpił w 1932 roku. Sześcioznakowe nagłówki depesz poddano ponownemu badaniu, które pozwoliło ustalić, co następuje: dla każdego dnia określa się pewną pozycję wirników, taką samą dla wszystkich szyfrantów. Do tego każdy szyfrant wybiera trzy dowolne litery, szyfruje je dwukrotnie po sobie, zaczynając od obowiązującej w danym dniu pozycji wspólnej, a następnie tak otrzymaną szóstkę liter wstawia na początku depeszy.

W ten sposób pomiędzy literami depeszy: 1 i 4, 2 i 5 oraz 3 i 6 powstają pewne relacje, które można badać w sposób czysto matematyczny i które są podstawą późniejszej rekonstrukcji Enigmy.

Postępuje się następująco: wybiera się dowolną depeszę, po czym zapisuje się jej pierwszą, a na prawo od niej czwartą literę. Potem należy znaleźć depeszę, w której ostatnio zapisany znak występuje jako pierwszy, i zapisać ten znak na prawo od poprzednich. Takie działanie powtarzamy aż powrócimy do litery zapisanej jako pierwsza. Wynik działania określamy jako cykl. Można udowodnić następujące twierdzenia:

1. Cykle tej samej długości występują zawsze w liczbie parzystej.

2. Znaki jednego cyklu są wywoływane przez znaki stanowiące elementy innego cyklu o tej samej długości.

3. Jeśli znak X jest wywoływany przez znak Y, to znak stojący na prawo od X jest wywoływany przez znak stojący na lewo od Y.

Te trzy twierdzenia stanowiły częściowe rozwiązanie zadania rekonstrukcji kluczy depeszy i problem zostałby całkowicie rozwiązany, gdyby w tym momencie nie pojawiła się pomoc w postaci dwóch dokumentów, które skierowały prace na inne tory.

4. Dwa ważne dokumenty

W tym czasie polskie Biuro Szyfrów weszło w posiadanie dwóch dokumentów o nadzwyczajnym znaczeniu. Pierwszy z nich nosił tytuł *Instrukcja obsługi szyfru maszynowego*, drugi zaś zawierał tzw. klucze dnia na miesiące październik i grudzień 1931 roku. Polski wywiad otrzymał wspomniane dokumenty z francuskiego sztabu generalnego, który zdobył je kanałami wywiadowczymi. Należy podkreślić, że posiadanie dokumentów, a zwłaszcza klucza dziennego, w rozstrzygający sposób wpłynęło na postęp prac. Bez nich rozwiązanie szyfru Enigmy opóźniłoby się co najmniej o lata. Jednocześnie należy zauważyć, że ani służbom francuskim, ani angielskim nie udało się złamać szyfru, mimo że obie dysponowały opisanymi dokumentami. Poniżej opisano metodę, która zapewne także doprowadziłaby do celu, także bez wspomnianych dokumentów.

Z pierwszego z wymienionych dokumentów wynikało, że od 1 lipca 1930 roku Enigma z połączeniami wtyczkowymi została zastąpiona przez nowy model z łącznicą. Następnie ustalono, że:

1. Maszyna zawiera 3 wirniki szyfrujące, których kolejność może być zmieniana. Zmiana kolejności wirników następuje co trzy miesiące.

2. Reflektor jest nieruchomy (w przeciwieństwie do modelu handlowego).

3. Wirniki są wyposażone w pierścień o opisie literowym lub liczbowym. Zmiana położenia pierścieni następuje codziennie.

4. Łącznica zamienia miejscami 6 par znaków. Zmiana połączeń łącznicy następuje codziennie.

5. Pozycja, od której rozpoczyna się szyfrowanie klucza depeszy, jest określana mianem pozycji bazowej. Zmiana pozycji bazowej następuje codziennie.

Drugi dokument zawierał klucze dnia, tj. kolejność wirników, pozycję bazową, ustawienia pierścieni oraz połączenia łącznicy na dwa miesiące.

5. Teoria podstawień

Przechodzimy obecnie do rozwiązania głównego problemu, tj. do rekonstrukcji połączeń wirników. W tym celu posłużyliśmy się teorią matematyczną, tzw. teorią podstawień, która nie została zaprezentowana w szczegółach, gdyż założono jej znajomość u czytelnika. Oczywiście nie można sądzić, że znajomość kilku twierdzeń tej teorii była wystarczająca do osiągnięcia wyniku. Przeciwnie, na drodze do celu należało pokonać wiele przeszkód. Poniżej prezentujemy główny tok naszego rozumowania. Szyfr Enigmy jest szyfrem podstawieniowym, tzn. że maszyna w każdym położeniu wirników zastępuje jedną literę alfabetu inną. Określamy podstawienie

obowiązujące w przewidzianej na dany dzień pozycji bazowej jako A_1, w kolejnej pozycji jako A_2 itd., aż do A_6.

Jeżeli dysponuje się wystarczającą liczbą depesz (średnio ok. 80), można wykorzystać teorię podstawień dla wyznaczenia iloczynów A_1A_4, A_2A_5, A_3A_6, które od tego momentu można uznać za znane. Oznaczmy dalej:

S podstawienie generowane przez łącznicę
C_γ " " " prawy wirnik
C_β " " " środkowy wirnik
C_α " " " lewy wirnik
U podstawienie generowane przez reflektor
E " " " walec wejściowy
Q = (1, 2, 3, 4, 5, 6, ..., 24, 25, 26).

Gdy środkowy wirnik nie porusza się w trakcie szyfrowania klucza depeszy, co jest prawdopodobne i co zakłada się w dalszych rozważaniach, to podstawienia od A_1 do A_6 mogą zostać przedstawione w następującej formie:

$$A_1 = S\ E\ C\gamma C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1} C\gamma^{-1} E^{-1} S^{-1}$$
$$A_2 = S\ E\ Q\ C\gamma Q^{-1} C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1} Q C\gamma^{-1} Q^{-1} E^{-1} S^{-1}$$
$$A_3 = S\ E\ Q^2\ C\gamma Q^{-2} C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1} Q^2 C\gamma^{-1} Q^{-2} E^{-1} S^{-1}$$
. . . . . .
$$A_6 = S\ E\ Q^5\ C\gamma Q^{-5} C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1} Q^5 C\gamma^{-1} Q^{-5} E^{-1} S^{-1}.$$

Pierwszym problemem, który należy przezwyciężyć, jest to, że nieznane są zarówno lewe, jak i prawe strony równań. Znane są wyłącznie iloczyny A_1A_4, A_2A_5, A_3A_6. Teoria cykli wskazuje jednak, że podstawienie A_1 w większości przypadków przyjmuje nie więcej niż sto postaci, a każda postać A_1 jednoznacznie określa podstawienie A_4. To samo zachodzi dla A_2 i A_5 oraz A_3 i A_6. Można zatem sobie wyobrazić, że znamy wszystkie postacie A_1 do A_6. W ten sposób możemy uznać pierwszą trudność za przezwyciężoną, choć za cenę znacznego wzrostu pracochłonności, w dalszych bowiem operacjach musimy uwzględniać wszystkie możliwe postaci A_1 do A_6.

Drugi problem jest jeszcze poważniejszy. Mimo największych wysiłków, które na gruncie teoretycznym można by czynić przez lata już po zrekonstruowaniu połączeń wirników, nie udało się w żaden sposób rozwiązać powyższego układu równań, przy czym podstawowym problemem było podstawienie S, generowane przez łącznicę. W końcu znaleziono metodę, która doprowadziłaby do celu, zakładała ona jednak znajomość podstawień A_1 do A_6 (a nie wyłącznie ich iloczynów A_1A_4, A_2A_5, A_3A_6), znajomość podstawienia E, a ponadto dostępność obszernego materiału szyfrowego.

Tak więc druga i główna trudność w drodze do rozwiązania Enigmy została w końcu przezwyciężona dzięki dokumentom przekazanym przez francuski sztab główny, które zawierały ustawienia łącznicy na dwa miesiące.

Trzeci problem sprowadzał się do nieznajomości podstawienia E. Wydaje się, że właśnie na nim załamały się wysiłki brytyjskich kryptologów. Późniejsze badania polskiego Biura Szyfrów dowiodły, że podstawienie E może zostać wyznaczone analitycznie (pod warunkiem znajomości podstawienia S), w rzeczywistości jednak znaleziono je metodą prób i błędów. Przyjęto, że podstawienie E może być identyczne z obecnym w handlowym modelu maszyny Enigma, tj.:

Q	W	E	R	T	Z	U	I	O	A	S	D	F	G	H	J	K	P	Y	X	C	V	B	N	M	L
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Kiedy założenie nie przyniosło oczekiwanego rezultatu, przyjęto, że w wybranym dniu w trakcie szyfrowania klucza depeszy nastąpiło przesunięcie środkowego wirnika. Proces powtórzono na podstawie materiału z innego dnia, a kiedy nie osiągnięto powodzenia, operację powtarzano dla danych z kolejnych dni. Kiedy prace nie przynosiły wyniku w ciągu kilku miesięcy, noszono się z zamiarem ich przerwania. Wcześniej jednak uczyniono jeszcze jedną próbę, tym razem przy założeniu

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Tym razem szczęście dopisało, założenie okazało się prawidłowe i doprowadziło do rozwiązania problemu.

Dla lepszej orientacji czytelnika zauważmy, że znalezienie połączeń prawego wirnika wymaga przekształcenia 6 zdefiniowanych powyżej równań do następującej postaci:

$$E^{-1}S^{-1}A_1SEQ^{-3}E^{-1}S^{-1}A_4SEQ^{3} = C_\gamma \quad [C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1} Q^{-3} C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1} Q^{3}]\, C_\gamma^{-1}$$
$$Q^{-1}E^{-1}S^{-1}A_2SEQ^{-3}E^{-1}S^{-1}A_5SEQ^{4} = C_\gamma Q^{-1} [C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1} Q^{-3} C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1} Q^{3}]\, Q C_\gamma^{-1}$$
$$Q^{-2}E^{-1}S^{-1}A_3SEQ^{-3}E^{-1}S^{-1}A_6SEQ^{5} = C_\gamma Q^{-2} [C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1} Q^{-3} C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1} Q^{3}]\, Q^2 C_\gamma^{-1}$$

Mimo swej długości równania nie są specjalnie skomplikowane. Wszystkie wyrażenia po lewej stronie są znane, wszystkie wyrażenia po prawej stronie mają wspólny środkowy człon. Jego eliminacja pozwala wyznaczyć $C_\gamma Q C_\gamma^{-1}$, a stąd bezpośrednio C_γ, tj. połączenia prawego wirnika.

Konieczne było oczywiście wyznaczenie połączeń także lewego i środkowego wirnika, a także pozycji ich przeskoku, ponieważ jednak nie stosowano w tym celu metod innych od wyżej opisanych, ich prezentację pominięto.

6. Podstawienie E

Zamierzamy naszkicować sposób wyznaczenia podstawienia E metodą dedukcyjną.

Ponieważ jesteśmy w posiadaniu kluczy dnia na dwa miesiące, to możemy łatwo znaleźć takie dwa dni, w których zarówno kolejność wirników, jak i pozycja prawego wirnika, tj. różnica pomiędzy pozycją bazową i pozycją pierścieni, jest tożsama. Konstruujemy dla obu dni układ równań A_1 do A_6, podstawiając:

$$F = C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1}$$

i oznaczając zmienne dla drugiego dnia podkreśleniem:

$$A_1 = S\ E\ C_\gamma\ F\ C_\gamma^{-1} E^{-1}\ S^{-1} \qquad \underline{A_1} = C_\gamma \underline{F}\ C_\gamma^{-1} E^{-1} \underline{S}^{-1}$$
$$A_2 = SEQC_\gamma Q^{-1} F\ Q\ C_\gamma^{-1} Q^{-1} E^{-1} S^{-1} \qquad \underline{A_2} = \underline{S}EQC_\gamma Q^{-1}\underline{F}\ Q\ C_\gamma^{-1} Q^{-1} E^{-1} \underline{S}^{-1}$$
$$A_3 = SEQ^2 C_\gamma Q^{-2} F\ Q^2 C_\gamma^{-1} Q^{-2} E^{-1} S^{-1} \qquad \underline{A_3} = \underline{S}EQ^2 C_\gamma Q^{-2}\underline{F}\ Q^2 C_\gamma^{-1} Q^{-2} E^{-1} \underline{S}^{-1}$$
$$\vdots\ \vdots\ \vdots\vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots \qquad \vdots\ \vdots\ \vdots\vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots$$

$A_6 = SE\,Q^5C_\gamma Q^{-5}F\;\; Q^5C_\gamma^{-1}Q^{-5}E^{-1}S^{-1}$ $\qquad\qquad$ $\underline{A_6} = \underline{S}E\,Q^5C_\gamma Q^{-5}\underline{F}\;\; Q^5C_\gamma^{-1}Q^{-5}E^{-1}\underline{S}^{-1}$

Na tej podstawie tworzymy następujące równania, których prawa strona jest znana:

$$S^{-1}A_1S\underline{S}^{-1}\underline{A_1}\underline{S} = EC_\gamma F\;\; \underline{F}\;\; C_\gamma^{-1}E^{-1}$$
$$S^{-1}A_2S\underline{S}^{-1}\underline{A_2}\underline{S} = EQC_\gamma Q^{-1}F\;\; \underline{F}QC_\gamma^{-1}Q^{-1}E^{-1}$$
$$\vdots\;\vdots\;\vdots\;\vdots\;\vdots\;\vdots\;\vdots\;\vdots\;\vdots\;\vdots\;\vdots\;\vdots\;\vdots\;\vdots\;\vdots$$
$$S^{-1}A_6S\underline{S}^{-1}\underline{A_6}\underline{S} = EQ^5C_\gamma Q^{-5}F\;\; \underline{F}Q^5C_\gamma^{-1}Q^{-5}E^{-1}$$

Przez eliminację $F\underline{F}$ otrzymujemy wyrażenia:

$$E\;\; (QC_\gamma\, Q^{-1}C_\gamma^{-1})\, E^{-1}$$
$$EQ\;\; (QC_\gamma\, Q^{-1}C_\gamma^{-1})\, Q^{-1}E^{-1}$$
$$EQ^2\; (QC_\gamma\, Q^{-1}C_\gamma^{-1})\, Q^{-2}E^{-1}$$
$$\vdots\;\vdots\;\;\;\vdots\;\vdots\;\;\;\vdots\;\;\;\vdots\;\;\;\vdots\;\;\;\vdots$$
$$EQ^4\; (QC_\gamma\, Q^{-1}C_\gamma^{-1})\, Q^{-4}E^{-1}$$

Stąd przez eliminację $QC_\gamma Q^{-1}C_\gamma^{-1}$, a następnie $EQ^{-1}E^{-1}$, otrzymujemy bezpośrednio E.

Droga do rozwiązania jest nieco wydłużona, szczególnie kiedy nie znamy podstawień A_1 do A_6, a tylko ich iloczyny A_1A_4, A_2A_5, A_3A_6; rzeczywiste wykonanie naszkicowanych operacji wymagałoby zapewne kilku miesięcy pracy jednej osoby. Dowiedliśmy jednak, że zakładając znajomość ustawień łącznicy, można w opisany sposób osiągnąć cel.

7. Podstawienie S

Na zakończenie pragniemy zademonstrować, jak można osiągnąć cel bez znajomości kluczy dnia na dwa miesiące. Należy zauważyć, że naszkicowana poniżej metoda zakłada znajomość podstawienia E, lub co najmniej jego odgadnięcie, jak to miało miejsce w rzeczywistości. Zakłada się następnie znajomość podstawień A_1 do A_6, a nie wyłącznie ich iloczynów A_1A_4, A_2A_5, A_3A_6, co także z pewnością dałoby się osiągnąć. Metoda wymaga w końcu dysponowania na tyle obszernym materiałem szyfrowym, aby dla kilkuset dni możliwe było wyznaczenie podstawień od A_1 do A_6. Jeżeli spełnione są powyższe założenia, to można oczekiwać, że będzie można znaleźć takie dwa dni, w których identyczna jest kolejność wirników, taka sama jest różnica pomiędzy pozycją bazową oraz pozycją pierścieni lewego i środkowego wirnika, a różnica między pozycją bazową a pozycją pierścieni prawego wirnika nie przekracza trzech pozycji. Jeżeli taki przypadek wystąpi, to jest on łatwy do zidentyfikowania. Zakładamy, że pozycje prawego wirnika dla obu dni różnią się o 3, zatem podstawienia A_1 i $\underline{A_4}$ powstają w tej samej pozycji wirników. Następnie iloczyny A_1A_2 i $\underline{A_4}\underline{A_5}$ z jednej strony oraz A_2A_3 i $\underline{A_5}\underline{A_6}$ z drugiej muszą być podobne, jak łatwo się przekonać, zapisując odnośne równania w formie:

$A_1A_2 = S(EGQGQ^{-1}E^{-1})S^{-1}$ $\qquad$ $\underline{A_4}\underline{A_5} = \underline{S}(EGQGQ^{-1}E^{-1})\underline{S}^{-1}$
$A_2A_3 = S(EGQGQ^{-2}E^{-1})S^{-1}$ $\qquad$ $\underline{A_5}\underline{A_6} = \underline{S}(EGQGQ^{-2}E^{-1})\underline{S}^{-1}$

przy czym użyto skrótu: $C_\alpha C_\beta C_\gamma U C_\gamma^{-1} C_\beta^{-1} C_\alpha^{-1} = G$.

Następnie z równań A_1A_2 i $\underline{A_4}\underline{A_5}$ oraz równań A_2A_3 i $\underline{A_5}\underline{A_6}$ można wyznaczyć iloczyn $S\underline{S}$, który w obu przypadkach powinien być równy, a ponadto powinien się on składać z co najmniej 14 cykli.

Główna trudność polega na tym, że w opisany sposób wyznaczamy iloczyn $S\underline{S}$, a nie osobno podstawienia S i $\underline{S}$. Okazuje się jednak, że S i $\underline{S}$ mogą przyjąć kilkaset różnych postaci. Ich wartości należy kolejno podstawiać do naszych równań, usiłując osiągnąć rezultat. Ta ważna praca okazałaby się niewykonalna, gdyby były znane nie podstawienia A_1 do A_6, lecz jedynie ich iloczyny.

8. Kilka liczb

Pełen opis maszyny Enigma przekraczałby ramy niniejszego szkicu. Pragniemy jednak podać kilka liczb ilustrujących, jak ważnym wyzwaniem z kryptologicznego punktu widzenia jest Enigma, przy założeniu, że jest właściwie używana.

Liczba możliwych różnych uporządkowań wirników wynosi przy trzech wirnikach

$$3\times2\times1 = 6,$$

a przy pięciu wirnikach

$$5\times4\times3 = 60.$$

Liczba różnych pozycji bazowych oraz pozycji pierścieni wynosi

$$26^3 = 17\,576.$$

Liczba możliwych pozycji wirników wynosi dla trzech wirników (łącznie z kolejnością wirników):

$$105\,456,$$

a dla pięciu wirników:

$$1\,054\,560.$$

Liczba różnych połączeń w łącznicy wynosi dla sześciu par przewodów:

$$(26!)/(2^6\times6!\times14!) = 100\,391\,791\,500,$$

a dla dziesięciu par:

$$(26!)/(2^{10}\times10!\times6!) = 150\,738\,274\,937\,250.$$

Liczba możliwych połączeń reflektora wynosi:

$$(26!)/(13!\times2^{13}) = 7\,905\,853\,580\,625,$$

a pozostałych wirników:

$$26! = 403\,291\,587\,620\,262\,925\,584\,000\,000.$$

Ostatnią liczbę można poglądowo przedstawić w następujący sposób: gdyby każdy z ludzi zamieszkujących Ziemię wypróbował jedno możliwe połączenie w ciągu sekundy, całość pracy zostałaby ukończona po upływie sześciu miliardów lat (można przy tym zauważyć, że Ziemia istnieje dopiero od dwóch miliardów lat).

9. Odtwarzanie klucza depeszy

Do tej pory rozwiązywaliśmy następujący problem: przy założeniu znajomości kluczy do szyfru na dwa miesiące należy zrekonstruować połączenia wirników. Na tym jednak zadanie się nie kończy. Tym razem chodzi o rozwiązanie odwrotnego problemu: przy znanych połączeniach wirników znaleźć klucz do szyfru.

Służby techniczne polskiego Biura Szyfrów zmodyfikowały egzemplarz handlowej maszyny tak, by mógł służyć do czytania depesz wojskowych. Następnie odczytano materiał szyfrowy z okresu dwóch miesięcy, dla których posiadano klucze, identyfikując i oczywiście wykorzystując błędy popełniane przez szyfrantów. Błędy służyły przede wszystkim do odtwarzania kluczy depesz, tj. kluczy wybieranych w dowolny sposób przez szyfrantów, szyfrowanych podwójnie i dołączanych na początku depeszy. Z biegiem lat Niemcom udało się wyszkolić szyfrantów na tyle, że popełniali coraz mniej błędów, jednak był to proces na tyle powolny, że długo udawało się opracowywać coraz bardziej wyrafinowane metody odtwarzania kluczy depesz.

10. Metoda charakterystycznych kluczy

W pierwszym okresie po wprowadzeniu Enigmy szyfranci wybierali z upodobaniem klucze składające się z trzech identycznych liter, jak AAA, BBB itd. Metoda kluczy charakterystycznych opierała się tym, aby za pomocą teorii cykli przyporządkować poszczególne cykle tak, by powstało możliwie wiele kluczy składających się z trzech równych liter. Wkrótce jednak szyfrantom zakazano wyboru kluczy składających się z trzech równych liter. W rezultacie zaczęli wybierać znaki:

Q W E R T Z U I O
A S D F G H J K
P Y X C V B N M L

które na klawiaturze maszyny sąsiadowały w wierszach lub na przekątnych, jak ASD, QAY, QWE itd. Teraz wystarczyło przyporządkować cykle, tak aby powstało możliwie wiele kluczy w rodzaju ASD i podobnych.

11. Metoda statystyczna

Wkrótce jednak zakazano i tego. Jednocześnie zauważono, że znaki alfabetu występują w kluczach z nierówną częstością. Jako pierwsza litera klucza najczęściej

występowały litery A oraz Q, jako druga – wszystkie samogłoski, jako trzecia litery L oraz O. Inne znaki, takie jak J i Y, występowały jedynie sporadycznie. Przygotowano statystykę częstości występowania znaków i usiłowano porządkować cykle tak, aby otrzymać możliwie najlepszą zgodność z danymi statystycznymi. Częstość ich występowania zmieniała się jednak w czasie, dlatego statystyki trzeba było aktualizować. Ponadto częstości występowania znaków różniły się w armii lądowej i Luftwaffe. W S.D. klucze wybierano na tyle uważnie, że wszystkie znaki występowały w nich z jednakową częstością – zastosowanie metody statystycznej okazywało się niemożliwe.

12. Metoda nierównych liter

Po zakazie wyboru trzech równych liter jako klucza depeszy szyfranci starannie unikali także kluczy, w których występowały choćby dwa równe znaki, jak np. AAB lub FVF. Ten zwyczaj okazał się najtrwalszy ze wszystkich i funkcjonuje do dnia dzisiejszego. Zaletą opartej na nim metody jest możliwość jej całkowitej automatyzacji.

Przyjmijmy, że w danym dniu otrzymaliśmy cykle w postaci:

(SAIZELWDPBOHU)(YCRKXFJQNGVMT)
(AZHNUGWMSFLR)(QBYKPDEVJIOT)(C)(X)
(AZCSYBVMFJPDO)(NUGTIRHQKXEWL)

Należy naszkicować przedstawioną poniżej tabelę oraz dwie analogiczne do niej, a następnie w jej wolnych polach skreślać te pozycje, które implikują równość dwóch znaków.

S	TYCRKXFJQNGVM
A	MTYCRKXFJQNGV
I	VMTYCRKXFJQNG
Z	GVMTYCRKXFJQN
E	NGVMTYCRKXFJQ
L	QNGVMTYCRKXFJ
W	JQNGVMTYCRKXF
D	FJQNGVMTYCRKX
P	XFJQNGVMTYCRK
B	KXFJQNGVMTYCR
O	RKXFJQNGVMTYC
H	CRKXFJQNGVMTY
U	YCRKXFJQNGVMT
AZHNUGWMSFLR	

TOIJVEDPKYBQ
QTOIJVEDPKYB
BQTOIJVEDPKY
YBQTOIJVEDPK
KYBQTOIJVEDP
PKYBQTOIJVED
DPKYBQTOIJVE
EDPKYBQTOIJV
VEDPKYBQTOIJ
JVEDPKYBQTOI
IJVEDPKYBQTO
OIJVEDPKYBQT

C	
X	

Kiedy dysponuje się wystarczającą liczbą depesz, w końcu pozostanie tylko jeden przypadek.

13. Określanie prawego wirnika

Po tym, jak w większości przypadków byliśmy w stanie odtworzyć klucz depeszy, można przejść do rekonstrukcji klucza dnia, tj. kolejności wirników, połączeń łącznicy, położenia bazowego i pozycji pierścieni. Ten proces rozpoczyna się od określenia kolejności wirników.

Jeśli zapiszemy dwa dowolne zdania w języku niemieckim jedno pod drugim, każde o długości 100 znaków, z reguły znajdziemy osiem kolumn, w których występują identyczne znaki. Ta właściwość zachodzi także, jeśli oba zdania zostały zaszyfrowane tym samym kluczem. Jeżeli jednak weźmiemy dwa teksty pozbawione sensu, w których częstość występowania znaków odpowiada częstości naturalnej dla języka niemieckiego, i zapiszemy je jeden pod drugim, znajdziemy średnio cztery kolumny zawierające identyczne znaki. Opisaną właściwość można wykorzystać dla określenia tożsamości prawego wirnika. Jeżeli dysponujemy wystarczającym materiałem szy-

frowym, można znaleźć w nim pewną liczbę par depesz, w których pierwsze dwa znaki klucza są identyczne, a trzecie różne. Obie depesze pary zapisujemy jedna pod drugą tak, by znaki zaszyfrowane w tej samej pozycji wirników znalazły się jeden pod drugim. A priori możliwe są jednak dwa przyporządkowania, zależne od tego, czy podczas szyfrowania nastąpiło przesunięcie środkowego wirnika. Zliczając liczbę kolumn zawierających identyczne znaki w przypadku właściwego przyporządkowania (co najmniej w ogólności), znajdziemy dwa razy większą liczbę par niż w przypadku fałszywego przyporządkowania. W ten sposób można się dowiedzieć, w jakim przedziale znaków nastąpił obrót środkowego wirnika, a po przeanalizowaniu wszystkich par można ten przedział zawęzić w takim stopniu, by pozwolił na jednoznaczną identyfikację prawego wirnika, który powoduje obrót wirnika środkowego. Pozostałe wirniki zostaną zidentyfikowane później w inny sposób.

14. Ruszt

Następna faza pracy polegała na odtworzeniu połączeń łącznicy. Był to problem trudny do rozwiązania, jednak w końcu opracowano metodę, dla której punktem wyjścia było to, że, po pierwsze, podczas szyfrowania klucza depeszy obrót środkowego wirnika następuje jedynie w pięciu przypadkach, po drugie zaś – łącznica pozostawia część liter bez zmiany.

W celu zilustrowania podejścia załóżmy, że w łącznicy brakuje połączeń. Wtedy sześć równań opisujących podstawienia od A_1 do A_6 można doprowadzić do następującej postaci:

$$
\begin{aligned}
&Q^{X}\ C_{\gamma}^{-1}Q^{-X}\ E^{-1}A_1 E Q^{X}\ C_{\gamma}Q^{-X} = F\\
&Q^{X+1}C_{\gamma}^{-1}Q^{-X-1}E^{-1}A_2 E Q^{X+1}C_{\gamma}Q^{-X-1} = F\\
&\ \vdots\quad\ \vdots\quad\ \vdots\quad\ \vdots\ \ \vdots\ \ \vdots\ \vdots\quad\ \vdots\quad\ \vdots\quad\ \vdots\ \vdots\\
&Q^{X+5}C_{\gamma}^{-1}Q^{-X-5}E^{-1}A_6 E Q^{X+5}C_{\gamma}Q^{-X-5} = F
\end{aligned}
$$

W powyższych równaniach znane są wszystkie zmienne z wyjątkiem wyrażenia $F = C_{\beta}C_{\alpha}UC_{\alpha}^{-1}C_{\beta}^{-1}$ oraz wykładnika X. Jeśli nawet dzięki opisanej powyżej metodzie wiemy, który wirnik zajmuje położenie po prawej, nie znamy jego pozycji.

Postępujemy w ten sposób, że przyjmujemy dla X kolejno wartości od 0 do 25 i każdorazowo wyznaczamy z powyższych sześciu równań wartość F. Sześć wartości wyrażenia F różni się wzajemnie w każdym przypadku za wyjątkiem jednego, w którym wszystkie sześć wartości jest tożsamych. W ten sposób wyznaczamy X, tj. pozycję prawego wirnika oraz wartość podstawienia F, która okaże się użyteczna później.

W praktyce postępuje się w ten sposób, że na arkuszu papieru wypisuje się wypisuje się kolejno drugie wiersze podstawień: C_{γ}, $QC_{\gamma}Q^{-1}$,. . ., $Q^{25}C_{\gamma}Q^{-25}$ (pierwsze wiersze mają zawsze postać 1 2 3 4 … 26):

19 3 15 23 11 20 4 16 26 10 14 22 2 17 6 25 9 1 21 12 18 5 24 13 8
2 14 22 10 19 3 15 25 9 13 21 1 16 5 24 8 26 20 11 17 4 23 12 7 6
13 21 9 18 2 14 24 8 12 20 26 15 4 23 7 25 19 10 16 3 22 11 6 5 17

(przytoczony przykład jest fikcyjny).

Na drugim arkuszu z otworami (stąd określenie rusztu) wypisujemy sześć podstawień od A_1 do A_6 w następującej formie:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

V T Z F K D R N O U E W Y H I S X G P B J A L Q M C

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

K Q H U V S Z C O N A T W J I Y B X F L D E M R P G

Po opisanych przygotowaniach nakładamy ruszt na pierwszy arkusz i przesuwamy go tak długo w dół i w górę, aby w pewnym położeniu w okienkach arkusza ukazały się identyczne wartości podstawienia F. Taka sytuacja wystąpi jedynie wtedy, gdy brakuje połączeń w łącznicy. W przeciwnym przypadku obraz ulega pewnej zmianie ze względu na łącznicę, ponieważ jednak jej połączenia nie modyfikują wszystkich liter, z reguły można zauważyć pewne analogie pomiędzy sześcioma różnymi podstawieniami F. Następnie należy próbować tak przestawiać znaki podstawień od A_1 do A_6, aby wszystkie wartości F okazały się identyczne. Jeżeli to się powiedzie, przestawienia znaków określają poszukiwane podstawienie łącznicy, a dodatkowo otrzymujemy pozycję prawego wirnika i wartość podstawienia F.

15. Katalog F

Po określeniu tożsamości i pozycji prawego wirnika można by próbować określić tożsamość i pozycje środkowego i lewego wirnika przez zbadanie wszystkich możliwych przypadków. Aby uniknąć zbytecznej pracy, przygotowano jednak katalog obejmujący wszystkie możliwe wartości podstawienia F, których jest:

$6 \times 26 \times 26 = 4056$.

Teraz wystarczało odnaleźć wartość F znalezioną podczas odtwarzania połączeń łącznicy w katalogu, aby natychmiast ustalić tożsamość i pozycję prawego i środkowego wirnika.

16. Cyklometr

Metoda, którą zastosowano dla znalezienia połączeń łącznicy, była nie tylko pracochłonna i nieelegancka, lecz także nie gwarantowała osiągnięcia wyniku. Poza tym zakładała znajomość klucza depeszy, a metody pozwalające go znaleźć były równie czasochłonne i nie zawsze uwieńczone powodzeniem. W rezultacie poszukiwano innych metod, które mogłyby doprowadzić do celu szybciej i pewniej, wychodząc od spostrzeżenia, że kształt cykli nie tylko stanowił niezmiennik podstawień generowanych przez łącznicę, lecz także charakteryzował klucz dnia w tym sensie, że stosunkowo rzadko przytrafiały się dwa dni o identycznych formach cykli. Stąd już było blisko do pomysłu, aby opracować katalog postaci cykli dla wszystkich możliwych pozycji wirników, których, jak już wcześniej wskazano, było 105 456.

Aby poradzić sobie z tą pracą, skonstruowano specjalne urządzenie, cyklometr,

który składał się z dwóch maszyn Enigma połączonych wzajemnie, tak aby w każdej pozycji zależnie od długości odpowiadającego jej cyklu zapalała się większa lub mniejsza liczba lampek. Zakończenie całej pracy wymagało ponad roku, jednak od tej pory w ciągu kilku minut znajdowano kolejność wirników, ich pozycję startową oraz ustawienia łącznicy na dany dzień.

17. Pozycja bazowa i pozycja pierścieni

Pod pojęciem pozycji wirników rozumiemy zawsze różnicę między pozycją bazową a pozycją pierścieni. Aby w pełni zrekonstruować klucz dnia, konieczne jest znalezienie obu jego brakujących elementów, tj. pozycji bazowej oraz pozycji pierścieni. W tym celu nie wystarczy analiza klucza depeszy, konieczne jest także zagłębienie się w jej treść.

Po odczytaniu materiału z października i grudnia 1931 roku, dla którego dysponowaliśmy kluczem, zauważono, że wiele depesz rozpoczyna się od frazy AN. Aby rozdzielić pozycję bazową i pozycję pierścieni, wybierano dowolną depeszę, którą podejrzewano o początek AN, po czym próbowano [sprawdzić] we wszystkich położeniach startowych maszyny, czy to założenie jest słuszne. Była to nudna praca zważywszy, że należało zbadać $26^3 = 17\,576$ możliwości. Później przekonano się, że jeżeli depesza zaczynała się od frazy AN, niektóre pozycje prawego wirnika były wykluczone z założenia. Ponieważ codziennie dysponowaliśmy wieloma depeszami o prawdopodobnym początku AN, z reguły udawało się wyznaczyć pozycję prawego wirnika całkowicie analitycznie.

18. Kilka spostrzeżeń

Przy opisywaniu metody rusztu i cyklometru założono, że podczas szyfrowania klucza depeszy nie porusza się środkowy wirnik. W rzeczywistości to założenie nie jest konieczne, pozycję bazową oraz ustawienie pierścieni można bowiem łatwo znaleźć także wtedy, gdy następuje przesunięcie wirnika środkowego. Określenie, w jakich przypadkach jest to możliwe, pozostawia się czytelnikowi.

Wcześniej zauważono, że w ramach klucza dziennego wśród sześciu znaków tworzących pozycję bazową oraz pozycję pierścieni nie było jednakowych liter. To spostrzeżenie prowadziło nie tylko do zasadniczego uproszczenia pracy, lecz także stanęło w późniejszych latach u podstawy tzw. metody Herivela, o której będzie mowa poniżej. Bywały także okresy, gdy w ciągu kolejnych czterech dni 24 znaki określające pozycję bazową oraz pozycję pierścieni były różne. Podobne spostrzeżenie sformułowano w innych okresach w odniesieniu do ustawień łącznicy.

19. Nowe sieci. Ciągłe zmiany

W miarę rozwoju niemieckich sił zbrojnych rosła także liczba stacji radiowych. Pojawiały się również nowe sieci radiowe używające takiej samej maszyny Enigma, jednak operujące odmiennym kluczem dziennym. Na przykład nowo powstałe niemieckie lotnictwo utworzyło 1 sierpnia 1935 roku własną sieć radiową z własnym kluczem do szyfru.

Aby zagwarantować bezpieczeństwo szyfru, wprowadzano różnego rodzaju zmiany. Od 1 lutego 1936 roku kolejność wirników zmieniano co miesiąc, a od 1 października 1936 roku – nawet codziennie. Jednocześnie zmieniono liczbę par przewodów w łącznicy; zamiast sześciu jak do tej pory, teraz liczba par wynosiła od pięciu do ośmiu. Pod koniec 2 listopada 1937 roku wycofano z użytku dotychczasowy reflektor i zastąpiono go nowym, tzw. reflektorem B.

20. Reflektor B

Niemieccy szyfranci popełnili nieostrożność, wspominając w depeszach z września 1937 roku o planowanej zmianie reflektora. Dzięki temu polskie Biuro Szyfrów było przygotowane na zmianę i nie zdziwiło się, gdy 2 listopada nie odnalazło w katalogu charakterystyk cyklicznych zarejestrowanych tego dnia cykli. Mimo to dzięki wykorzystaniu metody rusztu zdołano określić tożsamość i pozycję prawego wirnika oraz połączenia łącznicy.

Nieznana pozostawała tożsamość lewego i środkowego wirnika oraz pozycje ich obu. Zachodziło 2×26×26 = 1352 możliwych przypadków i każdy z nich określał jeden możliwy reflektor. Przez porównanie 1 352 hipotetycznych reflektorów z dwóch różnych dni można było łatwo otrzymać reflektor rzeczywisty.

21. Nowe wirniki

We wrześniu 1937 roku pojawiła się nowa sieć łączności należąca do służby bezpieczeństwa S.D., organizacji politycznej, o której będzie dalej mowa. Procedura szyfrowania odpowiadała w niej w większym lub mniejszym stopniu [procedurze] używanej w wojskach lądowych, jednak później wprowadzono w niej kilka nowości. I tak np. 15 września 1938 roku, kiedy w armii lądowej i flocie powietrznej dokonano całkowitej zmiany procedury szyfrowania, w S.D. pozostawała ona przez kilka miesięcy bez zmiany, co było poważnym błędem, który natychmiast się zemścił. Kiedy trzy miesiące później wprowadzono do użytku dwa nowe wirniki, tym razem we wszystkich sieciach naraz, w sieci S.D. używano nadal starej procedury. Pozwoliło to określić połączenia nowych wirników w sposób analogiczny, jak wcześniej połączenia reflektora B. Nie wchodząc w zbyteczne szczegóły, nadmieńmy jedynie, że posłużyliśmy się danymi z dwóch dni, w których nastąpiło przesunięcie środkowego wirnika. Gdyby w S.D. wcześniej wdrożono nową procedurę szyfrowania, to czysto kryptologiczna rekonstrukcja połączeń wirników IV i V z trudem okazałaby się możliwa.

22. Zmiana procedury szyfrowania

Dzięki metodom opisanym wyżej do września 1938 roku wszystkie sieci łączności wojsk lądowych, Luftwaffe, służby bezpieczeństwa i marynarki (o czym będzie mowa dalej) były czytane, często w niewiarygodnie krótkim czasie.

Sytuacja zmieniła się całkowicie, gdy 15 września 1938 roku wprowadzono nową procedurę szyfrowania, co było zagrożeniem dotychczasowych osiągnięć polskich kryptologów w tym obszarze.

Nowa procedura polegała na tym, że nie istniała jedna i ta sama pozycja bazowa dla wszystkich depesz wymienianych w ciągu dnia, a zmieniała się ona z depeszy na depeszę.

Zilustrujmy nową procedurę na przykładzie. Szyfrant wybiera dwie trójki znaków, np. SKR WTC, ustawia maszynę w położeniu SKR i szyfruje dwakroć po sobie znaki WTC (jak w dotychczasowej procedurze), otrzymując np. szóstkę znaków KFDLSF.

Pozycja bazowa SKR jest przesyłana w postaci niezaszyfrowanej w nagłówku depeszy, po niej następuje sześć znaków KFD LSF, a następnie tekst zaszyfrowanej depeszy, poczynając od pozycji WTC (także jak w dotychczasowej procedurze). Strukturę nowej procedury szyfrowania poznaliśmy dzięki temu, że niektórzy szyfranci posłużyli się nią w przeddzień jej oficjalnego wprowadzenia, co oczywiście stanowiło poważny błąd.

23. Określanie kolejności wirników

Ponieważ w nowym systemie klucz depeszy nie był już szyfrowany rozpoczynając od jednej i tej samej pozycji wirników, teoria cykli oraz oparte na niej metody – specyficznych kluczy depesz, rusztu i cyklometru – stały się nieprzydatne.

Jednak nie opuściliśmy rąk, przechodząc do badań nowego systemu. W pierwszej kolejności zauważyliśmy, że wśród materiału szyfrowego z danego dnia zdarzają się pary depesz, w których pierwsze dwie litery klucza były identyczne, a trzecie sąsiadowały w alfabecie, jak np. TKP i TKR. Jeżeli w tych samych depeszach także w kluczu depeszy pojawiały się pary identycznych znaków, można było wyciągnąć wnioski dotyczące tożsamości prawego lub środkowego wirnika. Zilustrujmy różne możliwości kilkoma przykładami.

1) załóżmy, że mamy dwie depesze o następujących kluczach depesz:

pozycja bazowa	klucz depeszy,
TKP	AN**V** CK**B**
TKR	**V**TS **J**QM

W tym przypadku jest oczywiste, że między literami P i R nastąpił obrót środkowego wirnika, tzn., że w prawej pozycji znajduje się wirnik I, ponieważ tylko on powoduje przesunięcie środkowego wirnika pomiędzy znakami Q i R. W przeciwnym wypadku literze V odpowiadałyby równe litery B lub J.

2)

pozycja bazowa	klucz depeszy,
TKP	AN**V** C K**B**
TKR	**V**TS **B**QM

W tym przypadku zachodzi mniejsze prawdopodobieństwo, że nastąpił obrót środkowego wirnika, czyli że w pozycji prawej znajduje się wirnik I.

3) wnioski dotyczące kolejności wirników można wyciągać także na podstawie pozycji bazowej, w której w środkowym położeniu występują różne litery, jak to zademonstrowano w poniższym przykładzie:

pozycja bazowa	klucz depeszy,
TKP	AN**V** C K**B**
TLR	**V**TS **J**QM

Pomiędzy P i R nie może nastąpić przesunięcie środkowego wirnika, zatem w pozycji prawej z pewnością znajduje się wirnik inny niż I.

4) w pewnych przypadkach wnioski dotyczące kolejności wirników można wyciągać nawet na podstawie kluczy depesz, w których pierwsza litera jest różna:

pozycja bazowa	klucz depeszy,

TJG CWS PKR
UKG CWT PLJ.

W tym przypadku jest prawdopodobne, że pomiędzy literami J i K nastąpiło przesunięcie lewego wirnika, z czego wynika, że w środkowej pozycji znajduje się wirnik IV.

W innych przypadkach można formułować podobne wnioski.

24. Bomby

W ciągu kilku dni po wprowadzeniu nowej procedury naszkicowano plan, który pozwalał usunąć trudności wynikające z nowej procedury. Nasze myśli biegły w następującym kierunku: weźmy pewną liczbą depesz i zapiszmy jedne pod drugimi ich pozycje bazowe oraz klucze depesz:

1.	K T L	W O C	D R B	7.	G R A	F D R	Y W D
2.	S V W	K K M	I Y S	8.	M D O	O T W	Y Z W
3.	J O T	I W A	B W N	9.	K J C	F S W	R S E
4.	E D C	D S P	L J C	10.	S G F	T E Y	A S R
5.	G D K	W A V	W H A	11.	A G H	M D F	R H F
6.	B W K	T C A	T O C	12.	J B R	W L T	S O Q

Zwróćmy uwagę na depeszę nr 3. W jej kluczu depeszy litera W występuje dwukrotnie w odstępie trzech znaków. Oznacza to, że w określonej pozycji maszyny nieznana nam litera, oznaczmy ją jako X, jest szyfrowana jako W, a trzy pozycje dalej ta sama litera X jest ponownie szyfrowana jako W. Załóżmy dalej, że litera X nie jest zmieniana przez połączenia łącznicy; założenie to przy 5 do 8 par połączeń w łącznicy jest spełnione w 50% przypadków.

W opisanej sytuacji można znaleźć początkową pozycję wirników w ten sposób, że naciskamy nieustannie literę W w dwóch egzemplarzach Enigmy, których wirniki są przesunięte wzajemnie o trzy pozycje i poruszają się synchronicznie. W każdym przypadku, gdy po naciśnięciu litery W obie maszyny wyświetlą tę samą literę, mamy do czynienia z prawdopodobnym, właściwym rozwiązaniem, które powinno zostać dalej zweryfikowane.

Ponieważ jednak takie przypadki występują zbyt często, radzimy sobie w ten sposób, że analizujemy nie jeden, ale trzy klucze depesz, w których litera W występuje dwukrotnie w odstępie trzech znaków. W naszym przypadku bierzemy pod uwagę depesze nr 3, 5 i 8. Musimy oczywiście posłużyć się nie dwiema, lecz sześcioma maszynami. W rzeczywistości manipulowanie sześcioma odrębnymi maszynami byłoby niepraktyczne. Dlatego zaprojektowano urządzenie składające się z sześciu maszyn Enigma, które były napędzane elektrycznie i zatrzymywały się automatycznie w momencie, gdy osiągały potencjalne rozwiązanie. W polskim Biurze Szyfrów zmontowano sześć egzemplarzy takiej bomby, po jednej dla każdej możliwej kolejności wirników (wirniki IV i V zostały wprowadzone dopiero później), przy czym każda bomba przebiegała w ciągu półtorej godziny przez wszystkie 17 756 możliwych pozycji startowych.

25. Płachty Zygalskiego

Bomby znajdowały się jeszcze w budowie, gdy nastąpiły dalsze zmiany. W dniu 15 grudnia 1938 roku wprowadzono wirniki IV i V, dziesięciokrotnie zwiększając liczbę możliwych kolejności wirników, a następnie, dwa tygodnie później, zwiększono liczbę par połączeń w łącznicy na 7-10. W wyniku tych zmian bomby utraciły swe praktyczne znaczenie, w nowej sytuacji bowiem rozwiązanie dnia wymagałoby zbyt wiele czasu. Niekiedy udawało się określić kolejność wirników dzięki metodzie, o której była mowa powyżej, wymagała ona jednak obszernego materiału szyfrowego, który rzadko był dostępny. Skuteczność bomb była ograniczona także wskutek większej liczby par połączeń w łącznicy.

Dość wcześnie zatem zaprojektowano inną nową metodę, która była niezależna od liczby par połączeń w łącznicy. Dla zilustrowania tej metody musimy wprowadzić nowej pojęcie – pozycji żeńskich i męskich. Powróćmy do depesz przytoczonych na stronie 171:

1.	K	T	L	W	O	C	D	R	B
2.	S	V	W	K	K	M	I	Y	S
3.	J	O	T	I	W	A	B	W	N
4.	E	D	C	D	S	P	L	J	C
5.	G	D	K	W	A	V	W	H	A
6.	B	W	K	T	C	A	T	O	C
7.	G	R	A	F	D	R	Y	W	D
8.	M	D	O	O	T	W	Y	Z	W
9.	K	J	C	F	S	W	R	S	E
10.	S	G	F	T	E	Y	A	S	R
11.	A	G	H	M	D	F	R	H	F
12.	J	B	R	W	L	T	S	O	Q

Przypadek zilustrowany w depeszy nr 3, w którym ta sama litera (w naszym przypadku W) występuje dwukrotnie w odstępie trzech znaków, nie może wystąpić we wszystkich pozycjach początkowych maszyny. Obliczenia wykazały, że taki przypadek zaistnieje w około 40% pozycji (dokładniej wartość wynosi $1 - (1/\sqrt{e})$, gdzie e – podstawa logarytmów naturalnych). Takie pozycje nazywamy pozycjami żeńskimi, pozostałe – męskimi. W naszym przykładzie pozycje nr 3, 5, 6, 8, 9 i 11 to pozycje żeńskie, podczas gdy o naturze pozostałych nie można wyrokować na podstawie dostępnych danych. Połączenia w łącznicy mają wpływ na to, jakie litery wystąpią w kluczu depeszy, jednak nie mają wpływu na płeć danej pozycji (czy będzie ona żeńska, czy męska).

Na podstawie powyższych spostrzeżeń można opracować wykaz obejmujący wszystkie pozycje żeńskie, a następnie przeszukiwać go pod kątem sześciu pozycji żeńskich, które występują w jednakowych odstępach, jak np. pozycje bazowe JOU, GKD, BWK, MDR, KJD, AGK (przy czym należy uwzględnić możliwe przesunięcia środkowego i lewego wirnika).

Ponieważ jest to praktycznie niewykonalne, poszliśmy inną drogą. Opracowaliśmy tzw. płachty Zygalskiego: dla każdej kolejności wirników na 26 arkuszach papieru zawierających 26×26 pól, do tego w poczwórnym wydaniu, naniesiono wszystkie możliwe pozycje żeńskie. Poszczególne arkusze odpowiadały pozycjom lewego wirnika, 26×26 pól na każdym arkuszu odpowiadało możliwym pozycjom środkowego i prawego wirnika. Przyczyna poczwórnego naniesienia pól zostanie wyjaśniona poniżej. Pola odpowiadające przypadkom żeńskim zostały przedziurkowane (stąd inna nazwa arkuszy: sieć).

Powracając do naszego przykładu, sześć 26 arkuszy nakłada się wzajemnie w kolejności i z przesunięciem odpowiadającym różnicom między pozycjami bazowymi. Jeśli istnieje pozycja, w której we wszystkich arkuszach jednocześnie pojawia się otwór, to znaleźliśmy prawdopodobnie właściwą pozycję, która wymaga

dalszego zbadania. Aby zbadać wszystkie możliwości, należy cyklicznie zamieniać arkusze. Każdy z nich zawiera poczwórny komplet 26×26 pól, arkusze są bowiem nakładane z przesunięciem wzajemnym. Osiągnięcie końcowego rezultatu jest uwarunkowane starannością w nakładaniu arkuszy. Dlatego początkiem prac jest przygotowanie odrębnego arkusza, tzw. menu, określającego kolejność nakładania i wzajemną pozycję poszczególnych arkuszy.

Wiedza, które pozycje są żeńskie, a które męskie, została zaczerpnięta wprost z wykazów wykonanych za pomocą cyklometru, pozycje żeńskie bowiem odpowiadają z reguły cyklom składającym się z jednej litery.

Sprawdzanie właściwych przypadków także odbywało się z wykorzystaniem cyklometru. Było to czasochłonne rozwiązanie, jednak liczyliśmy się wtedy z możliwością katalogowania nie tylko pozycji żeńskich, lecz wszystkich pozycji odpowiadających cyklom o długości jednego znaku. Ten zamysł został zrealizowany dużo później, już przez kryptologów brytyjskich.

26. Konferencja w Warszawie

W polskim Biurze Szyfrów wytworzono ręcznie dwa komplety 26 płacht Zygalskiego dla dwóch kolejności wirników i przekonano się w ten sposób, ze idea płacht jest praktyczna. Zupełnie inaczej prezentowało się jednak zastosowanie tego pomysłu.

Podczas gdy pozycje żeńskie dla kolejności wirników I II III, I III II, ..., III II I można było zaczerpnąć wprost z katalogu, dla pozostałych 54 kolejności wirników należało je najpierw określić albo z wykorzystaniem cyklometru, co zajęłoby kilka lat, albo za pomocą nowej i kosztownej maszyny, o czym nie można było nawet pomyśleć. Samo ręczne perforowanie obu pierwszych kompletów po 26 płacht było na tyle kłopotliwe, że dalsza praca wymagałaby specyficznej aparatury. I w końcu, gdyby nawet została zakończona, manipulowanie 60 kompletami płacht, aby znaleźć klucz dla kolejnych dni, wymagałoby licznego personelu pomocniczego.

Ponieważ polskie Biuro Szyfrów nie było w stanie przezwyciężyć opisanych trudności samodzielnie, postanowiono powierzyć ściśle do tej pory chroniony sekret Enigmy także francuskiej i angielskiej służbie kryptologicznej.

W dniu 26 lipca 1939 roku w Warszawie rozpoczęła się trzydniowa konferencja dotycząca Enigmy, w której uczestniczyli przedstawiciele służb kryptologicznych Francji i Anglii. Okazało się, że ani francuscy, ani brytyjscy kryptolodzy nie byli w stanie przezwyciężyć pierwszych problemów. Zaprezentowaliśmy im wyniki naszej siedmioletniej pracy, a także napotkanie ostatnio trudności. Anglicy zadeklarowali pomoc w wykonaniu kompletów płacht Zygalskiego dla 60 różnych kolejności wirników.

27. Wybuch wojny. Vignolles

Miesiąc później wybuchła wojna niemiecko-polska. Udało się jeszcze złamać depesze z 25 sierpnia 1939 roku, dnia powszechnej mobilizacji w Niemczech, wkrótce potem rozpoczęła się ewakuacja. Bomby, cyklometr, Enigmy, całość dokumentacji i rysunków technicznych zabraliśmy ze sobą, jednak przyszło je stopniowo niszczyć w drodze ku rumuńskiej granicy. Uratowano jedynie dwa egzemplarze Enigmy.

W Bukareszcie ambasada Francji przyjęła trójkę specjalistów od Enigmy i wyprawiła ich w dalszą podróż do Paryża, gdzie spotkali się z przyjaznym przyjęciem. Kilka tygodni później francuski sztab zorganizował w Vignolles, zameczku położonym w pobliżu Gretz i odległym o 30 km od stolicy kraju, biuro, w którym polscy kryptolodzy z udziałem personelu pomocniczego i pod dowództwem podpułkownika Langera usiłowali podjąć ponownie obowiązki przerwane w Polsce. Rozpoczęto, jak swego czasu w Warszawie, żmudną pracę nad ręcznym wykonaniem płacht Zygalskiego, pracę, której wyniki byłyby dostępne po latach.

W tym momencie zaczęła jednak przynosić owoce konferencja w Warszawie. Okazało się, że w tym czasie Anglicy skonstruowali urządzenie, które pozwoliło im wykonać komplet płacht Zygalskiego dla wszystkich 60 możliwych kolejności wirników w ciągu kilku tygodni. Jednakże podejmowane w Anglii próby zastosowania płacht nie przynosiły rezultatu. Ponieważ płachty zostały wykonane w dwóch egzemplarzach, jeden z nich Anglicy mogli przekazać do naszej dyspozycji, co też życzliwie uczynili. Gdy tylko płachty dotarły do Vignolles, rozpoczęła się wytężona praca i wkrótce złamano klucz dla dwóch dni: 28 października 1939 roku oraz 6 stycznia 1940 roku.

Anglicy świetnie zorganizowali swoją pracę. Dysponowali licznym personelem i obszernym materiałem z nasłuchu. Większość rozwiązanych dni była ich dziełem.

Gorączkowa praca trwała także w Vignolles. Ponieważ obecnie chodziło o odczytanie możliwie obszernego materiału szyfrowego i przekazanie go sztabowi generalnemu do oceny, polscy kryptolodzy siedzieli bez przerwy nad Enigmami, stukając depesze i manipulując płachtami, tak aby nie pozwolić się całkowicie zdystansować Anglikom. Była to całkowicie mechaniczna praca, którą mógł wykonać personel pomocniczy. W tej sytuacji było zrozumiałe, że polscy kryptolodzy nie osiągnęli już istotnych rezultatów kryptologicznych, a punkt ciężkości prac teoretycznych przesunął się do Londynu.

28. Metoda Knoxa

Brytyjski kryptolog Knox zauważył, że niemieccy szyfranci często wybierają jako pozycję bazową te litery, które są widoczne w okienkach maszyny po zakończeniu szyfrowania poprzedniej depeszy. Zjawisko to szczególnie często występowało w depeszach wieloczęściowych. W takich przypadkach wystarczało od pozycji bazowej odjąć długość poprzedniej depeszy, aby otrzymać (niezaszyfrowany) klucz depeszy. Jeżeli otrzymywano przy tym jeden z charakterystycznych kluczy, jak ASD, WER, OKL, to można było być pewnym, że szyfrant popełnił opisany błąd. Ponieważ przy odejmowaniu długości depeszy od pozycji bazowej należało uwzględnić ewentualne przesunięcia środkowego i lewego wirnika, otwierało to pole do częściowego określenia kolejności wirników, co przy odrobinie szczęścia pozwalało zredukować liczbę możliwych wariantów kolejności wirników z 60 do 3. Ważne było także to, że dzięki metodzie Knoxa można było poznać (niezaszyfrowane) klucze wielu depesz.

Ta metoda przysłużyła się w znacznym stopniu podczas kampanii norweskiej, kiedy rozwiązywano dzień po dniu, dostarczając ważnych i interesujących informacji.

29. Katalogi do płacht Zygalskiego

W tym czasie brytyjscy kryptolodzy urzeczywistnili jeszcze jedną metodę zaproponowaną wcześniej przez Polaków. Jak już wskazano, weryfikacja przypadków zidentyfikowanych z wykorzystaniem płacht Zygalskiego za pomocą cyklometru była zajęciem dość czasochłonnym. Należało każdorazowo po zidentyfikowaniu potencjalnego rozwiązania weryfikować literę odpowiadającą pozycji żeńskiej i wyszukać ją przy użyciu cyklometru, a następnie porównać ze znakami odpowiedniego klucza depeszy. Jeszcze w Polsce nosiliśmy się z zamiarem sporządzenia wykazów zawierających litery odpowiadające wszystkim przypadkom żeńskim, jednak trudności techniczne stanęły takiemu rozwiązaniu na przeszkodzie. Teraz Anglicy dostarczyli z wykorzystaniem tego samego urządzenia, które posłużyło do wykonania kompletów płacht Zygalskiego, kolejny spektakularny przykład korzyści wynikających z polsko-francusko-brytyjskiej współpracy. Dzięki swoim możliwościom finansowym i organizacyjnym wprowadzili w życie nasze plany, które w innym przypadku nie ujrzałyby światła dziennego, nie zważając przy tym na koszty i trudności.

30. Metoda Herivela

Jeszcze inny angielski kryptolog odkrył, że niektórzy niemieccy szyfranci, kiedy po północy lub rankiem ustawiali maszyny Enigma na kolejny dzień, nie zmieniali po ustawieniu pierścieni i nie obracali wirników, lecz używali znaków widocznych w okienkach maszyny jako klucza pierwszej depeszy w danym daniu. W rezultacie pozycja bazowa pierwszej depeszy nie różniła się istotnie od obowiązującej pozycji pierścieni.

Dzięki porównaniu pozycji bazowych depesz nadanych przez różnych szyfrantów nocą lub we wczesnych godzinach rannych można było określić pozycje pierścieni dokładnie lub co najmniej ze znacznym przybliżeniem. Dzięki temu odkryciu praca niezbędna dla złamania szyfru uległa znacznemu skróceniu tak, że często już we wczesnych godzinach porannych Anglicy byli w posiadaniu klucza na dany dzień.

Do opisanej metody należy dorzucić jeszcze kilka zdań. Kiedy połączenia wirników IV i V zostały określone, przez pewien czas nie udawało się określić obowiązującego dla nich punktu przeskoku na pierścieniach wirników. Mieliśmy do wyboru 26 możliwych wariantów, spośród których wybieraliśmy uważany za najlepszy. Panowała jednak zgoda, że wybrana w ten sposób pozycja nie jest tożsama z prawdziwą. Po tym, jak złamano znaczną liczbę depesz (jeszcze przez odkryciem Herivela), przypomnieliśmy sobie, że wcześniej punkty przeskoku były różne we wszystkich wirnikach. Jeśli ta cecha została zachowana także w nowych wirnikach (co było wysoce prawdopodobne), to należało wprowadzić korekty do wcześniejszych ustaleń dotyczących punktów przeskoku w wirnikach IV i V. Odpowiednie korekty zostały znalezione i natychmiast zakomunikowane Anglikom. Dopiero wtedy metoda Herivela mogła zostać efektywnie zastosowana.

31. Trzecia procedura szyfrowa

W dniu 1 maja 1940 roku, przed rozpoczęciem niemieckiej ofensywy w Belgii i Holandii, procedura szyfrowa została ponownie zmieniona. W nowej [procedu-

rze] klucz depeszy nie był szyfrowany dwukrotnie, jak do tej pory, lecz tylko raz. W nagłówku depeszy podawano teraz tylko sześć liter, przy czym pierwsza trójka określała pozycję bazową, a druga – zaszyfrowany klucz depeszy.

Ten stan rzeczy został rozpoznany dzięki temu, że niemieccy szyfranci ponownie popełnili błąd, stosując nową procedurę już wieczorem, w przeddzień jej oficjalnego wprowadzenia. Ten dzień, 30 kwietnia 1940 roku, został złamany, nawiasem mówiąc, przez polskich kryptologów, co umożliwiło określenie, na czym polega nowa procedura.

Nowa procedura stanowiła poważny cios. Płachty Zygalskiego i towarzyszące im katalogi okazały się w pełni bezużyteczne, pozostały jedynie metody Knoxa i Herivela. Polscy kryptolodzy, przeniesieni w tym okresie przejściowo z Vignolles do Paryża, próbowali z ich pomocą złamać choć jeden dzień, jednak na próżno.

Anglicy mieli więcej szczęścia. Dysponowali bardziej obszernym materiałem, dzięki czemu udało im się, po trzytygodniowej przerwie, rozwiązać 20 maja 1940 roku i wkrótce po nim prawie wszystkie kolejne dni. Przekazywali nam regularnie złamane klucze, toteż polscy specjaliści siedzieli dzień i noc nad obiema pochodzącymi jeszcze z Warszawy Enigmami, aby odczytywać cenny materiał ze złamanych depesz. Po ewakuacji z Paryża pracę wznowiono w La Ferté-St. Aubin, gdzie nadal pracowano dzień i noc, przerywając dekryptaż dopiero po podpisaniu rozejmu. Ostatnim dniem, dla którego Anglicy przesłali klucze, był 16 czerwca 1940 roku.

32. Chronologiczny przegląd zmian procedur szyfrowych w wojskach lądowych i Luftwaffe

<table>
<tr><td>15.07.1928
1929
31.05.1930</td><td colspan="6">Enigma G z połączeniami wtyczkowymi</td></tr>
<tr><td>1.06.1930
1931
1932
1933
1934
1935
31.01.1936</td><td rowspan="9">Enigma M z łącznicą</td><td>Kolejność wirników zmieniana co trzy miesiące.</td><td>W łącznicy zamieniane sześć par znaków.</td><td rowspan="3">Reflektor A</td><td rowspan="4">Wirniki I–III</td><td rowspan="3">Pierwsza procedura szyfrowania. Pozycja bazowa tożsama dla wszystkich depesz. Klucz depeszy szyfrowany dwukrotnie.</td></tr>
<tr><td>1.02.1936
30.09.1936</td><td>Kolejność wirników zmieniana co miesiąc.</td><td>W łącznicy zamieniane pięć–osiem par znaków.</td></tr>
<tr><td>1.10.1936
1.11.1937</td><td rowspan="5">Kolejność wirników zmieniana codziennie.</td></tr>
<tr><td>2.11.1937
14.09.1938</td><td rowspan="5">Reflektor B</td><td rowspan="2">Druga procedura szyfrowania. Pozycja bazowa zmienna dla każdej depeszy. Klucz depeszy szyfrowany dwukrotnie.</td></tr>
<tr><td>15.09.1938
14.12.1938</td></tr>
<tr><td>15.12.1938
31.12.1938</td><td rowspan="3">Wirniki IV–V</td><td rowspan="3">Trzecia procedura szyfrowania. Pozycja bazowa zmienna dla każdej depeszy. Klucz depeszy szyfrowany jednokrotnie.</td></tr>
<tr><td>1.01.1939
31.12.1939</td><td>W łącznicy zamieniane siedem–dziesięć par znaków.</td></tr>
<tr><td>1.01.1940
30.04.1940</td><td>W łącznicy zamieniane dziesięć par znaków.</td></tr>
<tr><td>1.05.1940</td></tr>
</table>

33. Sieć radiowa służby bezpieczeństwa

O sieci radiowej służby bezpieczeństwa wspomnieliśmy już na stronie 169. Ponieważ ta sieć, w skrócie określana mianem S.D., wykorzystywała procedurę szyfrowania, która różniła się w szczegółach od procedur używanych w wojskach lądowych i lotnictwie, należy opisać ją nieco bardziej szczegółowo.

Do 1 sierpnia 1939 roku najważniejszą różnicą między procedurą S.D. i pozostałymi było to, że tekst jawny był w niej maskowany przy użyciu trójpozycyjnego kodu. Kod służył wyraźnie skróceniu tekstu depesz. Złamanie go nie było rzeczą szczególnie trudną, jednak co kilka miesięcy był on zastępowany bardziej obszerną wersją, tak więc trzeba było rozpoczynać całą pracę od początku.

Klucz depeszy był, podobnie jak w siłach lądowych i lotnictwie, szyfrowany podwójnie, jednak nie był dodawany na początku depeszy, lecz okazjonalnie w różnych jej punktach. Poza tym w okresie kilku miesięcy znaki klucza depeszy były dodatkowo szyfrowane zewnętrznym podstawieniem. Okres jego ważności wynosił każdorazowo jeden miesiąc.

Klucze depesz były wybierane starannie, tak więc metody nierównych liter oraz cyklometru nie mogły zostać zastosowane.

Nie występowały depesze rozpoczynające się od frazy AN. Aby znaleźć położenie bazowe i pozycję pierścieni należało korzystać z innych charakterystycznych właściwości tekstu depesz. Ustalono, że w wielu depeszach czwarta i piąta lub piąta i szósta litera brzmiały QY, tak więc można było wykorzystywać te znaki tak samo, jak AN w depeszach wojsk lądowych.

Depesze były bardzo ważne z punktu widzenia zawartości. Często dotyczyły agentów służby bezpieczeństwa pracujących poza obszarem Niemiec, dlatego też na ich podstawie można było zbudować sobie obraz bardzo rozgałęzionej niemieckiej organizacji szpiegowskiej.

Procedura szyfrowania wprowadzona 15 września 1938 roku w wojskach lądowych i lotnictwie nie obowiązywała w sieci S.D. Szyfrowano w niej nadal na podstawie dawnego systemu, maskując to dodaniem w nagłówku depeszy trójliterowej grupy sugerującej użycie nowej procedury. Jednak 1 sierpnia 1939 roku nastąpiła całkowita zmiana procedury, której nie zdążyliśmy już rozpracować. Od tej pory depesze w sieci S.D. bronią się przed atakiem. Ostatnim złamanym dniem był 31 lipca 1939 roku.

Ze względu na brak źródeł nie jest obecnie możliwe podanie chronologicznego wykazu zmian różnych elementów szyfru, jak księgi kodu, tabele szyfrowania kluczy, pozycji kluczy w tekście depesz itd.

34. Procedura szyfrowa niemieckiej marynarki przed wprowadzeniem Enigmy

Procedury szyfrowe używane przez niemiecką Kriegsmarine różniły się istotnie od wykorzystywanych przez wojska lądowe i lotnictwo, choć począwszy od 1934 roku używano w niej identycznej maszyny Enigma, jak w pozostałych rodzajach sił zbrojnych. W ramach prezentacji osiągnięć w tym obszarze chronologiczne przedstawianie wszystkich prac byłoby niecelowe. Zostały one zresztą krótko zrekapitulowane na końcu niniejszego szkicu.

Depesze wymieniane w ramach sieci radiowej niemieckiej Kriegsmarine były szyfrowane w grupach po dwie, trzy lub cztery litery, przy czym nie występowały grupy niepełne. Zasadniczym wariantem były grupy czteroznakowe i tylko on był analizowany przez polskie Biuro Szyfrów.

Czteroznakowe grupy z lat 1926–1927 reprezentowały najczęściej szyfrowany kod. Pierwsza i ostatnia grupa depeszy stanowiła grupę ślepą lub znacznik depeszy. Pozostałe grupy były zaszyfrowanymi słowami kodu. Ani szyfrowanie, ani sam kod nie zostały rozwiązane.

W latach 1926–1927 używano dwóch czteroznakowych procedur. Jedna z nich stanowiła zwykły, nieszyfrowany kod. Jego księga kodowa została rozwiązana w 1933 roku. Grupy kodowe składały się wyłącznie z 18 znaków:

A B E F G I K L N O P S T U W X Y Z

Księga kodowa była obszerna i obejmowała ponad 90 000 słów kodowych, spośród których poznaliśmy znaczenie ok. 10 000[2].

35. Maszyna szyfrująca marynarki z 29 klawiszami

W okresie od stycznia 1926 do września 1934 roku niemiecka Kriegsmarine używała do szyfrowania swych radiogramów maszyny szyfrującej. Była to maszyna typu Enigma, jednak różniła się ona w szczegółach od Enigmy używanej w wojskach lądowych:

1) maszyna posiadała 29 klawiszy i tyleż lampek dla 29 znaków niemieckiego alfabetu z umlautami;
2) przy naciśnięciu klawisza X zapalała się zawsze lampka oznaczona X;
3) maszyna nie miała ani połączeń wtyczkowych, ani łącznicy;
4) walec wejściowy miał następujące połączenia:

A	Ä	B	C	D	E	F	G	H	I	J	K	L	M	N	O	Ö	P	Q	R	S	T	U	Ü	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

Maszyna dysponowała pięcioma wirnikami, z których trzy były użytkowane jednocześnie;

5) występy wirników były połączone nie z pierścieniem, lecz z wkładką wirnika;
6) reflektor był ruchomy; można było go ustawiać tak, jak każdy z pozostałych wirników;
7) pierścienie były opisane liczbami od 1 do 28.

Jakkolwiek maszyna była w użyciu już od 1926 roku, to udało się ją zrekonstruować dopiero na podstawie depesz z lat 1931–1934. W tym okresie depesze były szyfrowane analogicznie jak w wojskach lądowych, tzn. w każdym dniu istniała wspólna pozycja bazowa, od której rozpoczynano dwukrotne szyfrowanie trójznakowego klucza depeszy. Tak otrzymane trójliterowe grupy uzupełniano ślepą literą do czterech znaków, a następnie umieszczano je: pierwszą na początku i drugą na końcu depeszy. Wobec obu grup można było wykorzystać opracowaną na potrzeby maszyny wojsk lądowych teorię cykli.

Budowa podstawień A_1A_4, A_2A_5 i A_3A_6 była jednak utrudniona na skutek niewystarczającego materiału szyfrowego. Tym trudniej przychodziło wyznaczenie samego klucza depeszy. Uległo to zmianie dopiero w 1933 roku, gdy zauważyliśmy, że klucze depesz, wybierane z katalogu, nie wykorzystują umlautów. Można było od tej pory przyporządkować cykle wzajemnie, tak aby znaki pierwszej grupy zaszyfrowanego klucza depeszy przypadały na umlauty.

Dalszą trudnością była nieznajomość połączeń walca wejściowego. Szczęśliwie zdołaliśmy odgadnąć je podobnie, jak w przypadku maszyny wojsk lądowych. Założyliśmy

[2] Drugi typ czetroliterowych grup okazał się później szyfrem maszynowym. Został on omówiony na stronie 181.

przy tym, że w maszynie brakuje łącznicy, co okazało się trafną hipotezą. W przeciwnym wypadku próba rekonstrukcji maszyny zapewne zakończyłaby się niepowodzeniem. Następnie ustalono, podobnie jak w maszynie wojsk lądowych, połączenia wirników.

W tym momencie można było powrócić do depesz z poprzednich lat. W 1936 roku w okresach obejmujących kilka dni wszystkie depesze były szyfrowane w jednej i tej samej pozycji wirników (jednak odmiennej od Enigmy wojsk lądowych). Aby odczytać tekst jawny depesz w tych okresach, postępowano następująco.

Poszukiwano dwóch depesz, które najprawdopodobniej zawierały ten sam tekst jawny, jednak szyfrant w jednej z nich opuścił jedną literę. Naciśnięcie bezpośrednio po sobie klawiszy odpowiadających sobie znaków obu depesz powinno dać ten sam tekst jawny. Za pomocą rusztu otrzymywano pozycję prawego wirnika i następnie, już bez istotnych trudności, pozycje pozostałych wirników. Ustalono przy tym, że tekst jawny przed zaszyfrowaniem był uprzednio kodowany z użyciem tego samego kodu, który wykorzystywano także bez maszyny i który zdołaliśmy częściowo rozwiązać. Jak już wcześniej nadmieniliśmy, był to kod o grupach czteroznakowych, zawierających znaki z 18-znakowego alfabetu obejmującego ABEFGIKLNOPSTUWXYZ. Poza tym okresem nie zdołaliśmy złamać szyfru dla innych dni. Ustalono jedynie, że kolejność wirników, pozycja reflektora i pierścieni oraz klucz depeszy (w procedurze nie występowała pozycja bazowa) zmieniały się w nieregularnych odstępach czasu: od 3 do 15 dni.

W dniu 1 stycznia 1927 roku zmieniła się nie tyle procedura szyfrowania, ile książka kodowa, która została zastąpiona przez nową. Można było od tej pory odtwarzać klucze w następujący sposób: w szeregu depesz wybierano te, w których podejrzewano zakończenie w postaci grupy kodowej odpowiadające frazie „Fortsetzung folgt[3]". Ponieważ maszyna ma właściwość polegającą na tym, że znaki tekstu jawnego i odpowiadające im znaki szyfrogramu są różne (z wyłączeniem znaku X, który zawsze jest szyfrowany jako X), znalezienie tych grup (niezaszyfrowanych) było zawsze możliwe, a na ich podstawie po zastosowaniu rusztu można było określić pozycje wirników dla pewnego okresu. Okazało się, że nowa książka kodowa wykorzystuje wszystkie 29 znaków, włącznie z umlautami, ze względu na brak czasu nie udało się jej jednak rozwiązać. 1 stycznia 1929 r. nastąpiła kolejna zmiana, tym razem dotycząca samej procedury szyfrowania. Polegała ona na tym, że obecnie każda depesza posiadała własny klucz depeszy, przekazywany za pośrednictwem grupy dodawanej na początku i końcu depeszy, której funkcji nie zdołaliśmy jednak rozwikłać.

W dniu 1 maja 1931 r. nastąpiła kolejna zmiana procedury szyfrowania, której rezultatem było szyfrowanie klucza depeszy w sposób analogiczny jak w wojskach lądowych. Dzięki temu zdołano ustalić połączenia wirników. Można było przystąpić do odczytywania tekstów jawnych depesz. Usiłowaliśmy odgadnąć brzmienie grup kodu, jednak po kilku miesiącach wytężonej i bezskutecznej pracy przypadkowo odkryto, że tekst jawny nie jest kodowany (analogicznie jak w wojskach lądowych). Procedura szyfrowania okazała się, jak już wspomniano, identyczna z używaną w wojskach lądowych i Luftwaffe. Funkcjonowały w niej jednak tzw. ustawienia wewnętrzne, tj. kolejność wirników, pozycja reflektora i pozycja pierścieni, które jak dotychczas były zmieniane w nieregularnych odstępach czasu, podczas gdy pozycja bazowa była zmieniana codziennie.

Klucze depesz były wybierane z listy. Czy dlatego, że lista nie była dość obszerna, czy też dlatego, że szyfranci wybierali z niej ciągle te same pozycje, klucze depesz powtarzały się na tyle często, że możliwe okazało się przygotowanie staty-

[3] Ciąg dalszy nastąpi.

styki, która pozwalała na rekonstrukcję podstawień A_1A_4, A_2A_5, A_3A_6, przy czym brak umlautów okazał się pomocny. Cyklometr był bezużyteczny, opracowane z jego pomocą katalogi musiałyby bowiem obejmować:

$60 \times 28^4 = 36\,879\,360$

pozycji, co było niewykonalne. Tak więc pozycję prawego walca wyznaczano z zastosowaniem rusztu, co było łatwe ze względu na brak łącznicy. Pozycje pozostałych wirników wyznaczano, korzystając z wykazu podobnego do wykazu F w wojskach lądowych i Luftwaffe. Różnica sprowadzała się do jego większej objętości, obejmował on bowiem

$28^3 = 21\,952$ pozycji.

Usiłowano zapewnić minimalną długość teksów jawnych depesz, używając m.in. wszelkich skrótów. Drugie i kolejne części depesz wieloczęściowych rozpoczynały się zawsze od liter FORT (skrót od 'Fortzsetzung' – kontynuacja). Aby ustalić pozycję bazową i pozycję pierścieni, wychodzono właśnie od liter FORT, podobnie jak w armii lądowej i lotnictwie używano AN, a w sieci S.D. liter QY.

36. Użycie przez niemiecką Kriegsmarine maszyny szyfrującej z 26 klawiszami

Począwszy od 1 października 1934 roku w niemieckiej Kriegsmarine używano identycznej maszyny Enigma, jak w wojskach lądowych. Procedura szyfrowania pozostała bez zmiany, z tą różnicą, że obecnie doszły połączenia w łącznicy (zawsze sześć par), które zmieniano codziennie, podobnie jak pozycję bazową. Do 15 listopada 1936 w Kriegsmarine używano dodatkowo dwóch wirników, jednak w maszynie jednocześnie montowano tylko trzy.

Przy wykorzystaniu cyklometru i katalogów opracowanych na potrzeby Enigmy wojsk lądowych można było teraz złamać klucze niewielkiej części (około jednej dziesiątej) depesz w okresie do 16 listopada 1936 roku. Nie wystarczało to jednak do rekonstrukcji listy kluczy depesz. Dopiero kiedy 16 listopada 1936 roku oba dodatkowe wirniki zostały wycofane, a w użyciu pozostały jedynie wirniki I, II i III, stało się możliwe opracowanie listy kluczy, a następnie z jej pomocą – kluczy depesz w okresie od 16 listopada. Dalej z wykorzystaniem rusztu określono połączenia obu dodatkowych wirników, które nazwano IVM i VM w odróżnieniu od używanych przez wojska lądowe i lotnictwo wirników IV i V.

Oprócz klucza ogólnego dla szczególnie ważnych depesz funkcjonowały także klucze oficerski i sztabowy (admiralski). Klucz oficerski był używany następująco: wybrany klucz depeszy był najpierw szyfrowany dwukrotnie począwszy od pozycji bazowej klucza ogólnego, po czym dwie otrzymane trójznakowe grupy były uzupełniane do czterech liter i dołączane, jak zwykle, na początku i końcu depeszy. Następnie otrzymany klucz był ponownie szyfrowany, począwszy od pozycji bazowej klucza oficerskiego, a rezultat tej czynności był używany do szyfrowania tekstu depeszy.

Nie wiadomo, jak funkcjonował klucz sztabowy. 1 maja 1937 r. nastąpiła zmiana procedury szyfrowania, która polegała na tym, że klucz depeszy nie był od tej pory szyfrowany z użyciem maszyny, lecz w odmienny i nieco skomplikowany sposób. Szczegóły nowego systemu szyfrowania poznano dopiero, gdy Anglikom

udało się w 1940 roku odnaleźć instrukcje procedury na pokładzie zatopionego U-Boota. Nie możemy opisać tutaj procedury szczegółowo, odsyłając czytelnika do fotograficznych reprodukcji zdobytych dokumentów.

Nieznajomość nowej procedury nie przeszkodziła nam uzyskać w ciągu 1937 roku wyników, które relacjonujemy poniżej.

Klucz depeszy był podawany w pierwszych dwóch grupach depeszy, które dla uniknięcia błędów powtarzano na jej końcu. Właściwy tekst zaczynał się zatem od trzeciej grupy. Stosując przedstawioną poniżej metodę, udało się odczytać wiele depesz z okresu pomiędzy 1 i 8 maja 1937 roku, a w konsekwencji zrekonstruować obowiązujące w tych dniach: kolejność wirników, połączenia łącznicy oraz częściowo ustawienia pierścieni. Porównanie ich z wewnętrznymi ustawieniami z końcówki kwietnia 1937 roku wykazało, że ustawienia wewnętrzne nie uległy zmianie 1 maja 1937 roku i pozostały stałe od 27 kwietnia do 8 maja. Porównanie kluczy złamanych depesz z pierwszymi i ostatnimi grupami dało następujące wyniki.

Jeśli we wszystkich złamanych kluczach danego dnia podzielić obie pierwsze grupy na pary stojących obok siebie znaków, oraz jeśli dwie depesze mają jednakowe pierwsze, drugie i trzecie pary znaków, to mają jednakowe także pierwsze, drugie i trzecie litery klucza depeszy. Nie zachodzi jednak odwrotna relacja; jednakowe litery mogą odpowiadać różnym parom. Ponadto równe pary znaków w różnych miejscach odpowiadają różnym literom klucza depeszy.

Przy zmianie procedury szyfrowania 1 maja 1937 roku oprócz zachowania wcześniejszych ustawień wewnętrznych szyfranci Kriegsmarine popełnili jeszcze jeden poważny błąd. Ponieważ jeden z okrętów nie został w porę wyposażony w instrukcję użycia nowej procedury, w ciągu pierwszych trzech dni maja 1937 pracował on, posługując się starą procedurą. Dzięki temu mogliśmy 2 i 3 maja 1937 roku odtworzyć ustawienia bazowe dla kluczy ogólnego i oficerskiego.

Później Brytyjczycy zdołali ustalić, co następuje:

Jeżeli klucze depesz zaszyfrowanych nową procedurą zostaną odszyfrowane zrekonstruowanymi pozycjami bazowymi z 2 i 3 maja, to tym samym parom znaków odpowiadają te same znaki odszyfrowanego klucza, nawet jeśli występują one w różnych miejscach.

Zawartość depesz w okresie od 1 do 8 maja 1937 roku znajdowano w następujący sposób: załóżmy, że mamy depeszę, która po skreśleniu pierwszych dwóch grup zaczyna się następująco:

VLPP WGKS WKUL QBOR

Dalej załóżmy, że depesza ta stanowi kontynuację innej depeszy, w której nagłówku figurowała godzina nadania 16:23. Zgodnie z doświadczeniem tekst jawny depeszy musi zaczynać się od znaków:

F O R T Y Q Z W E Y Y Q Z W E Y

(QZWE oznacza 1623). Znamy zatem 16-znakowy fragment depeszy, zarówno w wersji jawnej, jak zaszyfrowanej. Ponieważ w marynarce używano tylko sześciu par połączeń w łącznicy, część znaków musi wystąpić w niezmienionej postaci. Można zatem poczynić pewne założenia dotyczące liter, które nie ulegną zmianie, i weryfikować te założenia albo bezpośrednio na maszynie z użyciem rusztu lub przez wykorzystanie płachty Jeffreysa, brytyjskiego wynalazku odpowiadającego

naszemu katalogowi F. W każdym przypadku wymaga to długiej pracy, która opłaca się jedynie wtedy, gdy chodzi o analizę nowej procedury szyfrowej.

Anglicy zdołali złamać kilka depesz z 1938 roku. W tym okresie w użyciu był już reflektor B. Najwidoczniej został on wprowadzony do użytku w Kriegsmarine w tym samym momencie co w wojskach lądowych. Bez zmiany pozostała liczba sześciu par połączeń w łącznicy.

W 1940 roku Anglicy znaleźli na pokładzie zatopionego U-Boota dwa wirniki noszące oznaczenia VI i VII. Nie wiadomo obecnie, czy w marynarce używa się wirników I, II, III, VI i VII, czy też kompletu od I do VII.

37. Chronologiczny przegląd zastosowania maszyny szyfrującej Enigma w niemieckiej marynarce

<table>
<tr><td>1926</td><td rowspan="4">Maszyna szyfrująca marynarki „Enigma“ (29 klawiszy)</td><td rowspan="4">5 wirników</td><td rowspan="4">Ustawienie wewnętrzne: kolejność wirników, ustawienie reflektora i ustawienie pierścieni</td><td rowspan="8">Ustawienie wewnętrzne zmienne w nieregularnych odstępach czasu (3–15 dni)</td><td rowspan="4">Pozycja bazowa zmieniana jednocześnie z ustawieniami wewnętrznymi</td><td rowspan="4">Klucz depeszy= = pozycja bazowa</td><td rowspan="4">Kod 18-znakowy</td></tr>
<tr><td>1927
1928</td></tr>
<tr><td>1929
1930
kwiecień 1931</td></tr>
<tr><td>maj 1931
1932
1933
wrzesień 1934</td></tr>
<tr><td>październik 1934
1935
15 listopada 1936</td><td rowspan="5">Maszyna szyfrująca „Enigma“ (26 klawiszy)</td><td>reflektor A</td><td>5 wirników
I, II, III, IVM i VM</td><td rowspan="3">Pozycja bazowa i ustawienia łącznicy zmieniane codziennie</td><td rowspan="3">Pozycja bazowa zmieniana codziennie</td><td rowspan="3">Pierwsza procedura szyfrowania</td><td rowspan="3">Kod 29-znakowy</td></tr>
<tr><td>16 listopada 1936
kwiecień 1937</td><td rowspan="3">3 wirniki
I, II, III</td></tr>
<tr><td>maj 1937
październik 1937</td><td rowspan="2">reflektor B</td></tr>
<tr><td>listopad 1937
1938</td><td rowspan="2">Druga procedura szyfrowania</td><td rowspan="3">Tekst jawny</td></tr>
<tr><td>1939
1940</td><td>5 wirników
I, II, III, VI i VII</td><td>Trzecia procedura szyfrowania</td></tr>
</table>

38. Udział trzech państw w złamaniu Enigmy

I. Polska
Teoria cykli.
Teoria podstawień.
Połączenia wirników I–III i reflektora A.
Metoda rekonstrukcji walca wejściowego.
Metoda rekonstrukcji połączeń łącznicy.
Metoda charakterystycznych kluczy depesz.
Metoda statystyczna.
Metoda nierównych liter.
Określanie prawego wirnika. Ruszt i katalog F.
Cyklometr (urządzenie i katalog).
Odtwarzanie tekstu jawnego.
Połączenia reflektora B.
Połączenia wirników IV i V.
Analiza drugiej procedury szyfrowania.
Bomby.
Płachty Zygalskiego (projekt).
Katalogi do płacht (projekt).
Analiza trzeciej procedury szyfrowania.
Sieć radiowa S.D.
Enigma floty z 29 klawiszami.
Połączenia wirników IVM i VM.
Analiza procedury szyfrowania floty od 1 maja 1937.

II. Anglia
Płachty Zygalskiego (wykonanie).
Katalogi do płacht (wykonanie).
Metoda Jeffreysa.
Metoda Knoxa.
Metoda Herivela.
Wirniki VI i VII (znalezione na pokładzie U-Boota).

III. Francja
Dostarczenie dwóch ważnych dokumentów.

Przekład oryginału na język angielski

Table of Contents

1. Introduction 215
2. Beginnings 215
3. Cycle theory 216
4. Two important documents 216
5. Substitution theory 217
6. Substitution E 219
7. Substitution S. 220
8. A few numbers 220
9. Message key recovery 221
10. Method of non-random keys 222
11. Statistical method 222
12. Method of unequal letters 222
13. Determination of the right rotor 223
14. The Grill method. 224
15. F catalogue 225
16. Cyclometer. 225
17. Base position and ring position 226
18. Some remarks 226
19. New networks. Continuous changes 226
20. Reflector B 227
21. New rotors 227

22. Change of ciphering procedure 227
23. Determination of rotor order 228
24. Bombs 229
25. Zygalski sheets 229
26. Warsaw conference 231
27. Outbreak of war. Vignolles 231
28. Knox method 232
29. Catalogues for Zygalski sheets 232
30. Herivel method 233
31. Third ciphering procedure 233
32. Chronology of changes in ciphering procedures of army and air force . . 234
33. Sicherheitsdienst wireless network 234
34. Kriegsmarine ciphering procedure before Enigma 235
35. Kriegsmarine ciphering machine with 29 keys 236
36. Kriegsmarine use of ciphering machine with 26 keys. 238
37. Chronology of changes in ciphering procedures of the German navy. . . 240
38. 150The Contributions of three countries to Enigma breaking 241

1. Introduction

A few years after the end of the First World War, the German armed forces had already started to use the Enigma ciphering machine to encrypt messages transmitted by radio.

The new ciphering procedure seems to have been introduced first by the navy. In any case, it is known that the navy was already using it in 1926, while the use of the procedure in the army has been confirmed since 15th July 1928.

On 1st August 1935, Enigma was introduced to the Luftwaffe, from September 1937 it was used by the Sicherheitsdienst (S.D.), and the machine was also used by the police.

As the scope of Enigma's use in the German armed forces widened, other methods of encryption, e.g. double transposition, started to disappear, and long before the outbreak of the German-Polish war in 1939, almost all messages sent by radio from German military or even semi-military institutions were encrypted with Enigma. The solution to this encryption was therefore of paramount importance for the military staffs of Poland, France and Great Britain. Over time, the machine was modified several times. Before the introduction of the M-type machine with a switchboard, which remains in use until now, the army was using Enigma G with so-called plugs from 15th July 1926 to 31st May 1930. For some time, military district commands used a printing Enigma called "Enigma II", which, however, quickly went out of use as it was found to be impractical. Until September 1934, the German navy used a machine with 29 keys instead of 26, and it was only in 1934 that it switched to the same type of machine as was used in the army. Incidentally, the navy retained a certain level of autonomy later on, including the use of more rotors than other services. In principle, however, it can be stated that from October 1934 until today all German services are using the same model of machine, which entered into operation in the army on 1st July 1930.

Below we present an overview of the activities of the Cipher Bureau of the Polish Main Staff, which resulted not only in reconstructing the Enigma model described above, but also in developing methods to read the intercepted cipher material almost on an ongoing basis, despite all the changes and improvements constantly introduced by the German cryptologic service in order to secure communication. The importance of cooperation in this area between the Staffs of Poland, France and Great Britain is also discussed.

2. Beginnings

Many years after the creation of the Polish Cipher Bureau, the shortage of staff did not allow attention to be paid to the cipher material coming from the German navy. Therefore, the appearance of the Enigma was noted for the first time only in 1928 when the army started to use it.

Among the messages coming from German military stations appeared those that were not encrypted by the double transposition cipher used up till now, but

by another cipher, undoubtedly using some substitution method. Their analysis allowed them to find out that the first six characters of each message are of special importance, probably representing the message key. At the same time a number of documents were obtained by Polish intelligence service, which showed that since 15th July 1928, a new cipher marked 'Maschinenschlüsselverfahren Enigma G' had entered into force in the German army alongside the previous one, that there is an element in the Enigma machine known as a plug connection (in later models known as the switchboard), and that each station receives a number of keys consisting of three numbers in the range 1 to 26.

It was obvious that the new cipher was identical to the procedure using Enigma. In order to facilitate its analysis, Polish staff purchased an Enigma of a commercial type, in which the rotor wiring was obviously different from the machine used by the army. In the course of later studies it also turned out that it differs from military counterpart in many other respects. The research into the new cipher did not register significant progress and after some time it was abandoned.

3. Cycle theory

The work was restarted in 1932. Re-examination of the six-character message headers allowed the determination of the following: for every day a certain rotor position is selected, the same for all the cipher clerks. Each clerk selects also three arbitrary letters, enciphers them two times in succession starting from the common position valid on a given day, inserting the six letters received at the beginning of the message.

In this way, looking at the 1st and the 4th, the 2nd and the 5th, and the 3rd and the 6th letters of a message, certain relationships emerge which can be studied in a purely mathematical way and which form the basis for the subsequent reconstruction of Enigma.

The following procedure is observed: one selects any message recording its first, and to its right, the fourth letter. Then one finds a message in which the just written-down character appears as the first character, writing the fourth character to the right of the previous one. One proceeds in this way until returning to the letter written first. The result is called a cycle. The following theorems can be proven:

1. An even number of cycles of the same length always appear.
2. Characters of one cycle are referenced by characters being the elements of another cycle of the same length.
3. If an X character is referenced by a character Y, a character standing to the right of X is referenced by a character standing to the left of Y.

These three theorems represented a partial solution to the task of reconstructing the message keys and the problem would have been fully solved except that two documents directed the work to other tracks.

4. Two important documents

At that time Polish Cipher Bureau acquired two documents of extraordinary importance. The first document was entitled *Machine Encryption Manual*, the second one contained the so-called keys of the day for October and December 1931. The Polish intelligence service received these documents from the French General Staff ha-

ving obtained them through its agents. It should be stressed that these documents, and in particular the daily keys, decisively influenced the progress of work. Without them, the Enigma cipher solution would have been delayed for years. On the other hand, it should be noted that neither the French nor the British authorities managed to break the cipher despite the fact that both of them had the same documents at their disposal. Moreover, below we describe the method that would probably have led to the objective even without these documents.

The first of these documents confirmed that Enigma with plugs had been replaced by a new model with a switchboard on 1st July 1930. It was subsequently established that:

1) the machine contains 3 ciphering rotors, the order of which can be changed. The rotor order is changed every three months;
2) the reflector is stationary (as opposed to that of the commercial model);
3) rotors are fitted with rings marked with either letters or numbers. The ring position is changed daily;
4) the switchboard interconnects 6 pairs of characters. The interconnections change every day;
5) the starting position at which message key is enciphered is referred to as the base position. The base position is changed on a daily basis.

The second document contained, as already mentioned, the daily keys, i.e. the rotor order, the base position, the ring settings and the switchboard connections for a period of two months.

5. Substitution theory

We are now moving on to the solution of the main problem, i.e. reconstruction of rotor wiring. To achieve that goal we used a mathematical theory, the so-called theory of substitutions, which we do not present in detail below, assuming its knowledge by the reader. Obviously it cannot be assumed that the knowledge of several theorems of this theory was sufficient to achieve the goal. On the contrary, a whole series of obstacles had to be overcome on the way. Below we present the main course of our reasoning. The Enigma Cipher is a substitution cipher, i.e. in every rotor position, the machine substitutes one letter of the alphabet with another letter. We define the substitution taking place at the base position as A_1, in the next position as A_2, and so on up to A_6.

If one has enough messages at his disposal (80 on average), one can use the substitution theory to determine the products A_1A_4, A_2A_5, A_3A_6, which from now on are considered as known. Let us define:

S substitution generated by the switchboard
C_γ ″ ″ ″ right rotor
C_β ″ ″ ″ middle rotor
C_α ″ ″ ″ left rotor
U ″ ″ ″ reflector
E ″ ″ ″ entry drum
Q = (1,2,3,4,5,6, ..., 24,25,26)

When the middle rotor does not move during encryption of the message key, which is probable and assumed in further considerations, substitutions A_1 to A_6 can be presented in the following form:

$$A_1 = \quad S\ E\ C\gamma C_\beta\ C_\alpha\ U\ C_\alpha^{-1}\ C_\beta^{-1}\ C\gamma^{-1}E^{-1}\ S^{-1}$$
$$A_2 = S\ E\ Q\ C\gamma Q^{-1} C_\beta\ C_\alpha\ U\ C_\alpha^{-1}\ C_\beta^{-1}\ Q\ C\gamma^{-1}\ Q^{-1}\ E^{-1}\ S^{-1}$$
$$A_3 = S\ E\ Q^2\ C\gamma Q^{-2} C_\beta\ C_\alpha\ U\ C_\alpha^{-1}\ C_\beta^{-1}\ Q^2\ C\gamma^{-1}\ Q^{-2}\ E^{-1}\ S^{-1}$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$A_6 = S\ E\ Q^5\ C\gamma Q^{-5} C_\beta\ C_\alpha\ U\ C_\alpha^{-1}\ C_\beta^{-1}\ Q^5\ C\gamma^{-1}\ Q^{-5}\ E^{-1}\ S^{-1}$$

The first problem to overcome is that both sides of equations consist of un= known values; we know only the products A_1A_4, A_2A_5, A_3A_6. However, the theory of cycles indicates that the substitution A_1 in most cases takes no more than a hundred representations, and each representation of A_1 unequivocally defines substitution A_4. The same applies to A_2 and A_5, A_3 and A_6. One can therefore imagine that we know all the representations A_1 to A_6. In this way we can consider the first problem as solved, although at the cost of a significant increase in labour, because in subsequent operations we have to take into account all possible representations A_1 to A_6.

The second problem is even more serious. Despite the greatest effort, which could be continued for years on the grounds of mathematical theory, even after the rotor wiring has been reconstructed, the above equation system could not be solved, with the main problem being the substitution S, generated by the switchboard. Finally, a method was found which would probably lead to the goal, but it assumed the knowledge of A_1 to A_6 (and not only their products A_1A_4, A_2A_5, A_3A_6), the knowledge of substitution E, and the availability of extensive cipher material.

The second and main difficulty on the road to Enigma solving was overcome with the help of the documents provided by the French headquarters, which included the switchboard settings for two months.

The third problem was the ignorance of the substitution E. It seems that it was precisely there that the efforts of British cryptologists failed. Subsequent research conducted by the Polish Cipher Bureau proved that substitution E could be determined analytically (given the knowledge of substitution S), but in reality it was found by means of trial and error. It was assumed that the substitution E could be identical to the commercial Enigma model, i.e.

Q	W	E	R	T	Z	U	I	O	A	S	D	F	G	H	J	K	P	Y	X	C	V	B	N	M	L
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

When this assumption did not give the required result, it was presumed that on the given day the middle rotor had moved during the ciphering of the message key. The process was repeated based on the cipher material from another day, and when no success was achieved, the operation was repeated for data from subsequent days. After no success was registered during a few months, consideration was given to discontinue that work. However, one more attempt was made, this time with the assumption of

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Fortunately, this time the assumption turned out to be correct and led to a solution of the problem.

For a better understanding by the reader, let us note that finding the connections of the right-hand rotor requires the transformation of the 6 equations defined above to the following form:

$$E^{-1}S^{-1}A_1SEQ^{-3}E^{-1}S^{-1}A_4SEQ^{3} = C_\gamma \quad [C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1} Q^{-3} C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1} Q^{3}]\, C_\gamma^{-1}$$
$$Q^{-1}E^{-1}S^{-1}A_2SEQ^{-3}E^{-1}S^{-1}A_5SEQ^{4} = C_\gamma Q^{-1} [C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1} Q^{-3} C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1} Q^{3}]\, Q C_\gamma^{-1}$$
$$Q^{-2}E^{-1}S^{-1}A_3SEQ^{-3}E^{-1}S^{-1}A_6SEQ^{5} = C_\gamma Q^{-2} [C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1} Q^{-3} C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1} Q^{3}]\, Q^2 C_\gamma^{-1}$$

Despite their length, the equations are not particularly complicated. All expressions on the left side are known, all expressions on the right side have a common fragment. Its elimination allows to determine the $C_\gamma Q C_\gamma^{-1}$ and hence directly C_γ, i.e. wiring of the right-hand rotor.

Of course, it was necessary to determine the wiring of the left and middle rotors as well as their turnover positions; presentation of this process is omitted as the methods used were identical to just described.

6. Substitution E

We intend to sketch the way of recovering substitution E using the analytical method.

Since we hold the daily keys for two months, we can easily find two days in which both rotor order and right rotor position, i.e. the difference between base position and ring position, is identical. For both days we build a system of equations A_1 to A_6 by substituting

$$F = C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1}$$

and marking the variables representing the second day with underscore:

$$\begin{aligned}
A_1 &= S\ E\ C_\gamma\ F\ C_\gamma^{-1} E^{-1}\ S^{-1} & \underline{A_1} &= C_\gamma \underline{F}\ C_\gamma^{-1} \underline{E}^{-1} \underline{S}^{-1} \\
A_2 &= SE\ Q C_\gamma Q^{-1} F\ Q\ C_\gamma^{-1} Q^{-1} E^{-1} S^{-1} & \underline{A_2} &= \underline{S}E\ Q\ C_\gamma Q^{-1} \underline{F}\ Q\ C_\gamma^{-1} Q^{-1} E^{-1} \underline{S}^{-1} \\
A_3 &= SE\ Q^2 C_\gamma Q^{-2} F\ Q^2 C_\gamma^{-1} Q^{-2} E^{-1} S^{-1} & \underline{A_3} &= \underline{S}E\ Q^2 C_\gamma Q^{-2} \underline{F}\ Q^2 C_\gamma^{-1} Q^{-2} E^{-1} \underline{S}^{-1} \\
&\ \vdots\ \ \vdots\ \ \vdots\ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots & &\ \vdots\ \ \vdots\ \ \vdots\ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots \\
A_6 &= SE\ Q^5 C_\gamma Q^{-5} F\ Q^5 C_\gamma^{-1} Q^{-5} E^{-1} S^{-1} & \underline{A_6} &= \underline{S}E\ Q^5 C_\gamma Q^{-5} \underline{F}\ Q^5 C_\gamma^{-1} Q^{-5} E^{-1} \underline{S}^{-1}
\end{aligned}$$

On that basis we create the following equations, the right side of which is known:

$$\begin{aligned}
S^{-1}A_1S\underline{S}^{-1}\underline{A_1}\underline{S} &= E C_\gamma F\ \underline{F}\ C_\gamma^{-1} E^{-1} \\
S^{-1}A_2S\underline{S}^{-1}\underline{A_2}\underline{S} &= EQ C_\gamma Q^{-1} F\ \underline{F}Q\, C_\gamma^{-1} Q^{-1} E^{-1} \\
&\ \vdots\ \ \vdots\ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots \\
S^{-1}A_6S\underline{S}^{-1}\underline{A_6}\underline{S} &= EQ^5 C_\gamma Q^{-5} F\ \underline{F}Q^5 C_\gamma^{-1} Q^{-5} E^{-1}
\end{aligned}$$

Eliminating $F\underline{F}$ we obtain:

$$\begin{aligned}
&E\,(Q\,C_\gamma\,Q^{-1}C_\gamma^{-1})\quad E^{-1} \\
&E\,Q\ \ (Q\,C_\gamma\,Q^{-1}C_\gamma^{-1})\,Q^{-1}\,E^{-1} \\
&E\,Q^2\,(Q\,C_\gamma\,Q^{-1}C_\gamma^{-1})\,Q^{-2}\,E^{-1} \\
&\ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots\ \ \vdots \\
&E\,Q^4\,(Q\,C_\gamma\,Q^{-1}C_\gamma^{-1})\,Q^{-4}\,E^{-1}
\end{aligned}$$

Hence, eliminating $QC_\gamma Q^{-1}C_\gamma^{-1}$, and then $EQ^{-1}E^{-1}$ we directly obtain E.

The road to the solution is a bit long, in particular when we do not know A_1 to A_6, but only their products A_1A_4, A_2A_5, A_3A_6; the actual execution of the outlined operations would probably require a few months of one person's work. However, we have proved that knowing the switchboard setting we can reach the goal in the way just described.

7. Substitution S

In conclusion, we want to demonstrate how we can achieve this goal without knowing the keys for two months. Note that the method outlined below is based on the knowledge of substitution E, or at least on guessing it, as was actually the case. Knowledge of substitutions A_1 to A_6, and not only of their products A_1A_4, A_2A_5, A_3A_6, is assumed, which could certainly also be achieved. Finally, the method requires a sufficiently large amount of cipher material to be able to determine the A_1 to A_6 substitutions for several hundred days. If the above assumptions can be met, there will be two days in which the rotor order is identical, the difference between the base position and the left and middle rotor ring positions is identical, and the difference between the base position and the right rotor ring position does not exceed three positions. If this occurs, it should be easily identifiable. We assume therefore, that the positions of the right rotor for both days differ by 3, so that the substitutions A_1 and A_4 are created in the same rotor position. Next, the products A_1A_2 and A_4A_5 on the one hand and A_2A_3 and A_5A_6 on the other hand must be similar, as can easily be seen by writing down the corresponding equations in the form:

$$A_1A_2=S(EGQGQ^{-1}E^{-1})S^{-1} \qquad \underline{A_4}\underline{A_5}=\underline{S}(EGQGQ^{-1}E^{-1})\underline{S}^{-1}$$
$$A_2A_3=S(EGQGQ^{-2}E^{-1})S^{-1} \qquad \underline{A_5}\underline{A_6}=\underline{S}(EGQGQ^{-2}E^{-1})\underline{S}^{-1}$$

where shortcut $C_\alpha C_\beta C_\gamma U C_\gamma^{-1} C_\beta^{-1} C_\alpha^{-1} = G$ was applied.

Subsequently equations A_1A_2 and $\underline{A_4}\underline{A_5}$ and the equations A_2A_3 and $\underline{A_5}\underline{A_6}$ can be used to determine the product $S\underline{S}$, which in both cases should be equal. Moreover, the product $S\underline{S}$ should consist of at least 14 cycles.

The main difficulty is that in the described way we determine the product of $S\underline{S}$, and not substitutions S and $\underline{S}$. However, it turns out that in general S and $\underline{S}$ can take several hundred different forms. Their values must be substituted into our equations trying to achieve a result. This represents a considerable effort that would probably prove impossible, especially if no substitutions A_1 to A_6 were known, but only their products.

8. A few numbers

A full description of Enigma would go beyond the scope of this sketch. However, we would like to give some figures illustrating how strong the challenge of Enigma is from a cryptological point of view, assuming that it is being used properly.

The number of possible rotor arrangements for the three rotors is as follows

$$3\times2\times1 = 6$$

and for five rotors

$5 \times 4 \times 3 = 60$.

The number of different base positions and ring positions is equal to

$26^3 = 17\,576$.

The number of possible rotor positions for three rotors (including rotor order) is equal to

105 456,

and for five rotors

1 054 560.

The number of different combinations in the switchboard for six pairs of letters is equal to

$(26!)/ (2^6 \times 6! \times 14!) = 10\,039\,179\,150\,000$

and for ten pairs

$(26!)/ (2^{10} \times 10! \times 6!) = 1\,507\,382\,727\,437\,250$.

The number of possible reflector connections is equal to

$(26!)/ (13! \times 2^{13}) = 790\,585\,353\,580\,625$

and for the rotors

$26! = 403291587620262925520000000$.

The last figure can be summarised as follows: if every person living on Earth had tried one possible connection every second, the entire work would have been completed after six billion years (but the Earth has only existed for two billion years so far).

9. Message key recovery

So far we have solved the following problem: reconstructing the rotor wiring, assuming knowledge of the keys for two months. However, the task does not end there. This time it is all about solving the opposite problem: with known rotor wiring, to find the key to the cipher.

The technical services of the Polish Cipher Bureau modified a commercial machine so that it could be used for reading military messages. Next, the cipher material from the two month period for which keys were known, was read, permitting

identification and obviously exploitation of a number of errors made by the cipher clerks. These errors were used to recover the message keys, i.e. keys selected by the cipher clerks, enciphered twice and attached at the beginning of the message. Over the years, the Germans managed to train their cipher clerks to such an extent that they made fewer and fewer mistakes, but it was a slow process; so slow that it was possible to develop more and more sophisticated methods of recovering the message keys.

10. Method of non-random keys

In the first period after the introduction of Enigma, the cipher clerks demonstrated a predilection for keys consisting of three identical letters, like AAA, BBB, etc. The method of non-random keys was based on the use of the theory of cycles to assign individual cycles in such a way that as many keys as possible were composed of three equal letters. Soon, however, the cipher clerks were forbidden to choose keys consisting of the three same letters. As a result, they started to select the characters based on the machine keyboard layout

Q W E R T Z U I O
A S D F G H J K
P Y X C V B N M L

using neighbouring letters in rows or in diagonals, such as ASD, QAY, QWE, etc. Now it was enough to assign the cycles so that as many keys as possible of the ASD type and similar could be created.

11. Statistical method

Soon, however, that practice was also banned. In the meantime, however, it has been noted that characters are found in keys with an uneven frequency. For example, A and Q were the most frequent letters followed by all vowels, and letters L and O as the next frequent group. Other letters, such as J and Y, were only occasionally present. Character frequency statistics were prepared and cycles were ordered in order to obtain the best possible match with statistical data. Frequency of character occurrence varied, however, over time, so the statistics had to be updated. In addition, the frequency of characters differed between the army and the Luftwaffe. In the S.D., keys were selected so carefully that all the characters were present with the same frequency – the statistical method proved impossible to use.

12. Method of unequal letters

After forbidding the choice of three equal letters as a message key, the cipher clerks carefully avoided keys with at least two equal characters, such as AAB or FVF. This custom has proved to be the most enduring of all and has been followed to this day. The advantage of the method based on it is that it can be fully automated.

Let's assume that on a given day we received cycles in the following form:

(SAIZELWDPBOHU)(YCRKXFJQNGVMT)
(AZHNUGWMSFLR)(QBYKPDEVJIOT)(C)(X)
(AZCSYBVMFJPDO)(NUGTIRHQKXEWL)

Now we need to draft the following table and two corresponding tables, deleting those positions in its free fields which imply the equality of two characters.

S	TYCRKXFJQNGVM
A	MTYCRKXFJQNGV
I	VMTYCRKXFJQNG
Z	GVMTYCRKXFJQN
E	NGVMTYCRKXFJQ
L	QNGVMTYCRKXFJ
W	JQNGVMTYCRKXF
D	FJQNGVMTYCRKX
P	XFJQNGVMTYCRK
B	KXFJQNGVMTYCR
O	RKXFJQNGVMTYC
H	CRKXFJQNGVMTY
U	YCRKXFJQNGVMT
AZHNUGWMSFLR	

TOIJVEDPKYBQ
QTOIJVEDPKYB
BQTOIJVEDPKY
YBQTOIJVEDPK
KYBQTOIJVEDP
PKYBQTOIJVED
DPKYBQTOIJVE
EDPKYBQTOIJV
VEDPKYBQTOIJ
JVEDPKYBQTOI
IJVEDPKYBQTO
OIJVEDPKYBQT

C

X	

With enough messages at our disposal, there will be only one case left in the end.

13. Determination of the right rotor

After we were able to recover in most cases the message key, we could proceed to the reconstruction of the daily key, i.e. the order of rotors, switchboard connections, base position and ring positions. Let us start from determining the rotor order.

If we write two sentences in German, each 100 characters long, one under another, we will usually find 8 columns with identical characters. This property also applies if both sentences are encrypted with the same key. However, if we take two meaningless texts in which the frequency of characters corresponds to the natural frequency for German, and write them down one below the other, we find on average only four columns containing equal characters. This property can be used to identify the right-hand rotor. If one has enough cipher material, one can find a number of message pairs in which the first two characters of message key are identical and the third characters are different. Both messages can be written one under another so that the characters coded in the same rotor positions are placed in columns. *A priori* two mutual assignments are possible, depending on whether the middle rotor has moved during encryption. By counting the number of columns containing equal characters we will find twice as many pairs in the case of the correct assignment (at least in general) as in the case of false one. In this way, it is possible to determine the range of characters where the rotation of the middle rotor occurred, and by analysing all pairs of messages, that range can be narrowed down to extent allowing unambiguous identification of the right-hand rotor. The remaining rotors shall be identified later in a different way.

14. The Grill method

The next phase of the work consisted of the reconstruction of the connections of the switchboard. This was a difficult problem, but finally a method was developed starting from the fact that, first of all, when encrypting the message key the middle rotor steps only in 5 cases, and secondly, the switchboard leaves some characters unchanged.

To illustrate this approach, let us assume that there are no connections in the switchboard. In this case, six equations describing A_1 to A_6 substitutions can be transformed to the following form:

$$
\begin{aligned}
&Q^{X} C_{\gamma}^{-1} Q^{-X} E^{-1} A_1 E Q^{X} C_{\gamma} Q^{-X} = F\\
&Q^{X+1} C_{\gamma}^{-1} Q^{-X-1} E^{-1} A_2 E Q^{X+1} C_{\gamma} Q^{-X-1} = F\\
&\vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots\\
&Q^{X+5} C_{\gamma}^{-1} Q^{-X-5} E^{-1} A_6 E Q^{X+5} C_{\gamma} Q^{-X-5} = F
\end{aligned}
$$

In the above equations all variables are known, except for the expression $F = C_{\beta} C_{\alpha} U C_{\alpha}^{-1} C_{\beta}^{-1}$ and exponent X. Even if, thanks to the method just described, we know the identity of the right-hand rotor, we do not know its position.

We proceed taking for X values from 0 to 25 in turn, and each time determining the value of F from the six equations above. Six values of the expression F differ in each case except for one, in which all six values are identical. In this way we determine X, i.e. the position of the right-hand rotor and the value of substitution F, which will be useful later on.

In practice, it is done in such a way that on a sheet of paper we write the second row of substitutions C_{γ}, $QC_{\gamma}Q^{-1}$,…, $Q^{25}C_{\gamma}Q^{-25}$ (the first lines are always in the form of 1 2 3 4 … 26)

19 3 15 23 11 20 4 16 26 10 14 22 2 17 6 25 9 1 21 12 18 5 24 13 8
2 14 22 10 19 3 15 25 9 13 21 1 16 5 24 8 26 20 11 17 4 23 12 7 6
13 21 9 18 2 14 24 8 12 20 26 15 4 23 7 25 19 10 16 3 22 11 6 5 17

(the example above is fictitious).

On the second sheet with rectangular openings (hence the name of "grill") we write out substitutions A_1 to A_6 in the following form:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

V T Z F K D R N O U E W Y H I S X G P B J A L Q M C

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

K Q H U V S Z C O N A T W J I Y B X F L D E M R P G

After the preparations described, we put the grill on the first sheet and shift it vertically until in a certain position identical values of the F are displayed in the windows. Such situation happens only when no connections are present in the switchboard. Otherwise switchboard connections distort the picture, but considering that they do not modify all the letters, one can usually see some similarity between six substitutions F. Then one should try to adjust the characters of the substitutions A_1 to A_6 so that all the values of F are identical. If this happens, the transpositions of the characters define the switchboard setting, and as a bonus we obtain also the position of the right-hand rotor and the value of the F.

15. F catalogue

After recovering the identity and position of the right rotor, one could try to determine the identity and positions of the middle and left rotor by examining all possible cases. In order to avoid unnecessary work, a catalogue has been prepared, once and for all time, containing all possible values of substitution F, which amount to

$6 \times 26 \times 26 = 4056.$

Now it was enough to find in the catalogue the F value recovered during the switchboard setting recovery to determine immediately the identity and position of the right and middle rotor.

16. Cyclometer

The method used to recover switchboard connections was not only laborious and not very elegant, but also did not assure reaching the result. Moreover, it assumed knowledge of the message key, and the methods used to recover it were equally time-consuming and not always successful. As a result other methods were sought that could lead to the goal more quickly and more efficiently, starting from the ob-

servation that the structure of cycles was not only invariant against the switchboard settings, but also represented a daily key discriminant, as two days with identical structure of cycles occurred relatively rarely. Hence, it was already close to the idea of creating a catalogue of cycle structures for all possible 105 456 rotor positions.

In order to cope with this work a special device, the cyclometer, was constructed, consisting of two Enigma machines connected so that in each rotor position some even number, in the range 2 to 26, of lamps were lit depending on the length of the corresponding cycle. The completion of the whole work took more than a year, but since then the order of rotors, their starting positions, and the switchboard setting for a given day were usually found within few minutes.

17. Base position and ring position

The rotor position is always defined as the difference between the base position and the ring position. In order to reconstruct the daily key fully, it is necessary to find both missing elements, i.e. the base position and ring positions. The analysis of the message key is not sufficient for this purpose, and it is necessary to delve into its content.

After reading the material from October and December 1931, for which we had the key, it was noticed that many messages started with the two letters AN. In order to separate the base position and ring position, any message suspected of starting with AN was selected and then tried in all machine starting positions to see whether this assumption was correct. It was a boring work, considering that $26^3 = 17\,576$ possibilities had to be examined. Later it was found that if the message started with the AN phrase, some positions of the right-hand rotor were excluded from the assumption. Since we had many messages every day with a probable beginning of AN, it was usually possible to determine the position of the right-hand rotor completely analytically.

18. Some remarks

When describing the methods of the grill and of the cyclometer, it was assumed that there is a requirement that the middle rotor does not move during encryption of the message key. In fact, this requirement does not always have to be met, because the base position and the rings can be found even when the middle rotor moves. It will be left to the reader to determine when this is possible.

It was earlier noted that there were no letter repeats among the six letters forming the base position and the ring positions within the daily key. This observation not only led to a fundamental simplification of work, but in later years it was at the root of the so-called Herivel method, which is mentioned below. In general, there were periods when during the next four days all the 24 characters defining the base position and the ring positions were different. Similar observations were made at different times with regard to the switchboard settings.

19. New networks. Continuous changes

As the German armed forces expanded, the number of radio stations also increased. New radio networks have also appeared, using the same Enigma machine,

but operating with a different daily key. For example, the newly created German air force set up its own radio network with its own key starting from 1st August 1935.

Various changes have been made to ensure the security of the cipher. Starting 1st February 1936 the order of rotors was changed every month, and from 1st October 1936 even daily. At the same time the number of connection pairs in the switchboard has changed; instead of 6 pairs their number now ranged from 5 to 8. Finally on 2nd November 1937, the existing reflector was retired and replaced with a new one, the so-called Reflector "B".

20. Reflector B

German cipher clerks committed some reckless acts, mentioning in their messages from September 1937 the pending reflector change. As a result the Polish Cipher Bureau was prepared for a change and not surprised when on 2nd November it could not find the resulting cyclic structures in the catalogue. Nevertheless, the right-hand rotor and switchboard settings were on the same day recovered using the grill method.

The identities of the left and middle rotor and positions of both were unknown. There were 2×26×26 = 1352 possible cases and each of them defined one possible reflector. By comparing 1352 possible cases from two different days it was easy to determine the actual reflector.

21. New rotors

In September 1937, a new communication network was launched, belonging to the security service S.D., a political organisation that will be discussed further. The ciphering procedure corresponded roughly to that used by the army, but later some modifications were introduced. For example, on 15th September 1938, when the ciphering procedure used by the army and the air force was completely changed, the S.D. procedure remained unchanged for several months; a serious error that would immediately avenge itself. When three months later two new rotors were introduced, this time in all networks, the S.D. was still using the old procedure, which allowed us to determine the wiring of the new rotors in the same way, as we previously determined the wiring of reflector B. Without going into unnecessary details, let us only mention that we used data from two days in which the middle rotor moved. Had the S.D. implemented the new procedure beforehand, a purely analytic reconstruction of the IV and V rotor wiring would have been difficult.

22. Change of ciphering procedure

Thanks to the methods described above, up till September 1938, all the wireless networks of the army, the Luftwaffe, the security service and the navy (as will be discussed below) were read, often in an incredibly short time.

However, the situation changed completely when, on 15th September 1938, a new ciphering procedure was introduced, thereby endangering the previous achievements of the Polish codebreakers in this area.

In the new procedure, the base position for messages exchanged during the day was not fixed, changing from message to message.

Let us illustrate the new procedure with an example. The cipher clerk selects two triplets, e.g. SKR WTC, sets the machine to SKR position and enciphers the characters WTC twice (as before) producing the six characters KFDLSF.

The base position SKR is transmitted unencrypted in the message header, followed by the six characters KFD LSF, followed by the message text encrypted starting from the position WTC (also as before). The nature of the new ciphering procedure was known because some of the cipher clerks used it on the eve of the official introduction, which was obviously a grave error.

23. Determination of rotor order

As, in the new procedure, message keys were not enciphered starting from the same base position, the cycle theory and the methods based thereon – non-random message keys, grill, and cyclometer - became useless.

However, we did not give up proceeding to analyse the new system. First of all, we noticed that, in the cipher material of a given day, one could find message pairs in which first two letters of the key were identical and the third letters succeeded each other in the alphabet, such as TKP and TKR. If in the same messages there were pairs of identical letters also in the message keys, it was possible to draw conclusions regarding the identity of the right or middle rotor. Let us illustrate the various possibilities with a few examples.

1) Let's assume that we have two messages with the following keys:

Base position	Message key
TKP	AN**V** CK**B**
TKR	**V**TS **J**QM

In this case it is obvious that, between letters P and R, a middle rotor shift has occurred, i.e. that rotor I is in the right-hand position, because it alone causes the middle rotor to move between the marks Q and R. Otherwise, instead of the same letter of key V, we would get equal letters B (or J).

2)

Base position	Message key
TKP	AN**V** CK**B**
TKR	**V**TS **B**QM

In this case there is a lower probability that the middle rotor moved, i.e. that the rotor I is in the right-hand position.

3) Conclusions regarding the rotor order can also be drawn from the base positions where the letters in the middle position are different, as demonstrated by the following example:

Base position	Message key
TKP	AN**V** CK**B**
TLR	**V**TS **J**QM

The middle rotor cannot move between P and R, so in the right-most position there is surely some rotor other than I.

4) In certain cases conclusions regarding the rotor order can be drawn even on the basis of the message keys, in which the first letter is different.

Base position	Message key
TJG	**C**WS **P**KR
UKG	**C**WT **P**LJ

In this case, it is likely that the left-hand rotor is moved between letters J and K, which means that rotor IV is in the middle position. In other cases, similar conclusions may be drawn.

24. Bombs

Within a few days after the introduction of the new procedure, a plan was drawn up to remove the difficulties that have arisen. Our thoughts were running in the following direction: take a number of messages and write down their base positions and message keys.

1.	K T L	W O C	D R B	7.	G R A	F D R	Y W D
2.	S V W	K K M	I Y S	8.	M D O	O T W	Y Z W
3.	J O T	I W A	B W N	9.	K J C	F S W	R S E
4.	E D C	D S P	L J C	10.	S G F	T E Y	A S R
5.	G D K	W A V	W H A	11.	A G H	M D F	R H F
6.	B W K	T C A	T O C	12.	J B R	W L T	S O Q

Let us now take note of message 3. The letter W appears twice in the message key 3 characters apart. This means that in a given position of the machine some unknown letter, let us mark it as X, is enciphered as W, and three positions later the same letter X is again enciphered as W. Let us assume that letter X is not changed by the connections of the switchboard; this assumption, with 5 to 8 pairs connected in the switchboard, is valid in 50% of cases.

In this situation, the starting position of rotors can be found by tapping the letter W continuously on two Enigma machines, in which the rotors are shifted 3 positions apart and move synchronously. Whenever the same letter is lit in both machines, we have a possible solution that should be further verified.

However, because such a case occurs too often, we can analyse not just one, but three message keys, in each of which the letter W appears twice 3 characters apart. Let us take into consideration the messages 3, 5 and 8. In this case we must use not two, but six machines. In reality, it would be impractical to manipulate six separate machines. Therefore, a device consisting of six Enigma machines was designed, which were electrically driven and stopped automatically whenever they reached a potential solution. Six examples of such a bomb were assembled in the Polish Cipher Bureau, one for each possible rotor order (rotors IV and V were only introduced later), with each bomb running for 1½ hours through all 17 576 possible starting positions.

25. Zygalski sheets

Bombs were still under construction when further changes took place. On 15th December 1938, rotors IV and V were introduced, increasing the number of rotor orders tenfold, and two weeks later the number of connection pairs in the switchboard was increased to 7–10. As a result of these changes, bombs have lost their practical meaning, because in the new situation solution would take too much time. Sometimes it was possible to determine the rotor order due to the above mentio-

ned method, but it required a large amount of cipher material, which was relatively rarely available. The effectiveness of the bombs was also limited by the increased number of connections in the switchboard.

A new method was therefore designed quite early, which was independent of the number of pairs of connections in the switchboard. To illustrate this method, we need to introduce a new concept – the female and male positions. Let us return to the messages cited on page 139:

1.	K	T	L	W	O	C	D	R	B
2.	S	V	W	K	K	M	I	Y	S
3.	J	O	T	I	W	A	B	W	N
4.	E	D	C	D	S	P	L	J	C
5.	G	D	K	W	A	V	W	H	A
6.	B	W	K	T	C	A	T	O	C
7.	G	R	A	F	D	R	Y	W	D
8.	M	D	O	O	T	W	Y	Z	W
9.	K	J	C	F	S	W	R	S	E
10.	S	G	F	T	E	Y	A	S	R
11.	A	G	H	M	D	F	R	H	F
12.	J	B	R	W	L	T	S	O	Q

The case illustrated in message 3, where the same letter (in our case W) occurs twice 3 characters apart, cannot occur in all the rotor starting positions. Calculations have shown that such a case will occur in about 40% of the positions (exact value is $1 - (1/\sqrt{e})$, where e is the basis of natural logarithms). Such positions are called female positions, the others, male positions. In our example, items 3, 5, 6, 8, 9 and 11 are female items, while the nature of the other items cannot be determined on the basis of data available. Connections in the switchboard determine which letters appear in the message key, but they do not affect the gender of a given position (whether it will be female or male).

Based on the above observations, a catalogue of all female positions can be developed and then searched for six female positions, which occur in the same distance as e.g. JOU, GKD, BWK, MDR, KJD, AGK base positions (where possible displacements of middle and left rotors should be taken into account).

Since this is practically impossible, we took a different route; we developed the so-called Zygalski sheets: for each rotor order all possible female positions were marked on 26 sheets of paper containing 26×26 fields, repeated in the four quadrants of each sheet. Individual sheets corresponded to the positions of the left rotor, the 26×26 fields on each sheet corresponded to the possible positions of the middle and right rotor. The reason for inserting the four copies in each quadrant of each sheet will be explained below. Holes were cut in the fields corresponding to female cases (hence another name for the sheets – a "net").

Then, returning to our example, six out of the 26 sheets are superimposed in order and with a shift corresponding to the difference between the base positions. If there exists a single position where a hole appears in all the sheets simultaneously, we have probably found the solution which requires further examination. To explore all the possibilities, we need to change all the sheets one by one. Each of them contains a quadruple set of 26×26 fields, because the sheets are superimposed with offset. The final result depends on the care taken in applying the sheets. Therefore at the beginning of the work we prepared a separate worksheet, the so-called menu, defining the order and mutual displacement of particular sheets.

Information concerning which positions are female and which are male has been taken directly from catalogues made with a cyclometer, because female positions usually correspond to cycles consisting of a single letter.

Possible solutions identified using the sheets were also checked using the cyclometer. It was a time-consuming job, but we were considering then cataloguing not only female positions, but all the positions corresponding to one letter cycles. This idea was implemented much later by British cryptologists.

26. Warsaw conference

Two sets of 26 Zygalski sheets for two rotor orders were hand-made by the Polish Cipher Bureau, confirming that the idea was practical. However, the question of its practical application was more complicated.

Whereas the female positions for rotor orders I II III, I III II,..., III II I could be consulted directly in the existing catalogue, for the remaining 54 rotor orders they should have been first determined either using the cyclometer, which would have taken several years, or with a new and expensive machine, which could not even have been thought of. Manual perforation of the first two sets of 26 sheets was very cumbersome; we realised that further work would require a specially designed machine. Finally, even if it had been completed, handling of 60 sets of sheets to solve the next few days would have required a large support staff.

Since the Polish Cipher Bureau was not able to overcome these difficulties on its own, it was decided to entrust the strictly protected secret of Enigma to the French and British codebreaking service.

On 26th July 1939, a three-day conference on the Enigma took place in Warsaw, attended by representatives of the codebreaking services of France and England. It turned out that neither French nor British cryptologists were able to overcome their earliest problems. We presented to them the results of our seven years of work, as well as the difficulties we have encountered more recently. The British offered to help in the manufacturing of Zygalski sheets for 60 different rotor orders.

27. Outbreak of war. Vignolles

A month later, the German-Polish war broke out. The message from 25th August 1939, the day of general mobilisation in Germany, was broken and the evacuation started soon afterwards. Bombs, cyclometer, Enigma, all the documentation and technical drawings we took with us, but we had to gradually destroy them on the road to the Romanian border. Only two Enigma copies were salvaged. In Bucharest, the French embassy received the three Enigma specialists and dispatched them on a further journey to Paris, where they met a friendly reception. A few weeks later, the French staff organised an office in Vignolles, a castle located near Gretz and 30 km away from the capital of the country, where Polish cryptologists, with the participation of auxiliary staff and under the command of Lieutenant Colonel Langer, tried to resume the duties interrupted in Poland. As in Warsaw, the painstaking work on manual manufacture of Zygalski sheets began, a work whose results would not be available for years.

However, the conference in Warsaw started to bear fruit. It turned out that in the meantime the British had constructed a device that allowed them to make a set of Zygalski sheets for all 60 possible rotor orders in just few weeks. However, British attempts to use the sheets did not yield results. As the sheets were made in

two copies, one of them could be placed at our disposal, which they helpfully did. As soon as the sheets arrived at Vignolles, the hard work began and the messages of two days, 28th October 1939 and 6th January 1940, were soon broken.

The British organised their work very well. They had at their disposal numerous staff and extensive cipher materials. Most of the days solved were a result of their work.

Feverish work continued also in Vignolles. Since it was now a matter of reading as many messages as possible and passing the information on to the general staff for evaluation, Polish cryptologists were sitting at the Enigmas constantly, tapping messages and manipulating sheets, so as not to let the British outperform us completely. It was purely mechanical work that auxiliary staff could do. It was thus understandable that Polish cryptologists did not achieve significant cryptological results anymore, and the focus of theoretical work shifted to London.

28. Knox method

The British cryptologist Knox noted that German cipher clerks often chose as the base position those letters which are visible in the machine windows after the encryption of the previous message has been completed. This phenomenon was particularly common in multi-part messages. In such cases, it was sufficient to subtract the length of the previous message from the base position to receive the message key (unencrypted). If any of the common keys, such as ASD, WER, OKL, ... were obtained, one could be sure that the clerk made a mistake. Since, when subtracting the length of the message from the base position, account had to be taken of possible displacements of the middle and left rotor, this presented an opportunity for partial determination of the rotor order, reducing the number of possible rotor sequence variations from 60 to 3. It was also important that, thanks to the Knox method, it was possible to determine the (unencrypted) keys of many messages.

This method provided significant services during the Norwegian campaign, when day after day was solved providing important and interesting information.

29. Catalogues for Zygalski sheets

In the meantime British cryptologists have implemented yet another method developed earlier by the Poles. As already noted, verification of cases identified with Zygalski sheets using a cyclometer was quite a time consuming exercise. Each time after identifying a potential solution, it was necessary to verify the character corresponding to the female position using a cyclometer and comparing it with the characters of the relevant message key. In Poland we had the idea to create catalogues with characters that would correspond to all female cases, but technical difficulties hindered such a solution. Now, the British, using the same device that they used to make sets of Zygalski sheets, delivered another spectacular example of the benefits of Polish-French-British cooperation. Thanks to their financial and organisational capacity they put our plans into practice, which otherwise would not have seen the light of day, without resolving the costs and difficulties.

30. Herivel method

Another British cryptologist discovered that some German cipher clerks, when setting up Enigma machines for the next day in the afternoon or morning, did not change the rotor position after setting the rings on the rotors, but used characters visible in the machine windows as the key of the first message in a given day. As a result, the base position of the first message did not differ significantly from the current ring positions.

By comparing the base positions of messages sent by different cipher clerks at night or in the early morning hours, it was possible to identify ring positions accurately or at least approximately. Thanks to this discovery, the work needed to break the cipher has been significantly reduced, so that the British were often able to break the key in the early morning.

A few more remarks should be added to the method just described. After rotor wiring for rotors IV and V was determined, for a period of time we could not determine their turnover points. We had a choice of 26 variants, out of which we chose the one considered the best. However, there was a consensus that the position thus chosen was only approximate. After significant number of messages were broken (yet before Herivel's discovery), we remembered that the turnover points were different for all rotors. If this feature was also present in the new rotors (which seemed highly probable), adjustments had to be made to the previous findings concerning the turnover points in rotors IV and V. Corrections were found and immediately communicated to the British. Only then could Herivel's method be applied effectively.

31. Third ciphering procedure

On 1st May 1940, before the German offensive in Belgium and the Netherlands began, the encryption procedure was changed again. In the new message key, it was not encrypted twice as before, but only once. The header of the message is now only six letters long, with the first three characters identifying the base position and the second triplet specifying the encrypted message key.

This was all the more clear because some German cipher clerks repeated their mistake applying the new procedure already on the eve of its official introduction in the evening. That day, 30th April 1940, was broken, incidentally by Polish codebreakers, which permitted the analysis of the new procedure.

This was again a serious blow. Zygalski sheets and accompanying catalogues now became completely useless; only the Knox and Herivel methods remained valid. The Polish cryptologists, temporarily transferred from Vignolles to Paris, tried to break at least one day's messages, but in vain.

The British were more successful. They had more extensive cipher material at their disposal, so they were able to solve it after a three-week break on 20th May 1940 and soon afterwards almost all the following days. They shared broken keys with us on a regular basis, so Polish codebreakers were sitting day and night over their Enigmas, brought from Warsaw, reading valuable material from broken messages. After evacuation from Paris, work resumed in La Ferté-Saint-Aubin, where work continued day and night; the decryption process stopped only after signing the truce. The last day for which the English sent the keys was 16th June 1940.

32. Chronology of changes in ciphering procedures of army and air force

<table>
<tr><td>15.07.1928
1929
31.05.1930</td><td colspan="6">Enigma G with plugs</td></tr>
<tr><td>1.06.1930
1931
1932
1933
1934
1935
31.01.1936</td><td rowspan="11">Enigma M with switchboard</td><td>Rotor order changed every three months.</td><td>6 pairs of letters changed in the switchboard.</td><td rowspan="3">Reflector A</td><td rowspan="4">Rotors I–III</td><td>First ciphering procedure. Base position same for every message. Double encipherment of message key.</td></tr>
<tr><td>1.02.1936
30.09.1936</td><td>Rotor order changed every month.</td><td rowspan="5">5–8 pairs of letters changed in the switchboard.</td><td rowspan="8">Second ciphering procedure. Base position variable. Double encipherment of message key.</td></tr>
<tr><td>1.10.1936
1.11.1937</td><td>Rotor order changed daily.</td></tr>
<tr><td>2.11.1937
14.09.1938</td><td rowspan="6">Reflector B</td></tr>
<tr><td>15.09.1938
14.12.1938</td></tr>
<tr><td>15.12.1938
31.12.1938</td><td rowspan="3">Rotors IV–V</td></tr>
<tr><td>1.01.1939
31.12.1939</td><td>7–10 pairs of letters changed in the switchboard.</td></tr>
<tr><td>1.01.1940
30.04.1940</td><td rowspan="2">10 pairs of letters changed in the switchboard.</td></tr>
<tr><td>1.05.1940</td><td>Third ciphering procedure. Base position variable. Single encipherment of message key.</td></tr>
</table>

33. Sicherheitsdienst wireless network

We have already mentioned the Sicherheitsdienst radio network in Section 21. Since this network, abbreviated to S.D., used an encryption procedure which differed in detail from the procedures used in army and air force, it should be described in more detail.

Until 1st August 1939, the main difference between the S.D. procedure and other services was the fact that the clear text was initially masked out with a three-digit code. The code was used clearly to shorten the messages. Breaking it was not particularly difficult, but every few months it was replaced by a more extensive version, so it was necessary to restart all the work from the beginning.

The key of the message was, as in army and air force, doubly enciphered, but it was not prepended at the beginning of the message, but inserted at various points throughout the message. In addition, for a few months, characters of the message key were additionally enciphered with an external substitution; this was valid for one month each time.

Message keys were carefully selected, so the methods of unequal letters and of the cyclometer could not be applied.

There were no messages starting with the AN letter-pair. In order to find the base position and the ring position, one had to use other properties of the message text. It was found that in many of the messages the fourth and fifth or the fifth and sixth letters were QY, so it was possible to use these characters in the same way as AN in army messages.

The content of messages was usually very interesting. Very often messages were about secret agents working in foreign countries, so it was possible to build a picture of the extensive German intelligence organisation.

The ciphering procedure introduced in the army and air force on 15th September 1938 did not apply in the S.D. network. It continued to work using the old system, masking this fact by adding a three-letter prefix in the message header, suggesting thus the use of a new procedure. However, on 1st August 1939, there was a complete change of procedure, which we did not manage to work out. Since then the S.D. messages resisted any attack. The last broken day was 31st July 1939.

Due to the lack of sources, it is currently not possible to give a chronological list of changes to various elements of the code, such as code books, key encryption tables, key positions in the text of messages, etc.

34. Kriegsmarine ciphering procedure before Enigma

The cipher procedures used by the German Kriegsmarine differed significantly from those used by the army and the air force, although from 1934 onwards it used the same Enigma machine as other services. It would be pointless to offer a chronological presentation of our efforts in this area. They have been only briefly recapitulated at the end of this document.

The messages exchanged within the German Kriegsmarine radio network were encrypted in groups of two, three or four letters, with no incomplete groups (e.g., at the ends of messages). Four character groups were the main variant and only this variant was analysed by the Polish Cipher Bureau.

During the period of 1926–1927 four-letter groups usually represented the super-enciphered code. The first and last group of messages were either a blind group or a message indicator. The other groups were encrypted code words. Neither the super-encipherment nor the code itself have been broken.

In the years 1926–1927, two four-character procedures were used. One of them was a simple, unenciphered code. Its codebook was broken in 1933. The code groups consisted of only 18 letters:

A B E F G I K L N O P S T U W X Y Z

The codebook was extensive and included more than 90,000 code words, of which we recovered some 10,000[1].

35. Kriegsmarine ciphering machine with 29 keys

From 1926 until 1934, the Kriegsmarine used a ciphering machine to encrypt their messages. It was an Enigma-type machine, but different in detail from the Enigma used by the army:

1) the machine had 29 keys and as many bulbs for the 29 characters of the German alphabet including umlauts;
2) when pressing the X key, the bulb marked X was always lit;
3) the machine had neither plug connectors nor switchboard;
4) the entry drum had the following wiring:

A	Ä	B	C	D	E	F	G	H	I	J	K	L	M	N	O	Ö	P	Q	R	S	T	U	Ü	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

The machine had five rotors, three of which were used at one time;

5) the rotors' turnover notches were not associated with the rings, but with the rotors themselves;
6) the reflector was movable; it could be set in four different orientations;
7) the rings showed the numbers 1 to 28.

Although machine has been in use since 1926, it was reconstructed only on the basis of messages from 1931–1934. During that period messages were encrypted in the same way as in the army, i.e. there was a common base position on each day, from which the double encryption of message key was started. The two three-character letter groups thus obtained were converted into four-character groups by the addition of a blind letter, the first of which was inserted at the beginning and the second at the end of the message. For both groups the theory of cycles developed during the attack on the army machine could be applied.

However, the recovery of products A_1A_4, A_2A_5 and A_3A_6 was hampered by insufficient cipher material. It was even more difficult to recover the message key. This changed only in 1933, when we discovered that the message keys, selected from the list, do not use the umlauts. From then on it was possible to reorder the cycles so that the characters of the first group of encrypted messages would be assigned to the umlauts.

Unknown connections of the entry drum connections represented another difficulty. Luckily, we were able to guess them in the same way as we did with an army machine. We assumed there was no switchboard in the machine, which turned out to be true. Otherwise our attempts to reconstruct the machine would probably have failed. Then, as in the case of army machines, the rotor wiring was recovered.

At that point we could return to the messages from the past years. In 1936, in periods spanning several days, all messages were encrypted starting from one and the same rotor position (but different from that of the army Enigma). In order to read message texts during these periods, the following steps were taken. Two messages were

[1] The second procedure was later identified as the machine cipher which is presented in detail in Section 35.

sought, which most probably contained the same clear text, but in one of them the cipher clerk omitted one letter. Pressing the keys of the corresponding characters of both messages immediately after each other should give the same clear text. The grill was used to determine the right rotor and then, without significant difficulties, to identify positions of the remaining rotors. It was also found that the clear text was coded using the same code, which was also used without a machine and which we partially managed to break, prior to encryption. As we mentioned earlier, it was a four-character group code containing characters from the 18-character alphabet including ABEFGIKLNOPSTUWXYZ. Outside that period we were unable to break the cipher. It was only established that the rotor order, positions of the reflector and the rings together with the message key (there was no base position in that procedure) changed at irregular intervals, from 3 to 15 days.

On 1st January, 1927, the codebook was replaced by a new one. The keys could henceforth be recovered in the following way: from among the messages we selected those ones, which we suspected to end with a code group corresponding to the phrase "Fortsetzung folgt"[2]. Since the machine has the property that the clear text and corresponding cipher letter are always different (except for the X character, which is always encrypted as X), it has always been possible to find these (unencrypted) groups and, to determine the rotor positions using the grill. It turned out that the new codebook uses all 29 characters, including the umlauts, but due to lack of time we were unable to solve it. On 1st January 1929 another change took place, this time concerning the ciphering procedure itself. Now each message had its own message key, transmitted at the beginning and the end of the message, the function of which we did not manage to determine.

On 1st May 1931, another change in the ciphering procedure took place, which resulted in encryption of the message key in a manner identical to that used in the army. Thus, the rotor wiring was recovered. We could proceed to reading clear texts; we tried to guess some code groups, but after a few months of hard and ineffective work it was accidentally discovered that the open text is not coded (as in the army). The encryption procedure has proved, as already mentioned, to be basically identical to that used in the army and the Luftwaffe. However, the so-called internal settings, i.e. rotor order, reflector position and ring positions, changed at irregular intervals as before, while the base position was changed daily.

Message keys were selected from the list. Either because the list was not long enough, or because the cipher clerks kept on choosing the same positions over and over again, the message keys were repeated so often that it was possible to compile statistics permitting to reconstruct substitutions A_1A_4, A_2A_5, A_3A_6, whereas the lack of umlauts was helpful. The cyclometer was useless, because the catalogues would have to include

$$60 \times 28^4 = 36\,879\,360$$

positions, which was not manageable. Thus, the position of the right rotor was determined using the grill, which was easy due to the lack of a switchboard. Positions of the other rotors were determined using a catalogue similar to the F catalogue in the army and the Luftwaffe; the only difference being its larger volume, as it included

$$28^3 = 21\,952$$

positions.

[2] Continuation follows.

It was attempted to ensure a minimum length of the clear text, using, among other things, any abbreviations possible. The second and subsequent parts of the multi-part messages always began with the letters FORT (abbreviation from Fortzsetzung - continuation). Recovery of the base position and ring positions started assuming the FORT clear text, just as was the case with AN in the army and air force and letters QY in S.D. network.

36. Kriegsmarine use of ciphering machine with 26 keys

Starting from 1st October 1934, the German Kriegsmarine used the same Enigma as the army. The encryption procedure remained unchanged, except that during this time there were connections in the switchboard (always 6 pairs) which were changed daily, as well as the base position. In the period until 15th November 1936, two additional rotors were used by the Kriegsmarine, but only three rotors were installed in the machine at the same time.

Until 16th November 1936, it was now possible to break the keys of a modest part (approximately one tenth) of the messages using the cyclometer and catalogues developed for army Enigma. However, this was not enough to reconstruct the list of the message keys. Only when on 16th November 1936 both additional rotors were retired, leaving only rotors I, II and III in use, did it become possible to recover the list of keys, and then the keys of messages sent in the period starting on 16th November. Further, the wiring of the two additional rotors, called IVM and VM as opposed to the rotor IV and V used by the army and air force, was determined using the grill.

In addition to the general key for particularly important messages, officer and staff keys were also used. The officer key was used as follows: selected message key was first encrypted twice from the base position of the general key, after which two groups of three characters were extended to four letters and attached as usual at the beginning and end of the message. Then the key received was encrypted again starting from the officer key base position and the result was used to encrypt the clear text of the message.

It is not known how the staff key functioned. On 1st May 1937, the encryption procedure was changed again, with the message key no longer encrypted using the machine, but in a different and somewhat complicated way. The details of the new encryption system were only learned when, in 1940, the British were able to recover instructions from a sunken U-Boot. We cannot describe the procedure here in detail, and refer the reader to photographic reproductions of the acquired documents.

The ignorance of the new procedure did not prevent us from obtaining a number of results in 1937, which we report below.

The message key was given in the first two groups of messages, which were repeated at the end to avoid errors. The ciphertext proper started therefore with the third group. Using the following method, it was possible to read many messages from the period between 1st and 8th May 1937, and consequently to reconstruct the rotor order, switchboard connections and partially ring position for these days. Comparison of these with the internal settings from April 1937 showed that the internal settings did not change on 1st May 1937, remaining constant between 27th April and 8th May. Comparison of the broken messages' keys with the first and last groups gave the following results.

If in the keys broken on a given day the first two groups are divided into pairs of neighbouring characters and if two messages have the same first, second and third pair of characters, they have the same first, second and third letters of the message key. However, there is no inverse relationship; identical letters may correspond to different pairs. Moreover, equal pairs of characters in different locations generally correspond to the different letters of the message key.

In addition to preserving the earlier internal settings, Kriegsmarine cipher clerks committed another serious mistake when the ciphering procedure was changed on 1st May 1937. As a certain ship was not provided with the new procedure in time, during the first three days of May 1937 she worked using the old procedure. Thanks to this we were able to recover the basic settings for general and officer keys on 2nd and 3rd May 1937.

Later the British managed to establish the following:

If the message keys encrypted using the new procedure are decrypted using the reconstructed base positions of 2nd and 3rd May, the same pairs of characters correspond to the same decrypted key characters, even if they appear in different locations.

The content of the messages for the period 1st May 1 to 8th May 1937 was found in the following way: suppose that we have a message which, after the first two groups are deleted, begins as follows

VLPP WGKS WKUL QBOR

Let us assume further that this message represents a continuation of another message, sent at 16:23. Experience has shown that its clear text must begin with letters

F O R T Y Q Z W E Y Y Q Z W E Y

(QZWE stands for 1623). We know, therefore, a 16 characters long fragment of this message, both in the clear and encrypted version. Since only 6 pairs of connections in the switchboard were used in the Kriegsmarine, some of the characters must appear in the same form. It is therefore possible to make assumptions regarding letters unchanged and verify these assumptions either directly on the machine, using a grill or using Jeffreys sheets, a British invention corresponding to our catalogue F. In any case, it requires a long effort that only pays off when it comes to analysing the new encryption procedure.

The British managed to break a few messages from 1938. At that time the reflector B was already in use. It was apparently introduced in Kriegsmarine at the same time as in the army. Also the number of 6 connection pairs in the switchboard remained unchanged.

In 1940 the British found two rotors marked VI and VII in a sunken U-Boot. It is not currently known whether only rotors I, II, III, VI and VII are used in the Kriegsmarine or the complete set I to VII.

37. Chronology of changes in ciphering procedures of the German navy

| 1926 | Navy Cipher machine „Enigma" (29 keys) | | |

38. The Contributions of three countries to Enigma breaking

I. Poland

Cycle theory

Substitution theory

Wiring of rotors I–III and reflector A

Method of entry drum reconstruction

Method of switchboard reconstruction

Method of non-random message keys

Statistical method

Method of non-equal letters

Determination of right rotor grill and catalogue F

Cyclometer (device and catalogue)

Cleartext recovery

Reflector B wiring

Rotors IV and V wiring

Analysis of second ciphering procedure

Bombs

Zygalski sheets (design).

Catalogue for Zygalski sheets (design).

Analysis of third ciphering procedure

S.D. wireless network

Kriegsmarine Enigma with 29 keys

Wiring of rotors IVM and VM

Analysis of ciphering procedure used by Kriegsmarine starting from 1st May 1937.

II. England

Zygalski sheets (manufacturing)

Catalogue for sheets (manufacturing)

Jeffrey's method

Knox method

Herivel method

Rotors VI and VII (found in U-Boot).

III. France

Delivery of two important documents

Transkrypt wersji francuskojęzycznej

urgent[1]

TRADUCTION

(„ENIGMA“ – Kurzgefasste Darstellung der Auflösunsmethoden)

3. Zykelntheorie 247

5. Substitutionentheorie 247

6. Substitution E 249

7. Die Substitution S 250

8. Einige Ziffern 251

9. Auffindung der Spruchschlüssel 252

11. Die statistische Methode 252

12. Methode ungleicher Buchstaben 253

13. Bestimmung der rechten Walze 254

14. Der Rost 255

15. Der Katalog F 256

16. Der Zyklometer 256

17. Grundstellung und Ringstellung 257

18. Einige Bemerkungen 257

23. Auffindung der Walzenlage 257

24. Bomben 258

25. Die Netze 259

28. Methode KNOX 261

[1] nota odręczna, handwritten note

29. Kataloge zu den Netzen 261

30. Methode HERIVEL 261

31. Drittes Schlüsselverfahren 262

32. (simplement, traduction du verbe „tauschen“ au sens technique qui lui est donné) 262

(Au point de vue linguistique, toutes questions pourront être posées à M. BARSAC)

3. Théorie des cycles

Une analyse détaillée des six premières lettres de chaque message conduisit au résultat que ces lettres constituent la clef chiffrée du message. Plus précisément, il fut constaté ce qu'il suit : on impose d'avance une certaine position des roues, la même à tous les chiffreurs pour une journée donnée. Ensuite chaque chiffreur choisit arbitrairement une clef de trois lettres qu'il chiffre deux fois consécutivement sortant de la position imposée des roues. De cette façon il obtient six lettres qu'il place à l'entrée avant le texte propre.

Or, comme la première et la quatrième, resp. la deuxième et la quatrième, resp. la troisième et la sixième lettres sont le résultat de chiffrement d'une même lettre, il est clair qu'il existe des rapports entre ces lettres. Il était possible de former certaines expressions avec les six premières lettres des divers messages d'une même journée quel l'on appelle cycles, et qui permettent à énoncer ces rapports sous forme de théorèmes suivants :

1) Le nombre des cycles d'une même longueur est toujours pair.
2) Les lettres qui se trouvent dans un certain cycle sont provoquées par des lettres qui se trouvent dans un autre cycle de la même longueur.
3) Si une lettre X fut provoquée par une lettre Y, alors la lettre qui se trouve du côté droit de X fut provoquée par la lettre qui se trouve du côté gauche de Y.

L'ensemble de ces trois théorèmes avec ces conséquences forme ce que l'on appelle la théorie des cycles. Par cette théorie on s'est approché du problème de la reconstruction des clefs individuelles des messages, c'est-à-dire des clefs choisies arbitrairement par les chiffreurs. La résolution complète de ce problème était déjà possible, mais les travaux cryptologiques furent dans ce temps-là dirigés dans une autre direction.

5. Théorie des substitutions

On aborda maintenant le problème le plus important, c'est-à-dire la recherche de connexions des roues. A cette effet on se servait d'une méthode mathématique, mais le chemin à parcourir était long et il fallait surmonter une série de difficultés sérieuses. Une exposition de la méthode mathématique appliquée dépasserait considérablement les cadres de cette esquisse. Pour son étude nous renvoyons le lecteur à un des œuvres suivants :

1) J.A. Serret : Cours d'Algèbre supérieure, tome II.
2) E. Netto, Substitutionentheorie.
3) Burnside : Theorie of groups of finite order.
4) Bianchi : Lezioni sulla teoria dei gruppi di sostituzioni.

Ici nous devons nous borner à donner une idée du chemin parcouru :

Le chiffre Enigma est une substitution, cela veut dire que la machine change les lettres de l'alphabet dans des autres lettres par chaque position des roues.

Désignons par A_1 la substitution effectuée sur les lettres de l'alphabet quand les roues se trouvent dans la position initiale (Grundstellung) fixée pour la journée donnée, par A_2 la position suivante, et ainsi de suite jusqu'à A_6.

Si nous disposons d'un nombre suffisant de messages (en moyen il en faut environ 80) ce que nous voulons admettre, nous pouvons former les produits A_1A_4, A_2A_5, A_3A_6. On peut donc regarder ces produits comme connus. Désignons ensuite par:

S la substitution effectuée par les Steckerverbindung
C_γ „ „ „ la roue de droit
C_β „ „ „ „ milieu
C_α „ „ „ „ gauche
U „ „ „ miroir
E „ „ „ d'entrée, c'est à dire par la succession dans laquelle le courant électrique coule des touches à la roue $C\gamma$.
Q la substitution (1,2,3,4,5,6, ..., 24,25,26)

Si pendant le chiffrement de la clef du message la roue de milieu ne tourne pas ce qui est assez probable et que nous voulons admettre dans la suite, alors on peut exprimer les substitutions A_1, A_2, A_3, ... A_6 de la façon suivante:

$A_1 = S\,E\,C\gamma\,C_\beta\,C_\alpha\,U\,C_\alpha^{-1}\,C_\beta^{-1}\,C\gamma^{-1}\,E^{-1}\,S^{-1}$
$A_2 = S\,E\,Q\,C\gamma\,Q^{-1}\,C_\beta\,C_\alpha\,U\,C_\alpha^{-1}\,C_\beta^{-1}\,Q\,C\gamma^{-1}\,Q^{-1}\,E^{-1}\,S^{-1}$
$A_3 = S\,E\,Q^2\,C\gamma\,Q^{-2}\,C_\beta\,C_\alpha\,U\,C_\alpha^{-1}\,C_\beta^{-1}\,Q^2\,C\gamma^{-1}\,Q^{-2}\,E^{-1}\,S^{-1}$
. . . . . .
$A_6 = S\,E\,Q^5\,C\gamma\,Q^{-5}\,C_\beta\,C_\alpha\,U\,C_\alpha^{-1}\,C_\beta^{-1}\,Q^5\,C\gamma^{-1}\,Q^{-5}\,E^{-1}\,S^{-1}$

Il faudrait donc, pour trouver les connexions des roues, résoudre ce système d'équations qui, bien entendu, ne sont pas des équations ordinaires mais des équations du substitution.

La première difficulté que nous rencontrons ici en ce que non seulement les membres droits, mais aussi les membres gauches des équations sont inconnus. Ce qui est connu, ce sont seulement les produits A_1A_4, A_2A_5, A_3A_6. Mais la théorie des cycles nous apprend qu'il n'existe, en général, plus que quelques dizaines des désignations pour la substitution A_1, et que chaque désignation de A_1 détermine en même temps une seule désignation pour la substitution A_4. La même observation s'applique aussi aux substitutions A_2 et A_5, et A_3 et A_6. On peut donc s'imaginer que l'on a écrit toutes les désignations possibles pour les substitutions A_1, A_2, A_3, ... A_6. De telle façon on peut surmonter cette première difficulté en augmentant en même temps, il est vrai, le travail à exécuter bien de fois, car dans les opérations à suivre il faut mettre successivement toutes désignations possibles pour A_1, A_2, ... A_6.

La deuxième difficulté était encore beaucoup plus grave. Elle consistait dans la substitution S qui était inconnu. On a encore étudié ce problème profondément quand les connexions des roues étaient déjà trouvés par d'autres voies, et on est venu à la conviction que pratiquement, sans connaissance de la substitution S, notre système d'équations était irrésoluble. Théoriquement on a élaboré une méthode, mais elle exigeait beaucoup de temps, beaucoup de matériel, la connaissance de la substitution E, et la connaissance des A_1, A_2, A_3, ... A_6 séparément.

La troisième obstacle était la manque de connaissance de la substitution E, et

il semble que c'est à cause de cet obstacle les recherches des cryptologues anglais sont échouées. Dans la bureau polonais des chiffres on supposait d'abord que la substitution E avait la même forme comme dans la machine à chiffrer commerciale, c'est à dire:

Q	W	E	R	T	Z	U	I	O	A	S	D	F	G	H	J	K	P	Y	X	C	V	B	N	M	L
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Les recherches postérieures conduisaient au résultat qu'il était possible de trouver la substitution E par un chemin déductif mais seulement avec la connaissance antérieure de la substitution S.

En résumé on peut donc dire qu'il était possible, au moins théoriquement, de trouver les connexions des roues sans aucun autre aide, seul à l'aide des matériaux d'écoute, mais à condition que l'on devine la substitution E. Mais si l'on veut éliminer tout moment de devination, il faut supposer qu'on bien la substitution E ou la substitution S soient connues. Et nous répétons: si l'inconnu est S, il faut un matériel qui s'étend sur un intervalle de temps bien long.

En réalité notre système d'équations fut résolu grâce au document français qui donnait la substitution S pour une période de deux mois, et grâce à la heureuse devination de la substitution E.

Pour orienter le lecteur nous communiquons qu'il faut pour trouver les connexions des roues, amener nos équations à la forme suivante:

$$E^{-1}S^{-1}A_1SEQ^{-3}E^{-1}S^{-1}A_4SEQ^{3}=C_\gamma[C_\beta C_\alpha UC_\alpha{}^{-1}C_\beta{}^{-1}Q^{-3}C_\beta C_\alpha UC_\alpha{}^{-1}C_\beta{}^{-}Q^{3}]C_\gamma{}^{-1}$$
$$Q^{-1}E^{-1}S^{-1}A_2SEQ^{-3}E^{-1}S^{-1}A_5SEQ^{4}=C_\gamma Q^{-1}[C_\beta C_\alpha UC_\alpha{}^{-1}C_\beta{}^{-1}Q^{-3}C_\beta C_\alpha UC_\alpha{}^{-1}C_\beta{}^{-1}Q^{3}]QC_\gamma{}^{-1}$$
$$Q^{-2}E^{-1}S^{-1}A_3SEQ^{-3}E^{-1}S^{-1}A_6SEQ^{5}=C_\gamma Q^{-2}[C_\beta C_\alpha UC_\alpha{}^{-1}C_\beta{}^{-1}Q^{-3}C_\beta C_\alpha UC_\alpha{}^{-1}C_\beta{}^{-1}Q^{3}]Q^{2}C_\gamma{}^{-1}$$

Ces équations malgré leur longueur ne sont pas très compliquées. Les membres gauches sont connus, et les membres droits ont la patrie du milieu commune. Par élimination de cette partie on reçoit $C_\gamma QC_\gamma{}^{-1}$, ce qui donne immédiatement C_γ, c'est à dire les connexions de la roue droit.

Il fallait encore trouver les connexions de la rue du milieu, du gauche, de la rue miroir, et déterminer les positions pour lesquelles les rues tournent, mais nous n'insisterons pas sur ces questions, parce que méthodiquement elles n'apportaient rien de nouveau.

Il vaut uniquement mentionner que les Allemandes en plaçant dans leur „Gebrauchsanweisung" un exemple authentique de chiffrement, ont allégé le travail considérablement.

6. La substitution E

Nous voulons esquisser en quelques mots, comment on pourrait trouver la substitution E aussi par une voie déductive.

Comme nous sommes en possession des clefs journalières pour deux mois, il est aisé à trouver deux journées pour lesquelles non seulement l'ordre des roues, mais aussi la position (c'est à dire la différence entre Grundstellung et Ringstellung) des roues du droit sont les mêmes. Pour une paire de telles journées nous formons nos deux systèmes d'équations A_1 jusqu'à A_6 et obtiendrons:

$A_1 = SEC_\gamma FC_\gamma^{-1}E^{-1}S^{-1}$ $\quad$ $\underline{A_1} = \underline{S}EC_\gamma\underline{F}C_\gamma^{-1}E^{-1}\underline{S}^{-1}$

$A_2 = SEQC_\gamma Q^{-1}FQC_\gamma^{-1}Q^{-1}E^{-1}S^{-1}$ $\quad$ $\underline{A_2} = \underline{S}EQC_\gamma Q^{-1}\underline{F}QC_\gamma^{-1Q-1}E^{-1}\underline{S}^{-1}$

$A_3 = SEQ^2C_\gamma Q^{-2}FQ^2C_\gamma^{-1}Q^{-2}E^{-1}S^{-1}$ $\quad$ $\underline{A_3} = \underline{S}EQ^2C_\gamma Q^{-2}\underline{F}Q^2C_\gamma^{-1}Q^{-2}E^{-1}\underline{S}^{-1}$

: : : : : : : : : : : : : $\quad$: : : : : : : : : : : : :

$A_6 = SEQ^5C_\gamma Q^{-5}FQ^5C_\gamma^{-1}Q^{-5}E^{-1}S^{-1}$ $\quad$ $\underline{A_6} = \underline{S}EQ^5C_\gamma Q^{-5}\underline{F}Q^5C_\gamma^{-1}Q^{-5}E^{-1}\underline{S}^{-1}$

Dans ces équation nous avons posé pour abréviation $F = C_\beta C_\alpha UC_\alpha^{-1}C_\beta^{-1}$, $\underline{F} = \underline{C_\beta}\underline{C_\alpha}U\underline{C_\alpha}^{-1}\underline{C_\beta}^{-1}$. Les lettres soulignées signifient les grandeurs qui se rapportent à la deuxième journée.

Nous transformons nos équations de façon à obtenir six nouvelles équations dans lesquelles les membres du côté gauche sont connus:

$S^{-1}A_1S\underline{S}^{-1}\underline{A_1}\underline{S} = EC_\gamma F\underline{F}C_\gamma^{-1}E^{-1}$

$S^{-1}A_2S\underline{S}^{-1}\underline{A_2}\underline{S} = EQC_\Gamma Q^{-1}F\underline{F}\underline{Q}C_\gamma^{-1}Q^{-1}E^{-1}$

: : : : : : : : : : : : :

facile à démontrer que les produits A1A2 et A4A5 sont semblable, et aussi les produits A2A3 et A5A6. Il suffit pour cela écrire les quatre équations correspondantes:

$$A_1A_2=S(EGQGQ^{-1}E^{-1})S^{-1} \qquad \underline{A_4}\underline{A_5}=\underline{S}(EGQGQ^{-1}E^{-1})\underline{S}^{-1}$$
$$A_2A_3=S(EGQGQ^{-2}E^{-1})S^{-1} \qquad \underline{A_5}\underline{A_6}=\underline{S}(EGQGQ^{-2}E^{-1})\underline{S}^{-1}$$

dans lesquelles, pour abréviation, on a posé $G = C_\alpha C_\beta C_\gamma U C_\gamma^{-1} C_\beta^{-1} C_\alpha^{-1}$.

Ensuite, on peut calculer le produit SS une fois à l'aide des équations A_1 A_2 et A_4 A_5, et une autre fois à l'aide des équations A_2A_3 et A_5A_6.

Les résultats doivent être naturellement dans les deux cas les mêmes. Et enfin le produit SS doit se composer d'au moins 14 cycles.

La difficulté essentielle consiste en ce que l'on obtient de telle façon seulement le produit SS et non les substitutions S et S séparément. Mais on peut montrer qu'en général les substitutions S et S n'admettent plus que quelques centaires de valeurs. Il faut donc poser toutes ces valeurs successivement dans nos équations et chercher à parvenir à un résultat.

C'est un très grand travail qui serait surement inexécutable si encore les substitutions A_1, A_2, … A_6 n'étaient pas connues séparement, mais seulement les produits A_AA_4, A_2A_5, A_3A_6.

8. Quelques chiffres

Une description détaillée de la machine Enigma dépasserait les cadres de cette esquisse. Aussi nous voulons nous contenter de donner quelques chiffres pour montrer la puissance du point de vue cryptologique de la machine Enigma pourvu que l'on s'en sert avec prudence.

Le nombre de différentes ordres de roues est

$$3.2.1 = 6$$

quand on utilise 3 roues, et

$$5.4.3 = 60$$

Quand on utilise 5 roues.
Il y a

$$26^3 = 17576$$

différentes positions fondamentales (Grundstellung) et autant différentes positions des anneaux (Ringstellung).

Il existe donc (avec les différentes ordres des roues) pour trois rues

105 456

différents position et pour cinq rues

1054560

différents positions.
Le nombre des différents Steckerverbindung est pour 6 paires

$$(26!)/(2^6.6!.14!) = 100\ 391\ 791\ 500$$

et pour 10 paires

$$(26!)/(2^{10}\cdot 10!\cdot 6!) = 150\ 738\ 274\ 937\ 250$$

Le nombre de différents connexions possibles est pour la rue miroir

$$(26!)/(13!\cdot 2^{13}) = 7\ 905\ 853\ 580\ 625$$

Et pour les autres roues

$$26! = 403\ 291\ 587\ 620\ 262\ 925\ 584\ 000\ 000$$

9. La reconstruction des clefs individuels

Jusqu'ici on a résolu le problème suivant : Connaissant les clefs pour deux mois trouver les connexions des roues. Maintenant il s'agit du problème inverse. Connaissant les connexions des roues trouver les clefs.

Avant tout la machine Enigma du type commerciale fut modifiée dans la bureau technique de bureau polonais des chiffres tellement qu'elle pouvait servir pour la lecture des télégrammes militaires. Ensuite on lisait tout le matériel de deux mois pour lesquels on possédait les clefs. A cette occasion on découvrit une série des fautes commises par les chiffreurs et on tira naturellement tout le profit possible. Ces fautes servaient surtout à la reconstruction des clefs individuelles, c'est à dire des clefs que les chiffreurs choisissaient arbitrairement, chiffraient deux fois et ensuite mettaient au commencement du message. Dans le courant de temps les Allemands réussirrent, il est vrai, à dresser leur personnel de telle façon qu'il commirent des fautes de moins en moins. Mais le développement dans cette direction avançait assez lentement pour que l'on put toujours dans l'entretemps réussir à inventer des méthodes de plus en plus raffinées, qui quand même permettaient à trouver les clefs individuelles.

11. Méthode statistique

Nous aperçûmes, que les lettres d'alphabet n'entraient pas dans les clefs avec la même fréquence. Par exemple comme première lettres paraissaient dans les clefs surtout les lettres A et Q, comme deuxième lettres toutes les voyelles, comme troisième lettres les lettres L et O. Il y avait aussi des lettres comme J et Y, qui se présentaient très rarement. On fabriquaient donc une statistique des lettres pour les trois places et puis on s'efforça à subordonner les cycles l'un à l'autre de façon à obtenir une concordance la meilleur possible avec la statistique. La fréquence des lettres changeait du reste un peu avec le temps, et il fallait la changer à plusieurs reprises.

En outre la fréquence des lettres dans l'armée différait considérablement de celle dans l'aviation. Et dans le « Sicherheitsdienst" on choisissait les lettres avec tant d'attention que toutes les lettres paraissaient avec la même fréquence et l'application de la méthode statistique était dans ce cas impossible.

12. Méthode des lettres différentes

Les chiffreurs après l'interdiction de choisir trois lettres égales comme clef évitaient mêmes telles clefs dans lesquelles entraient deux lettres égales comme AAB et FVF. Cette marque était la plus constante et s'est conservée jusqu'aujourd'hui. La méthode basée sur cette marque à cet avantage qu'on peut parfois agir tout à fait mécaniquement.

Supposons par exemple que, pour la journée donnée, on a obtenu des cycles de la forme suivante:

(SAIZELWDPBOHU)(YCRKXFJQNGVMT)
(AZHNUGWMSFLR)(QBYKPDEVJIOT)(C)(X)
(AZCSYBVMFJPDO)(NUGTIRHQKXEWL)

Il faut alors dessiner la figure ci-dessous et deux figures analogues et puis biffer dans les rectangles vides les carreaux qui entraineraient l'identité de deux lettres. Quand on dispose d'un matériel assez nombreux, il ne restera à la fin qu'un seul cas.

S	TYCRKXFJQNGVM
A	MTYCRKXFJQNGV
I	VMTYCRKXFJQNG
Z	GVMTYCRKXFJQN
E	NGVMTYCRKXFJQ
L	QNGVMTYCRKXFJ
W	JQNGVMTYCRKXF
D	FJQNGVMTYCRKX
P	XFJQNGVMTYCRK
B	KXFJQNGVMTYCR
O	RKXFJQNGVMTYC
H	CRKXFJQNGVMTY
U	YCRKXFJQNGVMT
AZHNUGWMSFLR	

TOIJVEDPKYBQ
QTOIJVEDPKYB
BQTOIJVEDPKY
YBQTOIJVEDPK
KYBQTOIJVEDP
PKYBQTOIJVED
DPKYBQTOIJVE
EDPKYBQTOIJV
VEDPKYBQTOIJ
JVEDPKYBQTOI
IJVEDPKYBQTO
OIJVEDPKYBQT

C	
X	

13. La détermination de la roue droite

On avait donc dans la plupart de cas la possibilité de reconstruire les clefs individuelles. Maintenant on passa à la découverte des clefs du jour, c'est à dire ordre des roues, « Steckerverbindung », position des anneaux, position fondamentale. On commença par la détermination de l'ordre des roues.

Quand on écrit l'un sous l'autre deux phrases allemandes quelconques chacune composée de 100 lettres, alors on obtient en moyenne 8 colonnes qui contiennent chacune deux lettres égales. Cette marque subsistera même quand on chiffrera les deux phrases d'après le même procédé.

Si par contre on prend deux textes dépourvus de sens dans lesquels les lettres paraissent avec la même fréquence (à peu près), alors en moyenne sur 100 lettres seulement 4 colonnes composées de deux lettres égales.

On se sert de cette marque pour déterminer la roue droite. Car si l'on dispose d'un matériel assez nombreux, on trouvera un nombre de paire de télégrammes telles que dans chaque paire les premières lettres et aussi les deuxième lettres sont identiques pendant que les troisièmes lettres sont différentes. On écrit alors les deux

télégrammes d'une paire l'un sous l'autre de telle façon que les lettres qui furent chiffrées dans la même position se trouvent verticalement l'une sous l'autre. Mais a priori il y a deux positions possibles, cela dépend du moment dans lequel la rue du milieu tourne. Il faut dons compter dans les deux positions le nombre de colonnes avec les lettres égales et on obtiendra dans la vraie position, en général, à peu près deux fois plus de colonnes que dans l'autre position. On apprend donc, dans quel intervalle la rue de milieu tourne, et si nous procéderons de la même façon avec toutes les paires, il sera possible de resserrer l'intervalle pour qu'on puisse déterminer la rue droite qui, comme on sait, produit la tourmentent de la roue de milieu. Les autres roues seront déterminées plus tard par une autre voie.

14. Le gril

La phase prochaine du travail consistait dans la découverte des „Steckerverbindung". C'était un problème assez difficile, mais on trouva enfin une méthode qui était basée sur le fait que la roue du milieu tourne en moyen une fois pour cinq et que les « Steckerverbindung » ne changent pas toutes les lettres.

Imaginons, pour rendre notre méthode clair, que les „Steckerverbindung" n'existent pas. On peut alors amener les six équations par les substitutions A_1, A_2 , ... A_6 à la forme suivante:

$$Q^X C_\gamma^{-1} Q^{-X} E^{-1} A_1 E Q^X C_\gamma Q^{-X} = F$$
$$Q^{X+1} C_\gamma^{-1} Q^{-X-1} E^{-1} A_2 E Q^{X+1} C_\gamma Q^{-X-1} = F$$
$$\vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots$$
$$Q^{X+5} C_\gamma^{-1} Q^{-X-5} E^{-1} A_6 E Q^{X+5} C_\gamma Q^{-X-5} = F$$

Tout est connu dans ces équations à l'exception de $F = C_\beta C_\alpha U C_\alpha^{-1} C_\beta^{-1}$ et de l'exposant X. Car quoiqu'on connait, grâce à la méthode précédente, quelle est la roue du côté droit, on ne sait pas, quelle est la position de cette roue.

Nous procédons donc de la manière suivante. On posse pour x successivement les valeurs 0, 1, 2, … 25, et on calcule chaque fois les valeurs correspondantes de F dans les six équations. En général ces six valeurs seront différentes entre eux. Mais pour un certain X tous les F deviendront égaux. De cette façon on obtient X, c'est à dire la position de la roue droite, et en même temps aussi la substitution F, dont nous servirons encore plus tard.

Dans la pratique on procède de telle façon, qu'on écrit sur une feuille de papier successivement les deuxièmes lignes des substitutions C_γ, $QC_\gamma Q^{-1}$,. . ., $Q^{25} C_\gamma Q^{-25}$ (les premières lignes seraient toujours 1, 2, 3, … 25, 26).

19 3 15 23 11 20 4 16 26 10 14 22 2 17 6 25 9 1 21 12 18 5 24 13 8
2 14 22 10 19 3 15 25 9 13 21 1 16 5 24 8 26 20 11 17 4 23 12 7 6
13 21 9 18 2 14 24 8 12 20 26 15 4 23 7 25 19 10 16 3 22 11 6 5 17

(l'exemple est arbitraire)

Ensuite on écrit sur un deuxième feuille avec ouvertures (d'où le nom gril) les six substitutions A_1 , A_2, ... A_6 de la manière suivante:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

V T Z F K D R N O U E W Y H I S X G P B J A L Q M C

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

K Q H U V S Z C O N A T W J I Y B X F L D E M R P G

Après ces préparations on pose le gril sur la première feuille et on le déplace du haut en bas jusqu'à ce que dans une position toutes les substitutions F qui apparaissent dans les ouvertures deviendront identiques. Mais cela se présent seulement dans le cas où les „Steckerverbindung" manquent. Dans le cas contraire l'image se change, mais comme les « Steckerverbindung » n'intervertissent toutes les lettres, on remarquera dans une certaine position des analogies parmi les 6 différentes substitutions F. Il faut alors tâcher à placer autrement les lettres dans le substitutions A_1 , A_2, ... A_6 (simultanément) pour que toutes les substitutions F deviendront identiques. Si l'on y réussit, les déplacement des lettres donnent les „Steckerverbindung" cherchés, et en même temps on obtient la position de la roue droite et la substitution F.

15. Le catalogue F

Connaissant déjà la rue droite et leur position on pourrait déterminer les roues du milieu et gauche et leur positions par un simple tâtonnement de tous les cas possibles sur la machine. Mais pour éviter ce travail inutile, le même pour chaque jour, on a confectionné une fois pour toutes un catalogue contenait toutes les substitutions possibles F dont il existe

$$6 \cdot 26 \cdot 26 = 4056$$

Maintenant il suffisait chercher la substitution F quel on a trouvé en même temps que les „Steckerverbindung" dans le catalogue pour apprendre tout de suite ordre et position des roue milieu et du gauche.

16. Le cyclomètre

La méthode longue et incommode qu'on employait pour trouver les „Steckerverbindungen" n'amena pas toujours à la solution. Au surplus elle exigea la connaissance d'avance des clefs individuelles et les méthodes pour les trouver étaient souvent onéreuses et ne conduisaient pas toujours au résultat. On chercha donc une méthode qui amènerait au bout plus vite et plus sûr. Sachant que la longueur des cycles est indépendante des « Steckerverbindungen » et que la forme de cycles est rarement la même dans deux jours différents, on tomba sur l'idée de cataloguer tous les cycles dans toutes les positions possibles des roues, c'est à dire dans 105456 positions.

Afin d'effectuer ce travail on construit une machine spéciale, le cyclomètre, qui contenait deux Enigmes couplées tellement que dans chaque position s'allumèrent simultanément une certaine quantité des petites lampes conforme à la longueur des cycles.

Ce travail exigeait une année de travail, mais le catalogue une fois faite on trouvait en quelques minutes l'ordre des roues, leur position et les « Steckerverbindungen » du jour.

17. La position fondamentale et la position des anneaux

Par position des roues nous comprenons toujours la différence entre la position fondamentale et la position des anneaux. Pour parvenir à la solution complète des clefs du jour, on doit trouver séparément la position fondamentale et la position des anneaux. Pour cela l'étude unique des clefs du message ne suffit pas, il faut passer aux textes des messages. Quand on résolvait le matériel du mois d'octobre et décembre 1931 dont les clefs étaient connues, on apercevait que le texte de plusieurs messages commençaient par les lettres AN.

Afin de trouver séparément la position fondamentale et la position des anneaux, on prenait un message quelconque, supposant qu'il commence par les lettres AN et on essayait dans toutes les positions de la machine si notre supposition était juste - un travail onéreux parce qu'on doit examiner $26^3 = 17576$ positions.

Plus tard on constata que, si un message commençait par les lettres AN quelques positions de la roue droite étaient a priori impossibles. Lorsqu'on disposait pour un jour d'un nombre suffisant des messages, ou on pouvait supposer AN au commencement, on parvenait presque toujours à l'aide d'un simple calcul à fixer la position exacte de la roue droite.

18. Quelques observations

Décrivant le gril et le cyclomètre on a supposé que la roue de milieu ne tourne pas pendant le chiffrement de la clef individuelle. En réalité cette supposition n'est pas indispensable, au contraire la détermination de la position fondamentale et de la position des anneaux est plus facile justement quand la rue de milieu tourne. Nous nous rapportons au lecteur d'examiner les détails du travail dans ces conditions.

On a remarqué que, pour une journée donnée, les six nombres forment la position fondamentale et la position des anneaux étaient toujours différents entre eux. Cette constatation conduisait dans certains cas non seulement à une considérable simplification du travail, mais elle permettait aussi dans les années ultérieures à appliquer convenablement la méthode Herivel dont ou parlera encore plus tard. Il y avait aussi de périodes où tous les 24 nombres qui, dans 4 journées successives formaient les positions fondamentales et les positions des anneaux étaient différents entre eux.

On a fait de pareilles observations à des temps divers aussi avec les « Steckerverbindung ».

23. La détermination de la position des roues

Chez le nouveau procédé de chiffrement on chiffrait les clefs individuelles sortant de différentes position des roues. Il s'ensuit qui la théorie des cycles et toutes les méthodes basées sur cette théorie, c'est à dire les méthodes de détermination des clefs individuelles, le gril, le cyclomètre, n'étaient plus valables.

On ne demeurait pas les bras croisés mais on se mettait à l'examen du nouveau procédé. On établira avant tout ce qu'il suit. Si le matériel était assez étendu, on trouvait de temps en temps de paires de télégrammes pour lesquelles les premières et aussi les deuxièmes lettres de la position fondamentale étaient identiques et pour lesquelles les troisièmes lettres se trouvaient dans l'alphabet côte à côte ou presque côte à côte comme par exemple TKP et TKR. Si alors par hasard aussi dans les clefs individuelles paraissent deux lettres identiques sur des places correspondantes, on y peut parfois conclure quelle roue se trouve à la droite ou au milieu. Nous voulons expliquer les différentes possibilités par quelques exemples.

1) Supposons que nous avons trouvé deux messages avec des clefs suivantes:

Position fondamentale	Clef individuelle
TKP	ANV CKB
TKR	VTS JQM

Dans ce cas il est sûr que, entre les lettres P et R, la roue de milieu tourne, c'est à dire que à droit se trouve la rue I parce que cette roue et seulement cette roue provoque un tournement entre les lettres Q et S.

Dans le cas contraire correspondaient aux deux lettres égales V aussi deux lettres égales B (ou J).

2)

Position fondamentale	Clef individuelle
TKP	ANV CKB
TKR	VTS BQM

Dans ce cas il est peu probable qu'il y ait un tournoyement entre P et R, c'est à dire que la roue droite soit la roue I.

3) Les positions fondamentales avec deux lettres différentes du milieu peuvent aussi donner parfois des informations sur l'ordre des roues, comme démontre l'exemple suivant:

Position fondamentale	Clef individuelle
TKP	ANV CKB
TLR	VTS JQM

Dans ce cas un tournoyement de la roue de milieu entre P et R est impossible, la roue de droite est donc différente de la roue I.

5) Même les positions fondamentales dont les lettres premières sont différentes, peuvent donner renseignements sur l'ordre des roues :

Position fondamentale	Clef individuelle
TJG	CMS PKR
UKG	CWT PLJ

Dans ce cas il est probable qu'il y avait un tournoyement entre J et K de la rue de gauche, c'est à dire que la roue de milieu est la roue IV.

On peut tirer de pareilles conclusion dans des autres cas.

24. Les „bombes"

Déjà quelques jours après l'introduction du nouveau procédé de chiffrement on a pris un projet comment on pouvait enlever les nouvelles difficultés. Notre marche des idées était la suivante :

Prenons un certain nombre de messages et écrivons leur positions fondamentales et leurs clefs individuelles :

1.	K T L	W O C	D R B	7.	G R A	F D R	Y W D
2.	S V W	K K M	I Y S	8.	M D O	O T W	Y Z W
3.	J O T	I W A	B W N	9.	K J C	F S W	R S E
4.	E D C	D S P	L J C	10.	S G F	T E Y	A S R
5.	G D K	W A V	W H A	11.	A G H	M D F	R H F
6.	B W K	T C A	T O C	12.	J B R	W L T	S O Q

Dirigeons maintenant notre attention sur le message Nr. 3. Dans sa clef individuelle la lettre W se présente deux fois dans l'intervalle de 3 lettres. Cela signifie que dans une certaine position de la machine la lettre W donnerait une lettre pour nous inconnue, disons X, et que trois positions plus tard la même lettre W donnerait encore une fois la même lettre X. Nous faisons encore une hypothèse que la lettre W ne fut pas modifiée par les « Steckerverbindung » ce qui (avec 5 – 8 Steckerverbindung) arrive dans 50% des cas.

On pourrait alors rechercher la juste position des roues en touchant la lettre W en même temps dans deux machines dont les positions des roues différent de trois lettres et que l'on fait tourner synchroniquement. Chaque fois ou la même lettre s'allume simultanément dans les deux machines, nous avons devant nous un cas qui peut être juste et qu'il faut dont examiner à part.

Mais de tels cas il y avait trop souvent. On prend donc lieu de un message trois message dans lesquels la lettre W paraisse deux fois dans un intervalle de trois lettres. Dans notre exemple ce seraient les messages 3, 5 et 8. Mais alors il faut se servir naturellement au lieu de deux de six machines. En réalité, se serait excessivement inopportun si l'on voulait vraiment manipuler avec six machines isolées. C'est pourquoi on inventa une machine appelée bombe, qui correspondait à 6 machines « Enigma », prossédait une impulsion électrique, et s'arrêtait à chaque cas favorable automatiquement. Dans le bureau polonais des chiffres on fabriqua 6 bombes correspondant aux 6 ordres des roues (les roues IV et V n'étaient pas encore en emploi). Chaque bombe venait à bout des 17576 cas possibles dans une heure et demie.

25. Les filets

La construction des bombes n'était pas encore finie, quand y avait déjà des nouveaux changements. Le 15 décembre 1938 les roues IV et V furent introduites, c'est à dire le nombre des ordres des roues décuplé. Deux semaines plus tard on augmentera le nombre de « Steckerverbindung » à 7 – 10. Les bombes, perdaient pratiquement une grande partie de leur importance par ces changements, parce que la solution d'une journée exigeait maintenant beaucoup de temps. On réussirait parfois par la méthode décrivée plus haut, à déterminer en partie l'ordre des roues, mais seulement quand on avait beaucoup de matériel, mais cela n'arrivait pas souvent. Au surplus l'application des bombes était limitée par les « Steckerverbindung ». On créa donc déjà très tôt une nouvelle méthode qui était indépendant du nombre des « Steckerverbindung ».

Pour expliquer la nouvelle méthode nous devons avant tout introduire une nouvelle notion, celle des positions masculines et féminines. Retournons encore une fois aux messages données sur page 21.

1.	K	T	L	W	O	C	D	R	B
2.	S	V	W	K	K	M	I	Y	S
3.	J	O	T	I	W	A	B	W	N
4.	E	D	C	D	S	P	L	J	C
5.	G	D	K	W	A	V	W	H	A
6.	B	W	K	T	C	A	T	O	C
7.	G	R	A	F	D	R	Y	W	D
8.	M	D	O	O	T	W	Y	Z	W
9.	K	J	C	F	S	W	R	S	E
10.	S	G	F	T	E	Y	A	S	R
11.	A	G	H	M	D	F	R	H	F
12.	J	B	R	W	L	T	S	O	Q

Un cas comme dans la clef Nr. 3 qu'une lettre (dans l'exemple la lettre W) paraisse deux fois à une distance de trois lettres, ne peut se produire dans toutes les positions. Par des calculs on peut montrer que cela n'arrive que dans 40% de toutes les cas (plus précis le rapport est égal à $1 - (1/\sqrt{e})$, e étant la base des logarithmes naturelles). Nous appelons ces positions positions féminines, les autres masculines.

Dans notre exemple les messages 3, 5, 8, 9 et 11 appartiennent sûrement aux positions féminines, quant au reste on ne peut rien dire. Les « Steckerverbindung » ont naturellement une influence sur les lettres des clef mais non sur le sexe des positions.

On pourrait donc faire un catalogue avec toutes les positions féminines et chercher dans ce catalogue si l'on ne trouve pas six positions féminines dont la distance est la même que la distance des positions fondamentales JOU, GKD, BWK, MDR, KJD, AGK (il faut aussi tenir compte à des tournoyements possibles de la roue du milieu et du gauche).

Mais comme cela serait en pratique inexécutable on inventa les ainsi nommés filets. Pour chaque ordre des roues on inscrit toutes les positions féminines sur 26 feuilles de papier, dont chacune contient 26x26 cases, et cela en quadruple exécution. Les diverses feuilles correspondent aux 26 positions de la roue gauche, les 26x26 cases de chaque feuille aux 26x26 positions de la roue de milieu et de la droite. On expliquera la cause de la quadruple exécution plus bas. On perfore les cases correspondant à des positions féminines (d'où le nom filet).

Maintenant on pose, pour revenir à notre exemple, 6 parmi les 26 feuilles l'une sur l'autre dans une succession et une position qui correspondent aux distances mutuelles des positions fondamentales. Si simultanément sur toutes les feuilles a la même place parait un trou, alors nous avons affaire à un cas qui peut être favorable et que l'on faut examiner séparément. Pour épuiser tous les cas possibles il faut échanger les feuilles cycliquement. Sur chaque feuille se trouvent les 26x26 cases dans une quadruple exécution parce qu'on ne pose pas les feuilles directement l'une sur l'autre mais décalées l'une envers l'autre.

Le résultat dépend d'une mise extrêmement soignée des feuilles l'une sur l'autre dans la juste position et s'est pourquoi on confectionna toujours avant la travail une petite fiche, appelée le menu, sur laquelle était inscrit la succession et la position mutuelle des feuilles.

La connaissance, quelles positions sont masculines et quelles féminines, fut prise aux catalogues pour le cyclomètre. Car il est clair que les positions féminines correspondent aux substitutions qui contiennent des cycles composées d'une seule lettre.

L'examen des cas favorables fut aussi exécuté à l'aide du cyclomètre. Mais comme cela exigeait beaucoup de temps, on voulait confectionner des catalogues spéciaux, dans lesquelles entrent non seulement toutes les positions féminines, mais aussi les lettres qui se présentent dans tous les cycles composées d'une seule lettre. Mais cette idée ne fut réalisée que plus tard, par le bureau anglais des chiffres.

28. Méthode Knox

Le cryptologue anglaise avait remarqué que les chiffreurs allemands choisissent souvent comme position fondamentale les lettres qui paraissent dans les fenêtres de la machine après avoir terminé le chiffrement du message précèdent. Cela arrivait surtout dans les messages composés de plusieurs parties. Il suffisait donc dans ces cas soustraire de la position fondamentale le longueur du message précédente pour obtenir la clef individuelle (en clair) du message précèdent. Quand on obtenait alors des clefs caractéristiques comme ASD, WER, OKL dans plusieurs parties d'un même message, on était sur que le chiffreur a commis une telle faute. Comme il fallait pendant la soustraction tenir compte des tournoyements possibles de la roue de milieu et de gauche, il était possible de déterminer en partie l'ordre des roue et réduire en cas favorable le nombre des ordres possibles de 60 à 3. Il était aussi très important que par cette méthode on connaissait les clefs (en clair) de quelques messages.

Cette méthode fournissait de services précieuses pendant la campagne norvégienne ou on résolvait chaque journée obtenant ainsi du matériel d'une extrême importance.

29. Les catalogues pour les filets

Dans l'entretemps les Anglais ont réalisé encore une autre idée des cryptologues polonais. On a déjà mentionné que la vérification des cas possibles obtenus par les filets exigeait beaucoup de travail et de temps. Il fallait chaque fois chercher à l'aide du cyclomètre les lettres qui déterminaient le caractère féminin de la position, et comparer avec les lettres qui entraient dans la clef individuelle correspondante. Déjà en Pologne on a voulu fabriquer des catalogues qui contiendraient les lettres en question de toutes les positions féminines, mais des difficultés techniques empêchaient l'exécution de cette idée. Maintenant elle fut réalisée par les Anglais à l'aide de la même machines qui servait à la fabrication des filets, encore un exemple brillant de la fécondité de la coopération polonais-français-anglaise. Grâce aux possibilités financières et organisatrices de nos collègues anglais nos plans, qui autrement ne verraient probablement jamais le jour, furent réalises sans égard aux frais et difficultés.

30. La méthode Herivel

Un autre cryptologue fit la découverture suivante: Quand les chiffreurs allemands mettaient après minuit ou le matin la machine a chiffrer au point pour le jour donnée, il arrivait qu'il ne tiraient pas les roues et après la mise au point des anneaux, ne les tournaient pas, et qu'il choisissaient comme position fondamentale pour la premier message les lettres qu'ils voyaient dans les fenêtres de la machine. Ainsi il passait que la position fondamentale de ce premier message ne différait pas beaucoup de la position des anneaux établi pour cette journée.

Comparant les positions fondamentales des messages chiffrés par des divers chiffreurs après minuit ou au grand matin, il était souvent possible à déterminer précisément ou avec une grande approximation la position des anneaux pour la journée donnée. Le temps exigé pour la résolution fut par cette découverte abrègé

prodigieusement de telle façon que les Anglais possédait souvent la clef pour toute la journée déjà tôt au matin.

A l'occasion de cette méthode nous voulons ajouter l'observation suivante : Quand on trouva les connexions de la roue IV et V, il n'était pas possible a fixer la position des anneaux d'une manière définitive. Il existaient 26 positions différents, parmi lesquelles on choisit une par hasard. Après la résolution d'une nombre de journées (avant la découverte d'Herivel) on se rappela qu'autrefois les trois lettres formant la position des anneaux étaient toujours différents entre eux. Pour que cette marque subsistait aussi maintenant il fallait corriger la position des anneaux sur les roues IV et V. On trouva cette correction et la communiqua tout suite aux Anglais. Seulement après cette correction la méthode Herivel fut véritablement applicable.

31. Le troisième procède de chiffrement

Le 1 Mai 1940, avant l'offensive allemande contre la Belgique et la Hollande, le système du chiffrement fut change encore une fois. On ne chiffrait plus la clef individuelle deux fois, mais seulement une fois. Dans la tête de chaque message figuraient maintenant 6 lettres, les trois premières signifiaient la position fondamentale, les trois dernières la clé chiffrée individuelle. Cette situation se clarifia, parce que les chiffreurs allemands commirent, comme déjà une fois, l'imprudence de chiffrer une suite de message d'après le nouveau procède déjà la veille de son introduction. Cette journée, le 30 Avril 1940, fut résolu, du reste par les cryptologues polonais, et de telle façon on apprit, en quoi consistait le nouveau procède.

C'était un coup très dur. Les filets et les catalogues pour les filets devinrent tout à fait inutilisable, seulement les méthodes Knox et Herivel restaient valables. Les cryptologues polonais, qui a titre passager furent transposés de Vignolles a Paris, cherchaient à l'aide de ces méthodes résoudre une journée, mais vainement.

Les Anglais ont en plus de succès. Ils disposaient d'un matériel beaucoup plus volumineux, et ainsi il réussirent, après une pause de trois semaines a résoudre de nouveau une journée, le 20 Mai 1940, et bientôt presque toutes les journées suivantes. Ils envoyaient les clefs régulièrement, et de nouveau les spécialistes polonais étaient assis aux deux machines d'origine de Varsovie pour aider à lire le matériel extrêmement important. Après l'évacuation de Paris le travail fut continué à La Ferté-St-Aubin et il ne fut interrompu qu'immédiatement avant l'armistice. La dernière journée pour laquelle les Anglais envoyèrent la clef, était le 16 Juin 1940.

32.

„Steckerverbindungen tauschen sechs Paar Buchstaben" veut dire:

La « Steckerverbindung » est composée de six paire de lettres.

Chaque paire de lettres effectue une substitution additionnelle de telle façon que les deux lettres d'une paire sont remplacées l'une par l'autre aussi bien dans le clair que dans le chiffre de chaque texte.