ROCZNIKI POLSKIEGO TOWARZYSTWA MATEMATYCZNEGO
Seria II: WIADOMOŚCI MATEMATYCZNE XXIII (1980)

wmptm 1897

Ministerstwo Nauki i Szkolnictwa Wyższego

MARIAN REJEWSKI

Jak matematycy polscy rozszyfrowali Enigmę

Od Redakcji. Rozpowszechnione przekonanie, że w dwudziestoleciu międzywojennym nie prowadzono w Polsce ważniejszych prac z zastosowań matematyki, nie wydaje się słuszne. W rzeczywistości bowiem w okresie tym – oprócz cennych wyników m. in. z mechaniki – w dwóch dziedzinach uzyskano u nas wyniki o wielkiej doniosłości: fundamentalne prace Jerzego Spławy-Neymana, które wywarły wielki wpływ na rozwój statystyki matematycznej w XX w. (por. *Wiadom. Mat.* 16 (1973), str. 55–70) oraz rozwikłanie zasad konstrukcji i użytkowania maszyny Enigma, używanej przez siły zbrojne III Rzeszy. Praca trójki matematyków polskich – z oczywistych względów dawniej nie ujawniana – walnie przyczyniła się do późniejszego zwycięstwa aliantów w II wojnie światowej; niewykluczone też, że wywarła pewien wpływ na brytyjskie prace konstrukcyjne, które doprowadziły do budowy pierwszych komputerów.

Niemieccy specjaliści uważali, że nawet gdyby przeciwnik zdobył egzemplarz maszyny i znał zasadę jej działania, to i tak rozszyfrowanie depesz byłoby absolutnie niemożliwe. Było to rzeczywiście niemożliwe przy ówczesnym stanie kryptologii i wymagało istotnie nowych metod. Zasługi polskie przy rozszyfrowaniu Enigmy zostały szeroko spopularyzowane przez historyków i dziennikarzy, a sama nazwa (pochodząca od greckiego słowa *ainigma* – zagadka, tajemnica) jest dobrze znana. Mało kto jednak wie, że istotną rolę odegrało tam zastosowanie metod matematycznych, przede wszystkim grup permutacji. Do niedawna brak było jakichkolwiek publikacji opisujących matematyczną stronę prac nad Enigmą. Obecnie można to znaleźć w [12] (por. [9]), aczkolwiek z dużymi skrótami i uproszczeniami.

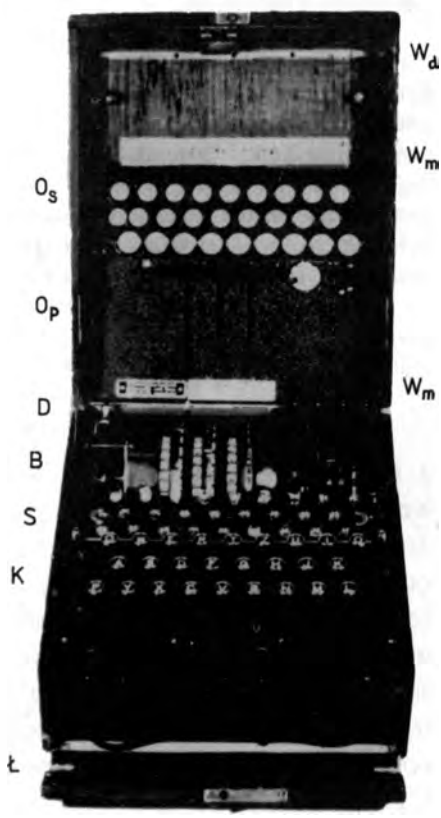
Poniższy artykuł, dający przegląd metod, którymi posługiwali się w latach 1932–1939 kryptolodzy polscy dla opanowania niemieckiego szyfru wojskowego Enigma, jest ważnym materiałem dla historii matematyki.

Wstęp. W końcu roku 1927, lub może na początku roku 1928, nadeszła z Rzeszy Niemieckiej do Urzędu Celnego w Warszawie przesyłka mająca, według deklaracji, zawierać sprzęt radiowy. Przedstawiciel niemieckiej firmy domagał się bardzo usilnie zwrotu tej przesyłki do Rzeszy jeszcze przed odprawą celną, jako wysłanej omyłkowo z innym sprzętem. Jego nalegania były tak natarczywe, że wzbudziły czujność urzędników celnych, którzy zawiadomili Biuro Szyfrów Oddziału II Sztabu Głównego, instytucję zainteresowaną wszelkimi nowościami w dziedzinie radiosprzętu. A ponieważ była to przypadkowo sobota po południu, więc wydelegowani przez Biuro pracownicy mieli czas sprawę spokojnie zbadać. Skrzynię ostrożnie otworzono i przekonano się, że istotnie sprzętu radiowego nie zawierała, była w niej

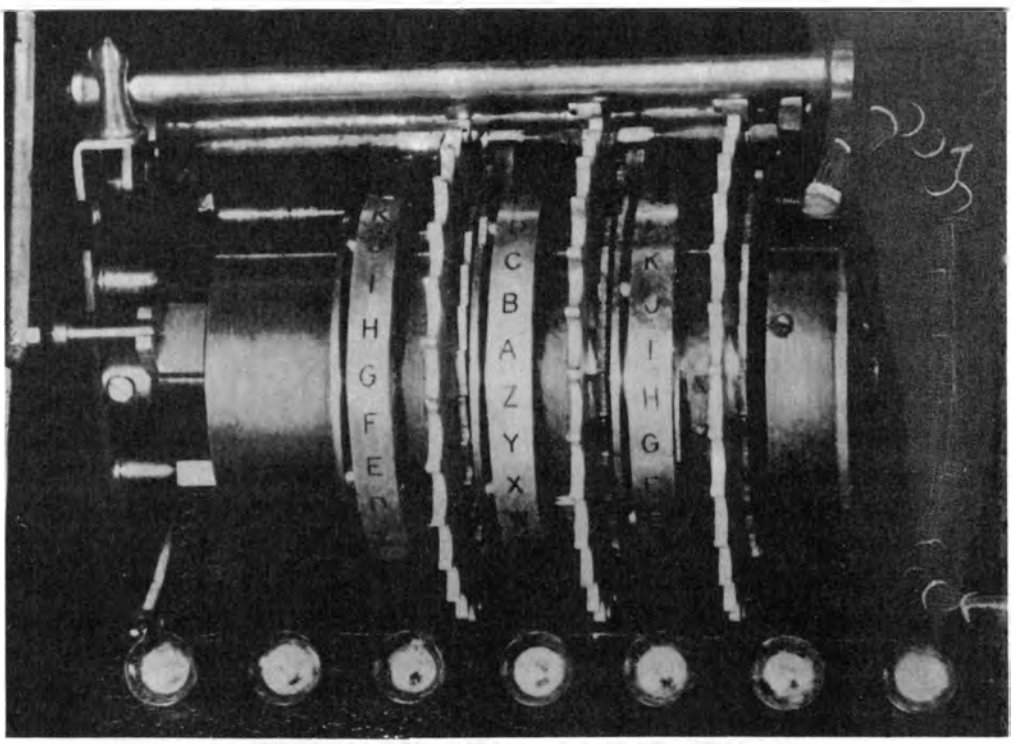
natomiast maszyna do szyfrowania. Maszynę bardzo dokładnie zbadano, po czym skrzynię znów starannie zamknięto.

Można się łatwo domyślić, że ową maszyną do szyfrowania była Enigma, oczywiście typu handlowego, gdyż typ wojskowy w tym czasie w ogóle jeszcze nie był w użyciu. Błahy ów epizod nie miał więc żadnego praktycznego znaczenia, stanowi jednak datę, od której zaczęło się zainteresowanie Biura Szyfrów maszyną Enigma, objawiające się przede wszystkim nabyciem drogą całkowicie legalną jednego egzemplarza maszyny typu handlowego. Gdy z dniem 15 lipca 1928 roku na falach eteru pojawiły się pierwsze depesze zaszyfrowane maszynowo, nadane przez wojskowe stacje niemieckie, polscy radiotelegrafiści pracujący w stacjach podsłuchowych zaczęli je odbierać, a polscy kryptolodzy zatrudnieni w sekcji niemieckiej Biura Szyfrów otrzymali polecenie podjęcia próby ich odczytania. Praca była jednak bezowocna i po pewnym czasie zaniechano jej. Pozostały bardzo nikłe ślady tej pracy w postaci kilku gęsto zapisanych arkuszy papieru, pozostała też maszyna Enigma typu handlowego.

Jednak Biuro Szyfrów, którego szefem w tym czasie był mjr F. Pokorny (spokrewniony z wybitnym kryptologiem armii austriackiej w I wojnie światowej, kpt. Hermanem Pokornym), nie dało za wygraną. Dlatego na przełomie lat 1928/29 zorganizowano w Poznaniu kurs kryptologii dla studentów



Rys. 1. Ogólny widok Enigmy typu wojskowego. W_d – wieko drewniane zewnętrzne, W_m – wieko metalowe, zakrywające bębenki i lampki, O_s – okienka w wieku metalowym do obserwacji liter na ruchomych pierścieniach, B – bęsię odpowiednia litera), O_p – okienka do obserwacji liter na ruchomych pierścianiach, B – bębenki (r, l, m, n, h), D – dźwignia dociskająca bębenki, S – lampki, K – klawisze, Ł – łącznica wtyczkowa



Rys. 2. Bębenki szyfrujące (por. ryciny 1 i 4)

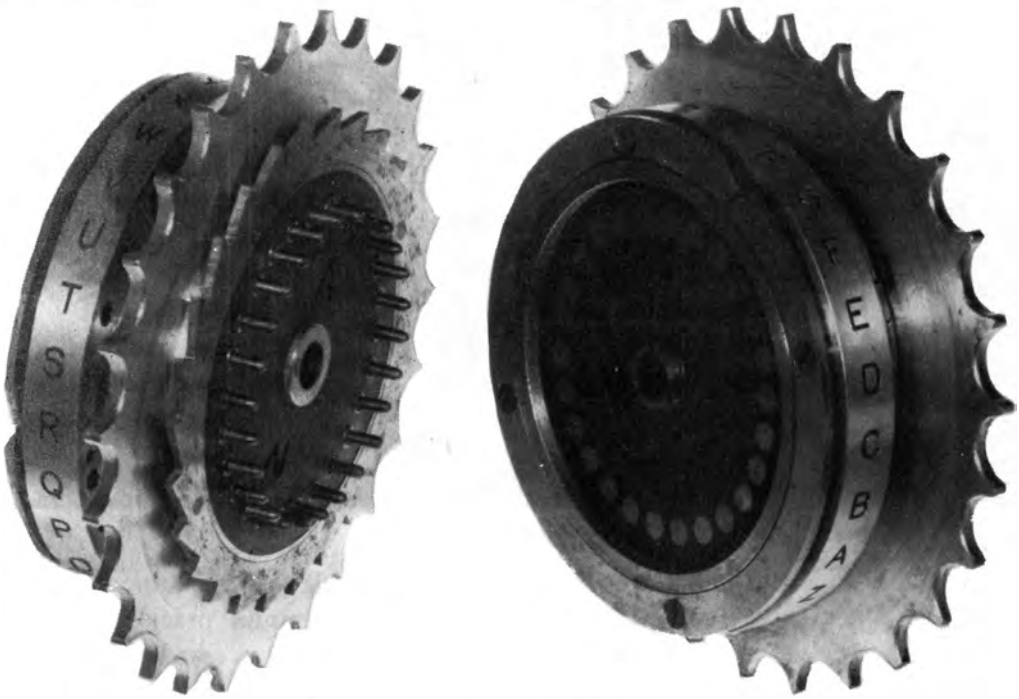
kończących studia matematyczne i władających biegle językiem niemieckim. Następnie, po zakończeniu kursu, stworzono w Poznaniu, przejściowo dla kilku uczestników kursu, ekspozyturę Biura Szyfrów i wreszcie, z dniem 1 września 1932 roku, trzech zatrudnionych w ekspozyturze absolwentów matematyki, Jerzego Różyckiego, Henryka Zygalskiego i mnie, zaangażowano do stałej pracy w Biurze Szyfrów w Warszawie, mieszczącym się w nie istniejącym obecnie gmachu Sztabu Głównego przy pl. Saskim.

Tam jako pierwsze samodzielne zadanie otrzymaliśmy do rozwiązania kod niemieckiej marynarki wojennej, w czym bardzo pomocną była znajomość języka niemieckiego. Do dalszych prac jednak, jak postaram się okazać, nie tyle znajomość języka, ile znajomość matematyki była przydatna i jest wielką zasługą wspomnianego już mjr. Pokornego, jak i jego następcy, ppłk. Jarola G. Langera i jego zastępcy, kpt. Maksymiliana Ciężkiego, że znacznie wcześniej niż w innych biurach szyfrów zorientowali się w celowości wymagania od kryptologów obok znajomości języków jeszcze studiów matematycznych.

W tym miejscu wspomnę o jeszcze jednej postaci, którą wymienię ponownie później, a która odegrała w sprawie złamania szyfru Enigma rolę zupełnie wyjątkową. Mam na myśli zmarłego w 1976 roku generała armii francuskiej Gustave Bertranda, który w roku 1932 (w randze kapitana), jako kierownik sekcji D wywiadu francuskiego, zdobył i dostarczył polskiemu

Biuru Szyfrów materiały wywiadowcze o olbrzymim znaczeniu, a i poza tym jeszcze kilkakrotnie wpłynął w sposób istotny na los polskich kryptologów i wreszcie ujawnił przed światem ich decydujący udział w złamaniu Enigmy, [1].

Nie jest moim zamiarem opisać szczegółowo maszynę handlową lub wojskową, podam jedynie w wielkim skrócie to, co jest nieodzowne dla

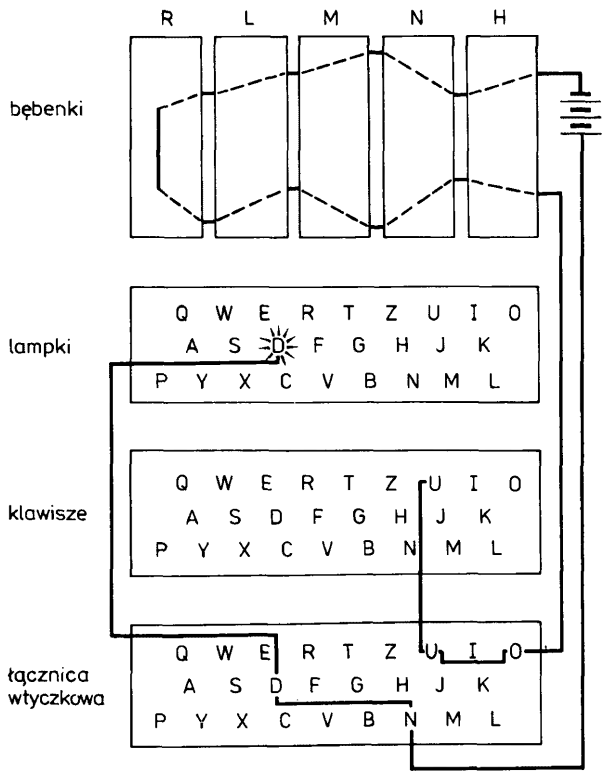


Rys. 3. Dwie strony bębenka szyfrującego

zrozumienia dalszych wywodów. Maszyna wojskowa (rys. 1) miała wymiary i wygląd przenośnej maszyny do pisania, miała 26 klawiszy oznaczonych literami alfabetu łacińskiego, lecz zamiast czcionek miała deskę z umieszczonymi na niej 26 żarówkami (takimi, jakich używa się w lampkach kieszonkowych) oznaczonymi tymi samymi literami co klawisze. Znajdowało się w niej też źródło prądu w postaci bateryjki.

Najistotniejszą jednak częścią maszyny były umieszczone na jednej osi trzy mogące się obracać — wzajemnie przestawialne — bębenki szyfrujące I, II, III (na pozycjach oznaczonych literami L, M, N na rys. 1 i 4) oraz czwarty (w maszynie wojskowej nieruchomy), tzw. *bębenek odwracający* R. Każdy z bębenków szyfrujących był zaopatrzony w pierścień z wyrytymi na obwodzie 26 literami alfabetu, widocznymi na rysunkach 2 i 3. Literę znajdującą się u góry było widać w małym okienku umieszczonym w metalowym wieku maszyny. Pierścień mógł zmieniać położenie w stosunku do reszty bębenka.

Środkową część bębenków stanowił ebonitowy krążek, na którym po jednej stronie znajdowało się koncentrycznie 26 kontaktów stałych (widocznych po prawej stronie rysunku 3), połączonych izolowanymi drucikami w sposób nieregularny ze znajdującymi się po drugiej stronie, też koncentrycznie umieszczonymi 26 kontaktami sprężynującymi (widocznymi z lewej strony rysunku 3). Bębenek odwracający miał tylko po jednej stronie 26 kontaktów sprężynujących, połączonych w sposób nieregularny między sobą.



Rys. 4. Schemat przebiegu prądu w Enigmie wojskowej

Gdy naciśnięto klawisz, bębenek szyfrujący *N* (tzn. bębenek znajdujący się na pozycji N, najbardziej na prawo), wykonywał obrót o 1/26 część obwodu, prąd od naciśniętego klawisza płynął poprzez trzy bębenki szyfrujące, przez bębenek odwracający, ponownie przez bębenki szyfrujące i zapalał którąś z żarówek (rys. 4). Gdy w danym momencie nacisnęło się klawisz np. z literą *u*, zapalała się lampka z inną literą (zawsze różną od naciśniętej, na rys. 4 jest to litera *d*), przy następnym naciśnięciu tego samego klawisza *u* otrzymywało się — na skutek dokonanego w międzyczasie obrotu bębenków — literę tę zaszyfrowaną już inaczej, tzn. zapalała się już na ogół inna lampka.

Gdy w ten sposób wystukiwało się kolejne litery tekstu otwartego, zwanego *klerem* (od słowa *clair*), wówczas litery zapalających się sukcesyw-

nie żarówek tworzyły *tekst zaszyfrowany*, czyli szyfrogram lub szyfr. Gdy natomiast wystukiwało się w ten sam sposób kolejne litery szyfru, wówczas litery zapalających się kolejno żarówek odtwarzały kler (innymi słowy, przy każdym ustawieniu bębenków aktualna permutacja szyfrująca była inwolucją, będącą iloczynem 13 transpozycji). Sprawia to bębenek odwracający.

Wiadomo, że bębenków szyfrujących o różnych połączeniach można utworzyć

$$26! = 403291461126605635584000000,$$

a różnych bębenków odwracających

$$\frac{26!}{2^{13} \cdot 13!} = 7905853580025;$$

fabryka wyrabiająca owe Enigmy mogła więc dostarczać każdemu odbiorcy zamówioną partię maszyn z odmiennymi połączeniami bębenków. Odnosiło się to w szczególności do bębenków maszyn wojskowych, które oczywiście musiały mieć inne połączenia niż bębenki jakichkolwiek maszyn handlowych. Wszystkie natomiast komplety bębenków maszyn wojskowych, których liczbę w czasie wojny ocenia się na 100 do 200 tysięcy, miały te same połączenia, tak że szyfranci jakichkolwiek jednostek wojskowych mogli porozumiewać się między sobą za pomocą tych maszyn, pod warunkiem atoli, że mieli maszyny nastawione na ten sam klucz.

Albowiem *klucz*, to była druga, obok połączeń bębenków, tajemnica wojskowego szyfru Enigma. Każdy bębenek szyfrujący można nastawić na 26 sposobów, trzy bębenki można więc nastawić na $26^3 = 17576$ sposobów, a ponieważ kolejność trzech bębenków na osi można jeszcze zmieniać na sześć sposobów, więc nastawienie i kolejność bębenków dopuszcza razem

$$6 \cdot 26^3 = 105456$$

możliwości. Jednak liczba ta wydawała się specjalistom z niemieckiego biura szyfrów za niska i dlatego dodano do maszyn typu wojskowego coś w rodzaju łącznicy telefonicznej, za pomocą której można było sześć par liter dowolnie ze sobą pozamieniać, co stworzyło dodatkowo dalszych

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

możliwości. Teraz więc, rozumowali Niemcy, jeżeli nawet przeciwnik zdobędzie, np. w wyniku działań wojennych, oryginalną maszynę wojskową, to i tak, nie znając klucza, żadnej depeszy nie odczyta. Postaram się jednak pokazać, że Niemcy pod tym względem się mylili.

Zespół narzuconych szyfrantom nastawień, a więc ustawienie bębenków, ich kolejność, połączenia na łącznicy i jeszcze pewne dalsze nastawienia, o których na razie nie wspominam, nazywano *kluczem dziennym* (chociaż

niektóre elementy tego klucza zmieniały się częściej niż co dobę, zwłaszcza w ostatniej fazie wojny, a inne rzadziej, przynajmniej w początkowym okresie używania maszyn). Szyfranci otrzymywali klucze dzienne w postaci drukowanych tabel na okres całego miesiąca.

Ale na tym nie koniec jeszcze tajemnic wojskowego szyfru Enigma. Zaszyfrowanie wszystkich depesz w danym dniu z tej samej pozycji bębenków oznaczałoby dekonspirację tych depesz. Wówczas bowiem pierwsze litery wszystkich depesz stanowiłyby zwykłą literówkę, czyli szyfr bardzo prymitywny, przy wystarczającym materiale łatwo rozwiązalny, wszystkie drugie litery depesz stanowiłyby inną literówkę itd. Nie są to rozważania tylko teoretyczne. Przecież tym właśnie sposobem rozwiązaliśmy we Francji w roku 1940 szwajcarską maszynę do szyfrowania typu Enigma. Istniała zatem konieczność pozostawienia do decyzji niemieckiego szyfranta wyboru pozycji bębenków, od której zamierzał rozpocząć szyfrowanie danej depeszy. I tę pozycję bębenków musiał on przekazać swemu koledze deszyfrantowi, aby i ten wiedział, jak bębenki nastawić, by móc depeszę odczytać. Wymagało to podania trzech, w przekonaniu Niemców koniecznie zaszyfrowanych, liter, a ponieważ droga radiowa nie zawsze zapewniała dobry odbiór, należało litery te podać – zaszyfrowane dwukrotnie, po czym otrzymane w ten sposób sześć liter umieszczano na początku danej depeszy. Owe trzy dowolnie przez szyfranta wybrane litery zwano – w odróżnieniu od kluczy dziennych – *kluczem depeszy* i one stanowiły trzecią tajemnicę wojskowego szyfru Enigma.

Klucze depeszy. Dzisiaj, po upływie blisko pół wieku, nie pamiętam już, czy orientowałem się w różnicy budowy Enigmy wojskowej i Enigmy handlowej, gdy jesienią 1932 roku odseparowano mnie od mych dotychczasowych kolegów Różyckiego i Zygalskiego, przydzielono osobny pokoik w gmachu Sztabu i polecono wznowić badania nad Enigmą zaniechane przez mych poprzedników. Nie jest wykluczone, że informacje te otrzymałem nieco później. Zresztą w fazie początkowej mej pracy nie były mi potrzebne. Oddano do mej dyspozycji wspomniany już egzemplarz maszyny handlowej oraz codziennie kilkadziesiąt depesz zaszyfrowanych Enigmą wojskową.

To, że pierwsze sześć liter każdej depeszy stanowiły jej trzyliterowy klucz dwukrotnie zaszyfrowany, rzucało się w oczy i nad tym nie będę się zatrzymywał. Ale co robić dalej? Podam naprzód, jak wówczas postąpiłem, a potem spróbuję swe postępowanie uzasadnić.

Wypisałem oddzielnie sześć pierwszych liter wszystkich depesz danego dnia, czyli ich klucze dwukrotnie zaszyfrowane. Wszystkie klucze, które miały tę samą pierwszą literę, miały oczywiście też tę samą czwartą literę. To samo można też powiedzieć o drugich i piątych, oraz o trzecich i szóstych literach. Wybrałem dowolnie którykolwiek klucz i napisałem pierwszą i obok niej czwartą literę. Potem wyszukałem klucz mający jako pierwszą literę –

czwartą literę poprzedniego klucza, czwartą zaś literę drugiego klucza napisałem obok czwartej litery poprzedniego klucza. Postępując tak dalej, doszedłem po pewnej liczbie kroków do pierwszej już napisanej litery. Drugi raz tej samej litery już nie napisałem, lecz dotychczas napisane litery ująłem w nawias. Mały przykład lepiej wyjaśni moje postępowanie. Niech

dmq vbn
von puy
puc fmq

stanowią trzy, nieco sztucznie wybrane, zaszyfrowane klucze depesz danego dnia. Dla większej przejrzystości klucze przedzieliłem na pół, tak że pierwsze trzy litery stanowią klucz po pierwszym zaszyfrowaniu, a dalsze trzy litery po drugim zaszyfrowaniu. Biorę więc literę *d* z pierwszej depeszy i piszę obok niej czwartą literę, czyli *v*, obok *v* piszę *p*, potem obok *p* literę *f*. W ten sposób otrzymuję fragment

dvpf.

Z kluczy dalszych depesz wynikłoby, że powstałby cały cykl liter

(*dvpfkxgzyo*),

a z pozostałych kluczy powstałyby jeszcze dalsze cykle, tak że ogół cykli utworzonych z pierwszych i czwartych liter wyglądałby na przykład tak:

$$AD = (dvpfkxgzyo)\,(eijmunqlht)\,(bc)\,(rw)\,(a)\,(s),$$

przy czym ogół cykli oznaczyłem literami *AD* dla zaznaczenia, że powstał z pierwszych i czwartych liter kluczy depesz danego dnia. W podobny sposób postąpiłem z drugimi i piątymi oraz z trzecimi i szóstymi lterami kluczy i w ten sposób otrzymałem obraz wyglądający na przykład w ten sposób:

(1)
$$\begin{aligned} AD &= (dvpfkxgzyo)\,(eijmunqlht)\,(bc)\,(rw)\,(a)\,(s),\\ BE &= (blfqveoum)\,(hjpswizrn)\,(axt)\,(cgy)\,(d)\,(k),\\ CF &= (abviktjgfcqny)\,(duzrehlxwpsmo). \end{aligned}$$

Układ ten jest niezmiernie charakterystyczny i choć obraz takiego układu był każdego dnia inny, to jednak jedna cecha była stale ta sama, ta mianowicie, że cykle tej samej długości występowały w każdym wierszu zawsze w liczbie parzystej. Ze względu na rolę, jaką układ ten będzie odgrywał w dalszym ciągu, nazwałem go *układem charakterystycznym* albo krócej *charakterystyką* danego dnia.

Jak można wyjaśnić powstanie układu charakterystycznego? Jeżeli nacisnę kolejno wszystkie klawisze w ten sposób, aby nastawienie bębenków szyfrujących się nie zmieniało, na przykład przez przytrzymanie jednego klawisza, wówczas będą się zapalać coraz inne żarówki. Powstanie w ten sposób pewna permutacja liter. Przy innym nastawieniu bębenków permutacja

będzie oczywiście inna, ale bębenek odwracający powoduje, że wszystkie permutacje będą składały się z samych transpozycji, bo jeżeli uderzenie klawisza t na przykład spowodowałoby zapalenie się żarówki z, to uderzenie klawisza z przy tym samym nastawieniu bębenków spowodowałoby zapalenie się żarówki t (we wstępie wzmiankowałem, że przepuszczony przez maszynę kler daje szyfr, szyfr daje kler).

Można łatwo sprawdzić, że jeżeli sześć kolejnych permutacji powstających w czasie dwukrotnego szyfrowania kluczy depesz oznaczę literami od A do F, to iloczyny tych permutacji AD, BE, CF będą identyczne z wyrażeniami tworzącymi charakterystykę danego dnia i tym samym znajduje uzasadnienie sposób oznaczania tych wyrażeń.

Tak, ale dlaczego w tych wyrażeniach cykle tej samej długości występują zawsze w liczbie parzystej? I to można łatwo wyjaśnić. Można bowiem wyprowadzić następujące twierdzenie:

Jeżeli dwie permutacje X i Y tego samego stopnia składają się z samych transpozycji rozłącznych, to w ich iloczynie XY wystąpią cykle rozłączne tej samej długości w liczbie parzystej.

Można też udowodnić twierdzenie odwrotne:

Jeżeli w jakiejkolwiek permutacji (stopnia parzystego) cykle rozłączne tej samej długości występują w liczbie parzystej, to permutację tę można uważać za iloczyn XY dwóch permutacji X i Y, z których każda utworzona jest z samych transpozycji rozłącznych.

Łatwego dowodu tych twierdzeń nie podaję dla zaoszczędzenia miejsca. Można też wykazać, że

1) *litery wchodzące do jednej i tej samej transpozycji permutacji X lub Y wchodzą zawsze do dwóch różnych cykli tej samej permutacji XY;*

2) *jeżeli dwie litery znajdujące się w dwóch różnych cyklach tej samej długości permutacji XY należą do tej samej transpozycji, to sąsiadujące z nimi litery (jedna z prawej, druga z lewej strony) też należą do tej samej transpozycji.*

Z właściwej interpretacji powyższych ustaleń wynika, że wystarczy jeszcze znać zwyczaje szyfrantów, by całkowicie zrekonstruować wszystkie klucze depesz. Bo niech na przykład będzie wiadomo, że szyfranci lubią wybierać jako klucze depesz trzy jednakowe litery, jak *aaa*, *bbb*, itp. Spójrzmy na charakterystykę (1). Ponieważ w iloczynie AD litery a i s tworzą cykle jednoliterowe, przeto jeżeli wśród kluczy depesz ma się znajdować klucz *aaa*, to po zaszyfrowaniu pierwsza litera powinna być s. Przypuśćmy, że wśród zaszyfrowanych kluczy depesz danego dnia były trzy klucze rozpoczynające się na literę s:

sug smf
sjm spo
syx scw.

Zaszyfrowany klucz *sug smf* nie mógł powstać z liter *aaa*, bo druga litera *u* znajduje się w cyklu dziewięcioliterowym iloczynu *BE*, podczas gdy *a* znajduje się w cyklu trzyliterowym tego samego iloczynu. Tak samo, zaszyfrowany klucz *sjm spo* nie mógł powstać z liter *aaa*, gdyż litera *j* też znajduje się w cyklu dziewięcioliterowym. Natomiast zaszyfrowany klucz *syx scw* mógł powstać z liter *aaa*, gdyż *s* i *a* znajdują się w dwóch cyklach jednoliterowych iloczynu *AD*, *y* i *a* znajdują się w dwóch różnych cyklach trzyliterowego iloczynu *BE*, a także *x* i *a* znajdują się w dwóch różnych cyklach trzynastoliterowych iloczynu *CF*.

To, że zaszyfrowany klucz *syx scw* rzeczywiście oznaczał przed zaszyfrowaniem litery *aaa*, zdawał się potwierdzać fakt, że przy tym właśnie założeniu bardzo wiele innych zaszyfrowanych kluczy dawało się rozszyfrować jako ciągi *bbb*, *ccc*, itp.

A więc jedna z tajemnic szyfru Enigma, tajemnica kluczy depesz, została rozwiązana. Jest rzeczą interesującą, że dla osiągnięcia tego rezultatu nie była potrzebna znajomość ani połączeń bębenków, ani kluczy dziennych, czyli żadnej z pozostałych tajemnic szyfru Enigma. Była natomiast potrzebna wystarczająca liczba depesz z tego samego dnia, około 60 sztuk, tak aby dał się utworzyć układ charakterystyczny *AD*, *BE*, *CF*.

Prócz tego potrzebna była dobra znajomość zwyczajów szyfrantów co do wyboru kluczy depesz. Pierwszy raz, gdy założyłem, że będzie dużo kluczy w rodzaju *aaa*, *bbb*, itp., była to tylko hipoteza, która się jednak szczęśliwie sprawdziła. Potem śledzono już bardzo uważnie ewolucję upodobań szyfrantów i gdy wkrótce zabroniono im używania jako kluczy trzech identycznych liter, udawało się zawsze odkryć jakieś inne ich nawyki, chociażby ten, że skoro nie wolno im było używać trzech liter jednakowych, unikali powtarzania jakiejkolwiek litery chociażby dwukrotnie, a ta cecha też już wystarczała, by dojść, jakie były klucze depesz przed ich zaszyfrowaniem.

Takich i podobnych metod udało się opracować jeszcze kilka. Jest bowiem zjawiskiem znanym, że człowiek jako istota obdarzona świadomością i pamięcią nie ma możności imitowania przypadku w sposób doskonały, a zadaniem kryptologa jest m. in. wykryć i we właściwy sposób wykorzystać owe odchylenia od przypadku.

Połączenia bębenków. Byłoby lepiej dla Niemców, gdyby kluczy depesz w ogóle nie zaszyfrowywali. Bo szyfrowanie, jak widzieliśmy, i tak nie ustrzegło kluczy przed dekonspiracją, a w dodatku dostarczyło premii w postaci sześciu kolejnych permutacji od *A* do *F*. Ich znajomość miała mi, jak pokażę, przybliżyć znalezienie połączeń bębenków wojskowej Enigmy. Jednak w tym celu muszę to, co dzieje się wewnątrz maszyny, wyrazić za pomocą działań na permutacjach. Oznaczmy więc permutację spowodowaną przez łącznicę literą *S*, przez trzy bębenki szyfrujące – literami *L*, *M*, *N*, licząc

od lewej ku prawej stronie, a przez bębenek odwracający — literą R. Muszę jeszcze wymienić jeden bębenek, o którym dotychczas nie wspominałem, mianowicie bębenek wstępny, nieruchomy, stanowiący przejście od łącznicy do bębenka N; bębenek ten oznaczam literą H. Przebieg prądu można teraz wyrazić w sposób następujący:

$$SH\,NMLRL^{-1}M^{-1}H^{-1}S^{-1}.$$

Ponieważ jednak przy każdym naciśnięciu klawisza bębenek N wykona obrót o 1/26 część obwodu, przeto dla uwzględnienia tego obrotu musiałem wprowadzić jeszcze jedną specjalną permutację, którą zawsze oznaczać będę literą P i która każdą literę zamienia na literę następną w alfabecie: a na b, b na $c, \ldots, z$ na a. Teraz więc permutacje A do F mogę przedstawić w postaci następujących równań:

$$\begin{aligned}
A &= SHPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}H^{-1}S^{-1},\\
B &= SHP^2NP^{-2}MLRL^{-1}M^{-1}P^2N^{-1}P^{-2}H^{-1}S^{-1},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
F &= SHP^6NP^{-6}MLRL^{-1}M^{-1}P^6N^{-1}P^{-6}H^{-1}S^{-1}.
\end{aligned}$$

Pisząc te równania zakładałem milcząco, że obracał się tylko bębenek prawy, czyli N, natomiast bębenki L i M podczas kolejnych sześciu uderzeń klawiszy żadnych obrotów nie wykonały. Założenie to sprawdza się średnio w 21 przypadkach na 26, a więc dostatecznie często, aby je usprawiedliwić. W takim przypadku, we wszystkich powyższych równaniach powtarza się wyrażenie $MLRL^{-1}M^{-1}$, które mogę chwilowo zastąpić jedną literą Q, oznaczającą fikcyjny bębenek odwracający:

$$Q = MLRL^{-1}M^{-1}. \tag{2}$$

Pozwala to w znacznym stopniu uprościć nasz układ równań:

$$\begin{aligned}
A &= SHPNP^{-1}QPN^{-1}P^{-1}H^{-1}S^{-1},\\
B &= SHP^2NP^{-2}QP^2N^{-1}P^{-2}H^{-1}S^{-1},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
F &= SHP^6NP^{-6}QP^6N^{-1}P^{-6}H^{-1}S^{-1}.
\end{aligned} \tag{3}$$

Zadanie polegało właśnie na rozwiązaniu powyższego układu sześciu równań z czterema niewiadomymi permutacjami S, H, N i Q. Zdając sobie sprawę z trudności zadania, starałem się przede wszystkim zmniejszyć liczbę niewiadomych. Ponieważ w maszynie handlowej połączenia bębenka wstępnego miały postać

$$H = \begin{pmatrix} q\,w\,e\,r\,t\,z\,u\,i\,o\,a\,s\,d\,f\,g\,h\,j\,k\,p\,y\,x\,c\,v\,b\,n\,m\,l\\ a\,b\,c\,d\,e\,f\,g\,h\,i\,j\,k\,l\,m\,n\,o\,p\,q\,r\,s\,t\,u\,v\,w\,x\,y\,z \end{pmatrix},$$

czyli górny wiersz permutacji H przedstawiał alfabet w kolejności liter na klawiaturze maszyny, przeto przyjąłem, że w maszynie wojskowej permutacja H ma taki sam kształt, jako że w obu rodzajach maszyn, handlowych i woj-

skowych, litery na klawiszach miały taką samą kolejność. Przekonałem się później, że ta hipoteza była błędna, a jej przyjęcie spowodowało dużo zbędnej roboty i znaczną stratę czasu, tak że niewiele brakowało, by studiów nad Enigmą nie przerwano ponownie. Nastąpił tu więc dość niecodzienny przypadek: zakup przez Biuro Szyfrów maszyny handlowej w intencji ułatwienia złamania szyfru wojskowego Enigma w istocie bardzo je utrudnił.

Na razie zakładałem jednak, że permutacja H jest mi znana. Miałem więc układ sześciu równań z trzema niewiadomymi S, N i Q. I gdy zastanawiałem się, jak układ ten rozwiązać, dostarczono mi 9 grudnia 1932 roku, zupełnie nieoczekiwanie, w najwłaściwszej chwili, fotokopię dwóch tablic kluczy dziennych na wrzesień i październik 1932 roku.

Teraz sytuacja zmieniła się radykalnie. Ponieważ tablice kluczy zawierały też codzienne zmiany połączeń łącznicy, więc permutację S mogłem już uważać za znaną i przenieść ją, podobnie jak przyjętą jako znaną permutację H, na lewą stronę układu, który teraz uzyskał następującą postać:

$$\begin{aligned} H^{-1}S^{-1}ASH &= PNP^{-1}QPN^{-1}P^{-1}, \\ H^{-1}S^{-1}BSH &= P^2NP^{-2}QP^2N^{-1}P^{-2}, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ H^{-1}S^{-1}FSH &= P^6NP^{-6}QP^6N^{-1}P^{-6}. \end{aligned}$$

W tak zapisanym układzie wszystkie permutacje po lewej stronie są całkowicie znane, a po prawej stronie nie są znane tylko permutacje N i Q. Przekształćmy jeszcze obie strony pierwszego równania przez automorfizm wewnętrzny wyznaczony przez P, drugiego równania – przez P^2 itd. i dla skrócenia oznaczmy lewe strony literami od U do Z:

$$\begin{aligned} U &= P^{-1}H^{-1}S^{-1}ASHP &&= NP^{-1}QPN^{-1}, \\ V &= P^{-2}H^{-1}S^{-1}BSHP^2 &&= NP^{-2}QP^2N^{-1}, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ Z &= P^{-6}H^{-1}S^{-1}FSHP^6 &&= NP^{-6}QP^6N^{-1}. \end{aligned}$$

Następnie utwórzmy jeszcze iloczyny przemnażając po dwa kolejne z tych wyrażeń:

$$\begin{aligned} UV &= NP^{-1}(QP^{-1}QP)PN^{-1}, \\ VW &= NP^{-2}(QP^{-1}QP)P^2N^{-1}, \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ YZ &= NP^{-5}(QP^{-1}QP)P^5N^{-1}, \end{aligned}$$

skąd przez wyeliminowanie wspólnego wyrażenia $QP^{-1}QP$ otrzymujemy układ czterech równań z jedną tylko niewiadomą NPN^{-1}:

$$\begin{aligned} VW &= NP^{-1}N^{-1}(UV)NPN^{-1}, \\ WX &= NP^{-1}N^{-1}(VW)NPN^{-1}, \\ XY &= NP^{-1}N^{-1}(WX)NPN^{-1}, \\ YZ &= NP^{-1}N^{-1}(XY)NPN^{-1}. \end{aligned}$$

Widzimy, że wyrażenie VW jest przekształcone z wyrażenia UV za pomocą permutacji NPN^{-1}. Podpisując VW pod UV na wszystkie możliwe sposoby, a tych sposobów jest na ogół kilkadziesiąt, otrzymujemy kilkadziesiąt możliwych rozwiązań dla wyrażenia NPN^{-1}. Podobnie WX jest przekształcone z VW za pomocą tego samego wyrażenia NPN^{-1}. Podpisując więc WX pod VW otrzymamy znów kilkadziesiąt możliwych rozwiązań dla wyrażenia NPN^{-1}. Jedno z tych rozwiązań powinno być identyczne z jednym z poprzednio otrzymanych. To właśnie jest nasze szukane NPN^{-1}. Dwa ostatnie równania na XY i YZ są już zbyteczne.

Dalszy ciąg jest prosty. Wystarczy pod otrzymane wyrażenie NPN^{-1} podpisać znaną nam permutację P na wszystkie możliwe 26 sposobów, aby otrzymać 26 wariantów dla połączeń bębenka N. Który z tych wariantów wybierzemy, nie ma na razie większego znaczenia, gdyż wybór takiego czy innego wariantu oznacza tylko większe lub mniejsze skręcenie w bębenku N strony z kontaktami stałymi w stosunku do strony z kontaktami sprężynującymi. Ostateczne ustalenie właściwego skrętu będzie mogło nastąpić dopiero później.

Tak wyglądała sprawa w teorii. W praktyce było niestety inaczej. Jak wynika z wzorów, iloczyny UV, VW, WX, XY, YZ powinny być wszystkie do siebie podobne. Ale tak nie było i wskutek tego było też niemożliwe podpisanie tych iloczynów jednych pod drugimi. I chociaż tę samą operację przeprowadzałem kilkakrotnie na materiałach z coraz innego dnia, gdyż brałem też pod uwagę możliwość, że nastąpiło przesunięcie środkowego bębenka, wynik był zawsze negatywny. Dokonywanie prób zajęło mi bardzo dużo czasu i rozważano już ponowne przerwanie pracy nad Enigmą, gdy wreszcie uświadomiłem sobie, że przyczyną mych niepowodzeń może być tylko błędne założenie odnośnie do połączeń bębenka wstępnego.

Tu mała dygresja: Mam wszelkie podstawy do przekonania, że przez trudności spowodowane połączeniami bębenka wstępnego nie potrafili przebrnąć angielscy kryptolodzy. Bo po pierwsze, gdy w lipcu 1939 roku doszło do spotkania w Polsce przedstawicieli biur szyfrów polskiego, francuskiego i angielskiego, pierwszym pytaniem, jakie postawił angielski kryptolog Dillwyn Knox, było: Jakie są połączenia bębenka wstępnego? A po wtóre, siostrzenica Knoxa, Penelope Fitzgerald, w swej książce *The Knox Brothers* opublikowanej w roku 1978 podaje, że Knox był wściekły, gdy dowiedział się, jakie to było proste.

Jakie więc były połączenia bębenka wstępnego? Okazało się później, że można je znaleźć drogą dedukcyjną, lecz w grudniu 1932 roku lub może w pierwszych dniach roku 1933 otrzymałem połączenia te drogą odgadnięcia. Założyłem mianowicie, że skoro klawisze nie są połączone z kolejnymi kontaktami bębenka wstępnego w kolejności liter na klawiaturze, to może połączone są w kolejności alfabetycznej, czyli że permutacja wywołana przez bębenek wstępny jest identycznością i można jej w ogóle nie uwzględniać.

Tym razem szczęście mi dopisało. Hipoteza okazała się trafna i już pierwsza próba dała wynik pozytywny. Z ołówka mego, jak pod wpływem czarów, zaczęły spływać liczby oznaczające połączenia bębenka *N*. Tak więc połączenia jednego bębenka, bębenka prawego, były wreszcie znane.

Jak znaleziono połączenia pozostałych bębenków? Przypomnę, że dostarczono mi fotokopie kluczy dziennych za okres dwóch miesięcy, za wrzesień i październik 1932 roku. W tym okresie zmiana kolejności bębenków na osi następowała co kwartał, a ponieważ wrzesień i październik należą do dwóch różnych kwartałów, więc miały różną kolejność bębenków, przy czym po prawej stronie znalazły się różne bębenki. W obu kwartałach mogłem zatem zastosować dokładnie taką samą metodę dla znalezienia ich połączeń. Znalezienie połączeń bębenka trzeciego, a zwłaszcza połączeń bębenka odwracającego, nie przedstawiało już większych trudności. Tak samo nie było trudności z ustaleniem właściwego skrętu bocznych ścian bębenków względem siebie, czy też momentów, gdy następuje obrót bębenka lewego i środkowego.

Czynności potrzebne dla ustalenia tych szczegółów polegały w zasadzie na próbach odczytania treści kilku depesz z tego okresu i dokonania takich korekt w bębenkach, by w końcu otrzymać treść całkowicie bezbłędnie. Pewnym ułatwieniem w tej pracy była dostarczona wraz z miesięcznymi tablicami kluczy dziennych niemiecka instrukcja posługiwania się maszyną Enigma, w której jako przykład podano kler pewnej depeszy i jej autentyczny szyfrogram przy określonym kluczu dziennym i kluczu depeszy. W późniejszych wydaniach tej samej instrukcji podany przykład był zawsze fikcyjny.

Skoro okazało się, że, jak już podałem, połączenia bębenka wstępnego można było znaleźć też drogą dedukcyjną, a nie tylko przez odgadnięcie, narzucało się pytanie, czy drogą dedukcyjną, czyli bez pomocy materiału wywiadowczego, nie można by też rozwiązać układu równań (3) i w ten sposób uzyskać połączeń bębenków. Do dziś nie wiadomo, czy układ równań (3) jest rozwiązalny. Znaleziono wprawdzie, przynajmniej w teorii, inną drogę do odtworzenia połączeń bębenków, jednak droga ta jest niedoskonała i uciążliwa. Jej opisanie, nawet pobieżne, spowodowałoby dalsze wydłużenie artykułu. Wspomnę więc tylko, że wymaga posiadania depesz z dwóch dni z tym samym lub zbliżonym nastawieniem bębenków, uzależnia więc znalezienie połączeń bębenków od przypadku, a i potem jeszcze wymaga wielu prób, tak że nie wiadomo, czy kierownictwu Biura Szyfrów starczyłoby cierpliwości zatrudnienia kilku pracowników przez długi okres bez pewności uzyskania wyników, czy też raczej zaleciłoby ponowne zaniechanie pracy nad Enigmą. Wniosek jest więc taki, że dostarczenie materiału wywiadowczego należy uznać za sprawę decydującą o rozwiązaniu maszyny. Szereg lat później dowiedziałem się, że dostarczycielem materiału był wspomniany już kapitan (później generał) Bertrand.

Klucze dzienne. Skoro połączenia bębenków były już znane, przystąpiono do szukania drogi dla odnalezienia trzeciej i ostatniej tajemnicy Enigmy, to znaczy kluczy dziennych. Przedtem jednak w sekcji technicznej Biura Szyfrów przerobiono odpowiednio maszynę handlową, mnie zaś polecono — był to prawdopodobnie początek stycznia 1933 roku — wtajemniczyć mych dwóch kolegów Henryka Zygalskiego i Jerzego Różyckiego, tak by mogli, korzystając z dostarczonych przez wywiad francuski kluczy dziennych na dwa miesiące wrzesień i październik 1932, odczytać materiał szyfrowy za ten okres. Ja sam natomiast miałem nadal pozostać w odosobnieniu aż do całkowitego zakończenia zadania.

Jednak zakończenie to bynajmniej nie było łatwe i nie mogło być łatwe, skoro Niemcy byli przekonani, że szyfru, nawet w przypadku posiadania maszyny, bez znajomości kluczy dziennych rozwiązać nie można. Skoncentrowałem swą uwagę na fakcie, że permutacja S zamienia tylko sześć par liter, a więc 14 liter pozostawia niezmienionych. Przypatrzmy się jeszcze raz układowi równań (3). Wiemy już, że permutacja H jest identycznością, a więc można ją opuścić. Na chwilę przypuśćmy też, że i permutacja S jest tożsamościowa. Jeżeli teraz wszystkie permutacje, z wyjątkiem nieznanej permutacji Q, przeniesiemy na lewą stronę, otrzymamy następujący układ

$$\begin{aligned} PN^{-1}P^{-1}APNP^{-1} &= Q,\\ P^2N^{-1}P^{-2}BP^2NP^{-2} &= Q,\\ &\dots\dots\dots\dots\\ P^6N^{-1}P^{-6}FP^6NP^{-6} &= Q. \end{aligned}$$

Połączenia bębenka N są wprawdzie znane, nieznane jest jednak jego nastawienie. Ażeby to uwzględnić, poprawniej jest napisać:

$$\begin{aligned} P^xN^{-1}P^{-x}AP^xNP^{-x} &= Q,\\ P^{x+1}N^{-1}P^{-x-1}BP^{x+1}NP^{-x-1} &= Q,\\ &\dots\dots\dots\dots\\ P^{x+5}N^{-1}P^{-x-5}FP^{x+5}NP^{-x-5} &= Q. \end{aligned}$$

Gdyby permutacja S rzeczywiście była tożsamościowa, to podstawiając za niewiadomą x kolejno liczby od 1 do 26 i za każdym razem obliczając lewe strony powyższego układu równań, otrzymalibyśmy przy pewnym określonym x to samo na wszystkie wyrażenia Q układu i w ten sposób znaleźlibyśmy nastawienie bębenka N. Permutacja S jednak istnieje, więc dla żadnego x wyrażenia Q nie będą równe między sobą, ale przy pewnym określonym x będą między nimi pewne podobieństwa, ponieważ permutacja S wszystkich liter nie zmienia. Wykonanie wskazanych działań byłoby jednak zbyt pracochłonne. Szukałem metody praktyczniejszej. Znalazłem ją w postaci metody nazwanej przeze mnie *metodą rusztu.*

Wpisuje się dla każdego z trzech bębenków na stałe na arkuszu odpo-

wiedniej wielkości 31 permutacji N, PNP^{-1}, P^2NP^{-2}, ..., $P^{25}NP^{-25}$, N, PNP^{-1}, ..., P^4NP^{-4} z połączeniami trzech bębenków w następującej postaci:

$$\begin{array}{ll} N & k\,j\,p\,z\,y\,d\,t\;\;i\,o\,h\,x\,c\,s\,g\,u\,b\,r\,n\,w\,f\,m\,v\,e\,q\;\;l\;\;a \\ PNP^{-1} & i\;\;o\,y\,x\,c\,s\,h\,n\,g\,w\,b\,r\,f\;\;t\;\;a\,q\,m\,v\,e\;\;l\;\;u\,d\,p\,k\,z\;\;j \\ P^2NP^{-2} & n\;\;x\,w\,b\,r\,g\,m\,f\,v\;\;a\,q\,e\,s\,z\,p\;\;l\;\;u\,d\,k\;\;t\;\;c\,o\,j\;\;y\;\;i\;\;h \\ \ldots\ldots & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ P^4NP^{-4} & u\,z\,p\,e\,k\,d\;\;t\;\;y\,o\,c\,q\,x\,n\,j\,s\,b\;\;i\;\;r\,a\,m\,h\,w\,g\,f\;\;l\;\;v, \end{array}$$

a na innej kartce z sześcioma otworami, nazwanej przeze mnie „rusztem" wypisuje się — poznane wcześniej — permutacje od A do F w następującej postaci:

$$\begin{array}{ll} A & \begin{pmatrix} a\,b\,c\,d\,e\,f\,g\,h\,i\,j\,k\,l\,m\,n\,o\,p\,q\,r\,s\,t\,u\,v\,w\,x\,y\,z \\ s\,r\,w\,i\,v\,h\,n\,f\,d\,o\,l\,k\,y\,g\,j\;\;t\,x\,b\,a\,p\,z\,e\,c\,q\,m\,u \end{pmatrix} \\ \ldots\ldots & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ F & \begin{pmatrix} a\,b\,c\,d\,e\,f\,g\,h\,i\,j\,k\,l\,m\,n\,o\,p\,q\,r\,s\,t\,u\,v\,w\,x\,y\,z \\ w\,x\,o\,f\,k\,d\,u\,i\,h\,z\,e\,v\,q\,s\,c\,y\,m\,t\,n\,r\,g\,l\,a\,b\,p\,j \end{pmatrix}. \end{array}$$

Następnie przesuwa się ruszt po kartce z połączeniami bębenka N tak długo, aż trafi się na pozycję, w której odnajdzie się pewne podobieństwa między poszczególnymi wyrażeniami Q. W tej pozycji należy litery górne i dolne we wszystkich permutacjach od A do F poprzestawiać tak, aby wszystkie permutacje Q stały się takie same. W ten sposób znajdzie się jednocześnie nastawienie bębenka N i zmiany spowodowane przez permutację S. Praca ta wymaga znacznego skupienia uwagi, gdyż podobieństwa, o których wspominałem, nie zawsze wyraźnie się uwydatniają i można je bardzo łatwo przeoczyć.

Zadanie jednak wciąż jeszcze nie jest ukończone. Pozostaje bowiem niewiadoma Q. Lecz Q — jak pamiętamy — to tylko skrót (2), oznaczający fikcyjny bębenek odwracający. Obecnie znane już są połączenia bębenków M, L, R. Jednak nie znane są jeszcze pozycje bębenków M i L, gdyż tylko bębenek R jest nieruchomy. Poprawniej więc byłoby napisać

$$Q = P^y M P^{-y} P^z L P^{-z} R P^z L^{-1} P^{-z} P^y M P^{-y}, \tag{4}$$

gdzie niewiadome y i z, podobnie jak poprzednio niewiadoma x, mogą przyjmować wszystkie wartości od 1 do 26. Jedyny sposób, który w tym czasie (początek roku 1933) mogłem zastosować dla znalezienia y i z, polegał na codziennym przerabianiu wprost na maszynie wszystkich możliwych $26^2 = 676$ pozycji bębenków M i L, dopóki nie trafiłem na ich właściwą pozycję. Była to praca dość nużąca, raczej mechaniczna, ale jeszcze nie ostatnia.

Należy bowiem przypomnieć o jeszcze jednym szczególe budowy maszyn Enigma, o którym już wzmiankowałem przy opisie maszyny; na obwodzie

bębenków szyfrujących L, M, N umieszczone były przesuwalne pierścienie z wygrawerowanymi na nich literami alfabetu. W jaki sposób owe pierścienie codziennie należało nastawić, podawano szyfrantom na dostarczanych tabelach miesięcznych razem z pozostałymi składnikami kluczy dziennych. Należało więc jeszcze znaleźć nastawienie pierścieni.

Z odczytanych w międzyczasie depesz za miesiąc wrzesień i październik 1932 roku dowiedziałem się, że w zasadzie wszystkie depesze, nie biorąc oczywiście pod uwagę dalszych części depesz dwu- i więcej częściowych, rozpoczynały się od liter ANX od słowa „an" (niem. „do") i „x" odzielającego słowa. Należało wybrać odpowiednią depeszę, zaczynającą się na przykład od liter *tuv* i stale przyciskając klawisz *t* obracać bębenkami i jednocześnie obserwować, kiedy zapali się lampka A. Wówczas trzeba nacisnąć klawisz *u* i w przypadku, gdy zapali się lampka N, nacisnąć jeszcze klawisz *v*. Jeżeli zapali się lampka X, jest duże prawdopodobieństwo, że znaleźliśmy dobry przypadek i wówczas trzeba nastawić odpowiednio pierścienie. Jeżeli nie, trzeba dalej szukać, aż do skutku.

Metoda ta była bardzo prymitywna i daleko bardziej nużąca niż metoda znajdowania pozycji bębenków L i M, gdyż w wypadku skrajnie niekorzystnym należało przejść wszystkie możliwe pozycje bębenków, których, jak wiadomo, jest $26^3 = 17576$, była jednak skuteczna.

Tak więc rezultat pracy osiągnięty w ciągu zaledwie kilku miesięcy można tak streścić:

1) odtworzono niemiecką wojskową maszynę Enigma,
2) znaleziono metodę codziennego odtwarzania kluczy depesz,
3) znaleziono metodę odtwarzania kluczy dziennych.

Okres względnego spokoju (1933–1935). Pierwszą decyzją, jaką podjęli moi przełożeni, gdy zakomunikowałem im moje wyniki, było wydanie polecenia fabryce AVA, będącej pod kontrolą Biura Szyfrów, a wytwarzającej stacje radiowe nadawczo-odbiorcze, by zbudowała serię sobowtórów niemieckich Enigm wojskowych według modelu handlowego z połączeniami bębenków przeze mnie dostarczonymi i z uwzględnieniem innych różnic w budowie obu typów maszyn, przede wszystkim przez dodanie łącznicy. Następnie, zaangażowano do pracy i umieszczono w oddzielnym pokoju pięciu czy sześciu młodych ludzi, z wyłącznym zadaniem deszyfrowywania potoku depesz, do których klucze dzienne zaczęto niebawem dostarczać. I wreszcie zarządzono, by moi dwaj koledzy Zygalski i Różycki znów, i odtąd już na stałe, ze mną pracowali.

Było nas więc teraz trzech zamiast jednego. Metodami dopiero co opisanymi odnajdowaliśmy dzień po dniu klucze dzienne, by je dostarczać deszyfrantom. Ponieważ przez kolejne trzy lata do końca 1935 roku Niemcy żadnych istotniejszych zmian w szyfrze Enigma nie wprowadzili, mogliśmy też nieco czasu poświęcić dla ulepszenia naszych metod dekryptażu.



Rys. 5. W ogrodach zamku Les Fouzes na południu Francji, w 1941 r.
Od lewej: Henryk Zygalski, Jerzy Różycki, Marian Rejewski

I tak, na przykład, sporządziliśmy dla sześciu możliwych układów bębenków I, II, I, III, II, I, II, III, III, I, III, II katalog wszystkich możliwych permutacji Q według wzoru (4). Obejmował w sumie $6 \cdot 26^2 = 4056$ pozycji. Gdy był gotowy, wystarczyło – jeżeli, stosując metodę rusztu, odnaleźliśmy nastawienie bębenka N – odszukać otrzymaną jednocześnie permutację Q w katalogu, by w jednej chwili już mieć nastawienie bębenków L i M.

Albo inne usprawnienie: Gdy dla odnalezienia nastawienia pierścieni stosując metodę ANX przekręcaliśmy na maszynie kolejno wszystkie możliwe $26^3 = 17576$ pozycji bębenków, zauważyliśmy wnet, że jeżeli treść którejś z depesz miała rozpoczynać się na ANX, to tym samym już kilka pozycji bębenka N odpadało jako niemożliwe. A ponieważ depesz, w których można było spodziewać się liter ANX na początku, było codziennie kilkanaście, przeto najczęściej można było drogą czysto rachunkową odrzucić, jako niemożliwe, wszystkie pozycje bębenka N z wyjątkiem jednej lub może dwóch. Jednak obecnie już nie pamiętam, jakie obliczenia należało przeprowadzić i na jakich podstawach teoretycznych się opierały.

W tym też okresie kol. Różycki opracował metodę, którą nazwał *metodą zegara* i która w wielu wypadkach pozwalała określić, który z trzech bębenków I, II, III był w danym dniu bębenkiem *N*, to znaczy znajdował się w maszynie po prawej stronie. Wprawdzie do końca roku 1935 kolejność bębenków zmieniała się raz na kwartał, więc określenie bębenka *N* nie było jeszcze sprawą zbyt istotną, ale już od 1 lutego 1936 roku zmiana kolejności bębenków następowała co miesiąc, a od 1 października 1936 roku codziennie. Na czym owa metoda polegała?

Jeżeli podpiszemy pod sobą, litera pod literą, dwa teksty w języku niemieckim, na przykład

WEMGOTTWILLRECHTEGUNSTERWE
UEBIMMERTREUUNDREDLICHKEIT

to w obrębie 26 liter znajdą się przeciętnie dwie kolumienki z jednakowymi literami i ta właściwość będzie zachowana również wówczas, gdy oba teksty zaszyfrujemy tym samym kluczem. Jeżeli natomiast każdy tekst zaszyfrujemy innym kluczem szyfru maszynowego, to w obrębie 26 liter znajdzie się przeciętnie tylko jedna kolumienka z jednakowymi literami. Przyczyna tego zjawiska tkwi oczywiście w nierównej częstości występowania liter w języku niemieckim (tak samo zresztą jak i w innych językach). W obrębie 26 liter zjawisko to nie występuje w sposób dostrzegalny, gdy jednak mamy dwie depesze długości na przykład 260 liter każda, to na ogół tą metodą można orzec, czy obie zostały zaszyfrowane tym samym kluczem, czy kluczami różnymi. Z tej możliwości korzystamy w sposób następujący:

Dysponując dostateczną ilością materiału szyfrowego znajdujemy zwykle po kilkanaście par depesz takich, że w każdej parze dwie pierwsze litery kluczy są równe, a różnią się jedynie trzecie litery kluczy. Podpisujemy teraz obie depesze jednej pary tak pod sobą, ażeby litery zaszyfrowane przy tym samym nastawieniu bębenków znalazły się pod sobą. *A priori* są jednak możliwe dwa sposoby podpisania depesz pod sobą, w zależności od tego, przy której pozycji bębenka *N* nastąpi przesunięcie bębenka środkowego, czyli *M*. Te pozycje są znane i są inne dla każdego z trzech bębenków. Gdy na przykład na miejscu *N* znajduje się bębenek I, wówczas przesunięcie bębenka *M* nastąpi, gdy w okienku bębenka *N* przesunie się litera Q na R. Jeżeli na miejscu *N* znajduje się bębenek II, wówczas przesunięcie nastąpi przy zmianie litery E na F, a jeżeli bębenkiem *N* jest bębenek III, wówczas przesunięcie nastąpi przy zmianie litery V na W. Wystarczy przy każdym z obu możliwych sposobów podpisania pod sobą depesz policzyć liczbę kolumienek z jednakowymi literami, aby dowiedzieć się, który ze sposobów podpisania depesz jest właściwy, a tym samym stwierdzić, który z trzech bębenków znajduje się po prawej stronie.

Metoda zegara Różyckiego, która w wielu wypadkach ułatwiała nam pracę, miała również tę ciekawą własność, że wśród wynalezionych przez

nas metod była jedyną opierającą się na cechach językowych, a mianowicie na właściwej językowi niemieckiemu częstotliwości występowania liter. Na ogół bowiem, jak już wspomniałem, wprowadzenie maszyn szyfrowych wpłynęło na zmianę charakteru pracy kryptologów od dociekań lingwistycznych w kierunku matematycznych.

Okres wzmożonych zmian (1936 – VIII 1938). Wzrastająca potęga militarna Niemiec powodowała rozszerzenie się kręgu użytkowników maszyn Enigma. Lotnictwo niemieckie nawet już nieco wcześniej, bo z dniem 1 sierpnia 1935, utworzyło własną sieć łączności radiowej z własnymi kluczami dziennymi, ale oczywiście posługując się tą samą Enigmą. Stopniowo dołączały inne formacje militarne i paramilitarne, a ponieważ też tworzyły oddzielne sieci, musieliśmy coraz więcej kluczy dziennych odtwarzać. O coraz częstszej zmianie kolejności bębenków już wspominałem. Ale z dniem 1 października 1936 roku zwiększono i zmodyfikowano liczbę zmienianych par liter na łącznicy z sześciu na 5 do 8, co utrudniło posługiwanie się metodą rusztu. Szukaliśmy więc innych metod.

Zwróciliśmy uwagę na charakterystyki, które miały kształt rzadko się powtarzający, a zatem w pewnym stopniu określający dany dzień. Z wzoru

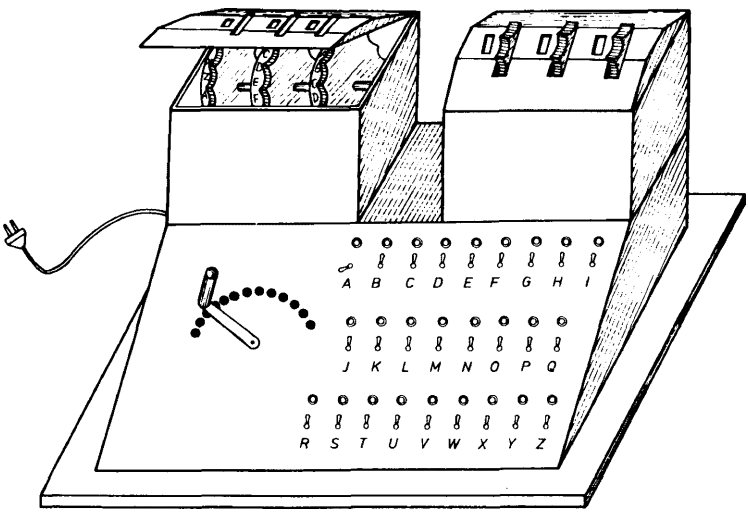
$$AD = SPNP^{-1}QPN^{-1}P^{3}NP^{-4}QP^{4}N^{-1}P^{-4}S^{-1}$$

i dwóch analogicznych dla BE i CF wynikało, że permutacja S jako przekształcająca nie wpływa na długość cykli w charakterystyce, a jedynie na litery wewnątrz cykli. Gdyby więc udało się wymyślić przyrząd podający długość cykli dla każdego z wyrażeń typu AD (a tych wyrażeń nie jest znów tak bardzo dużo, bo dla każdej z 6 możliwych kolejności bębenków tylko $26^3 = 17576$), wówczas moglibyśmy utworzyć kartotekę długości cykli wyrażeń typu AD i przez porównanie z charakterystyką danego dnia określić nastawienie bębenków. Taki przyrząd, i to niezwykle prosty, udało się nam rzeczywiście wymyślić (rys. 6). Nazwaliśmy go *cyklometrem*, a wykonała go fabryka AVA, ta sama, która wcześniej już zbudowała sobowtóry wojskowych Enigm.

Cyklometr składał się w swej istocie z dwóch zestawów bębenków (przy czym bębenek N drugiego zestawu był o trzy litery przesunięty w stosunku do bębenka N pierwszego zestawu), z płyty ebonitowej z umieszczonymi na niej 26 żarówkami od lampek kieszonkowych i przełącznikami przy każdej żarówce oraz ze źródła prądu. Gdy przy którejś z żarówek włączono prąd przez zmianę przełącznika, wówczas zapalała się nie tylko dana żarówka, lecz wszystkie żarówki, które należały do tego samego cyklu i do drugiego cyklu tej samej pary. Należało jeszcze odnotować na kartce papieru pozycję bębenków i liczbę zapalających się żarówek, a same kartki w określony sposób, na przykład według długości cykli, uporządkować.

Praca trwała długo, ponad rok, gdyż wykonywaliśmy ją obok naszych

normalnych zajęć odtwarzania kluczy dziennych za pomocą rusztu. Gdy jednak wszystkie sześć kartotek było gotowych, uzyskanie klucza dziennego było zazwyczaj sprawą zaledwie kilkunastu minut. Z karteczki odczytywano



Rys. 6. Cyklometr

pozycję bębenków, z pudełka, z którego karteczkę wyjęto, kolejność bębenków, a permutację S otrzymywano, porównując litery w cyklach charakterystyki z literami w cyklach permutacji AD, BE, CF, które otrzymywano przez wystukanie na maszynie.

Niestety, 2 listopada 1937 roku, gdy kartoteka była gotowa, Niemcy wymienili dotychczasowy bębenek odwracający oznaczony przez nich literą A na bębenek inny, B, wobec czego całą pracę musieliśmy wykonać ponownie, oczywiście po uprzednim odtworzeniu połączeń bębenka B.

We wrześniu 1937 roku, a więc na kilka miesięcy przed zmianą bębenków odwracających, pojawiła się w eterze nowa sieć. Jak się wkrótce okazało, była to sieć partyjnej służby bezpieczeństwa, czyli tak zwanego „Sicherheitsdienst", w skrócie SD. Ze względu na rolę, jaką odczytanie przez nas tej sieci odegrało kilkanaście miesięcy później w dalszych pracach nad Enigmą, chcę jej poświęcić kilka słów.

Sposób szyfrowania przez SD w zasadzie nie różnił się od sposobu stosowanego w innych sieciach. Gdy po raz pierwszy utworzono charakterystykę któregoś dnia tej sieci, znaleziono ją bez trudu w naszej kartotece. Ustalono więc kolejność i pozycję bębenków oraz permutację S, gdy jednak próbowano metodą ANX ustalić nastawienie pierścieni, napotkano trudności. Najwidoczniej w żadnej z branych pod uwagę depesz początek nie brzmiał ANX. Wybrano więc ze środka jednej z depesz jakiś fragment i zaczęto go wystukiwać na maszynie przy wszelkich możliwych pozycjach bębenków, w nadziei otrzymania w ten sposób fragmentu treści. I rzeczy-

wiście, szczęśliwym trafem otrzymano, po stosunkowo niedługim czasie, litery „ein". Mógł to być fragment treści, ale mogło to też być zupełnie przypadkowe pojawienie się takich właśnie liter. Gdy przy tej pozycji bębenków wystukano całość depeszy, żadnego dalszego fragmentu w języku niemieckim nie znaleziono.

Po dokładniejszej jednak analizie tego pozornie bezsensowego zbioru liter okazało się, że można z niego wyłowić pewne powtórzenia liter, że powtórzenia te tworzą grupy czteroliterowe i że odstęp między nimi wynosi wielokrotność czterech, jednym słowem, że można całą depeszę podzielić (pomijając owo słowo „ein") na czteroliterowe grupy kodowe. Mieliśmy więc tutaj do czynienia z tak zwanym podwójnym zaszyfrowaniem. Naprzód nadawca depeszy, zapewne oficer, zaszyfrowywał treść depeszy za pomocą książki kodowej na czteroliterowe grupy kodowe, słowa „ein" zaś użył tylko dlatego, że nie znalazł tego słowa w książce kodowej, a dopiero potem przekazał tak spreparowaną treść szyfrantowi do dalszego zaszyfrowania na maszynie.

Właśnie dzięki takiemu potknięciu, tzn. mieszaniu kleru z kodem, no i łutowi szczęścia, stało się możliwe odtworzenie całego klucza dziennego wraz z nastawieniem pierścieni. Kod okazał się na szczęście też nietrudny do rozwiązania, choć oczywiście nigdy w takich przypadkach nie można odtworzyć książki kodowej w $100^0/_0$, gdyż nigdy wszystkie grupy kodowe nie pojawiają się w depeszach.

Na początku roku 1938 szef naszego wydziału wywiadowczego, płk Stefan Mayer, zarządził przeprowadzenie przez okres dwutygodniowy statystyki rozwiązanego materiału w porównaniu z materiałem zaszyfrowanym Enigmą odebranym przez radiotelegrafistów. Okazało się, że stosunek wynosi $75^0/_0$. Peter Calvocoressi, były pracownik angielskiego Biura Szyfrów, w pogadance nadanej w angielskim Radio dnia 18 stycznia 1977 roku, [3], stwierdził, że takich rezultatów nikt inny na świecie nie osiągnął. Miał oczywiście na myśli czasy późniejsze, bo w roku 1938 poza Polakami nikt jeszcze żadnych depesz zaszyfrowanych niemiecką Enigmą wojskową nie czytał. Zresztą owe $75^0/_0$ odczytanych depesz też nie stanowiło kresu naszych możliwości. Przy nieznacznie zwiększonym personelu moglibyśmy byli dojść do około $90^0/_0$ odczytanych depesz. Ale pewna ilość materiału szyfrowego, czy to z powodu błędnego nadania, czy z powodu błędnego odbioru, czy z różnych innych przyczyn pozostaje w takich wypadkach zawsze nie odczytana.

Zmiany największe (wrzesień 1938 – wrzesień 1939). Z dniem 15 września 1938 roku Niemcy, nic nie zmieniając w samej maszynie ani nic do niej nie dodając, zmienili sposób podawania kluczy depesz. Od tej daty począwszy, szyfrant obowiązany był obrać sobie trzy dowolne litery, które bez zaszyfrowania umieszczał w nagłówku depeszy. Potem nastawiał bębenki na owe litery, wybierał trzy inne litery jako klucz depesz i te, tak jak przedtem,

po dwukrotnym zaszyfrowaniu, umieszczał na początku depeszy, a następnie nastawiał bębenki na klucz depeszy i rozpoczynał właściwe szyfrowanie samej depeszy.

Zmianę przekazywania kluczy depesz wprowadzono we wszystkich formacjach wojskowych, lecz nie wprowadzono jej w sieci SD. Cały nasz dotychczasowy dorobek odtwarzania kluczy dziennych i kluczy depesz, a więc metoda kartoteki i metoda rusztu w odniesieniu do formacji wojskowych odpadły, gdyż nie było już charakterystyk. Jedynie sieć SD mogliśmy rozwiązywać i odczytywać tak jak do tej pory.

Jednak w ciągu bardzo krótkiego czasu, może tygodnia, może dwóch, mieliśmy dwa pomysły, a raczej, bo to ważniejsze, znaleźliśmy drogi ich zrealizowania. Spróbuję naszkicować i pomysły i wykonanie.

Tak jak przy dawnym sposobie przekazywania klucza podawaliśmy go w postaci dwóch grup trzyliterowych, tak teraz musieliśmy go podawać w postaci trzech grup, na przykład

SHP, CHV PZT,

przy czym pierwsza grupa, oddzielona przecinkiem od pozostałych, jest niezaszyfrowana, a dwie dalsze stanowią klucz depeszy dwukrotnie zaszyfrowany. Przy dostatecznie obfitym materiale szyfrowym może się zdarzyć, że w danym dniu znajdą się trzy depesze o takich na przykład kluczach:

RTJ, WAH WIK
HPL, RAW KTW
DQX, DWJ MWR,

w których pierwsza i czwarta lub druga i piąta, lub trzecia i szósta litera w kluczach wszystkich trzech depesz jest ta sama, w tym przykładzie jest nią litera W, ale może być też zupełnie inna litera, byleby była ta sama we wszystkich trzech depeszach. Załóżmy na chwilę, że permutacja S jest tożsamościowa. Gdyby również nie istniało nastawienie pierścieni i gdybyśmy jeszcze znali kolejność bębenków na osi, wówczas wystarczyłoby nastawić bębenki na pozycję RTJ, a wtedy naciśnięcie klawisza W spowodowałoby zapalenie się jednej i tej samej lampki w odstępie trzech uderzeń. To samo stałoby się w pozycji HPN i w pozycji DQY bębenków. Nastawienie pierścieni powoduje, że pozycje bębenków, przy których to się stanie, są nam nie znane, jednak różnice w pozycjach będą zachowane, są nam więc znane.

Wystarczy zatem skonstruować urządzenie, które by w zasadzie składało się z zestawów bębenków sześciu Enigm i które – zachowując znaną nam wzajemną różnicę pozycji bębenków – synchronicznie obracałoby te bębenki i po przejściu w ten sposób w określonym czasie około 2 godzin wszystkich możliwych $26^3 = 17576$ pozycji zasygnalizowało, kiedy warunek zapalenia się trzech par lampek (w każdej parze te same) byłby spełniony.

Nie znana jest jednak kolejność bębenków, więc najlepiej byłoby zbudować od razu sześć takich urządzeń, po jednym dla każdej możliwej kolejności. No tak, ale istnieje przecież permutacja *S*. Lecz w tym okresie permutacja *S* składała się z 5–8 transpozycji, czyli przeciętnie zamieniała połowę liter, można było się zatem spodziewać, że litera powtarzająca się w trzech depeszach sześciokrotnie (w podanym przykładzie litera W) choć co drugi raz przez permutację *S* nie będzie zmieniona.

Podałem wówczas zasadę działania, a wspomniana już fabryka AVA zbudowała w niewiarygodnie krótkim czasie – bo już w listopadzie 1938 roku – sześć takich urządzeń, z braku lepszego pomysłu zwanych przez nas *bombami*. Było to niewątpliwie zasługą dyrektora fabryki, inż. Antoniego Pallutha, który nie był wprawdzie etatowym pracownikiem Biura Szyfrów, lecz ściśle z nim współpracował i – sam będąc kryptologiem – miał wielkie zrozumienie dla potrzeb Biura.

Drugi pomysł, który zrodził się niemal jednocześnie z pomysłem bomb, był oparty na pozornie podobnych, w rzeczywistości zupełnie innych założeniach. Podobnie jak w przypadku bomb musieliśmy rozporządzać wystarczająco obfitym materiałem szyfrowym. Mogliśmy wówczas spodziewać się wśród tego materiału około dziesięciu depesz z takimi na przykład kluczami

KTL, WOC DRC	GRA, FDR YDP
SVW, DKR IKC	MDO, CTW YZW
BWK, TCL TSD	AGH, SLM PZM
EDV, PRS ZRT	JBR, LPS TOS
GRN, UTS UQA	ITY, APO ZPD

to znaczy takimi, w których bądź pierwsze litery są równe czwartym, bądź drugie piątym, bądź trzecie szóstym, lecz w których pary jednakowych liter w każdym kluczu mogą być inne. Jeżeli przypomnimy sobie charakterystykę (1), to uprzytomnimy sobie też, że identyczne litery na odpowiednich miejscach w kluczu oznaczają cykle jednoliterowe w charakterystyce. Ale permutacja *S* nie wpływa przecież na długość cykli w charakterystyce, więc również nie wpływa na fakt występowania lub niewystępowania cykli pojednyczych.

Należałoby więc stworzyć – zamiast kartoteki długości cykli we wszystkich iloczynach typu *AD* – kartotekę pozycji tych wszystkich iloczynów typu *AD*, w których występują cykle jednoliterowe i potem porównywać z cyklami jednoliterowymi występującymi w kluczach depesz danego dnia. Ale jak przeprowadzić to porównanie? Bo i tutaj, tak jak w pomyśle poprzednim, znane są tylko odległości względne cykli jednoliterowych uwidocznionych w kluczach depesz danego dnia. I tu właśnie kol. Zygalski wskazał sposób przeprowadzenia porównania:

Dla każdej z 26 możliwych pozycji bębenka *L* narysowano na dość dużych, bo wielkości około 60×60 cm, arkuszach papieru oznaczonych

kolejnymi literami alfabetu kwadrat podzielony na 51×51 mniejszych poletek. Po bokach, na górze i u dołu każdego kwadratu, umieszczono litery od *a* do *z* i jeszcze raz od *a* do *y*. Był to niejako układ współrzędnych, w którym odcięte i rzędne oznaczały kolejne możliwe pozycje bębenków *M* i *N*, a każde poletko — odpowiadające tym pozycjom permutacje z cyklami jednoliterowymi lub bez cykli jednoliterowych. Przypadki z cyklami jednoliterowymi perforowano.

Praca była ogromna, tym bardziej, że przypadki z cyklami jednoliterowymi należało perforować czterokrotnie. Gdy te arkusze, według ściśle określonego programu, w odpowiedniej kolejności i odpowiednio względem siebie przesunięte, nakładano na siebie, wówczas liczba przeświecających otworów stopniowo się zmniejszała, a jeżeli dysponowano dostateczną liczbą kluczy z cyklami jednoliterowymi, pozostawał w końcu jeden otwór przeświecający przez wszystkie arkusze, odpowiadający prawdopodobnie dobremu przypadkowi.

Z kompletu, do którego arkusze należały, dowiadywano się o kolejności bębenków. Z pozycji otworu i litery arkusza można było wyliczyć nastawienie pierścieni, a przez porównanie liter kluczy z literami w maszynie również permutację *S*, czyli cały klucz dzienny. Ale, jak już wspomniałem, praca była ogromna, gdyż w każdym arkuszu należało wyciąć około tysiąca otworów, każdy komplet obejmował 26 arkuszy, a kompletów należało wykonać sześć. Toteż, ponieważ pracę tę wykonywaliśmy obok naszych normalnych zajęć, zdołaliśmy wykonać do dnia 15 grudnia 1938 roku tylko dwa komplety.

Tymczasem dnia tego Niemcy dokonali nowej zmiany w szyfrze Enigma, dodając we wszystkich formacjach łącznie z formacją SD do dotychczasowych trzech bębenków dwa dalsze, bębenek IV i V. Na osi nadal pozostawały trzy bębenki, jednak do wyboru były teraz trzy spośród pięciu bębenków, czyli zamiast sześciu możliwych kolejności było ich teraz 60. Ale pomijając nawet dziesięciokrotne zwiększenie liczby możliwych kolejności bębenków, nie znane przede wszystkim były połączenia tych bębenków. W jaki sposób je otrzymać? Przy nowym systemie szyfrowania już nie było charakterystyk, cyklometr, kartoteki były bezużyteczne. Na szczęście mieliśmy sieć SD, która, choć bębenki IV i V u siebie wprowadziła, pozostała przy dawnym systemie szyfrowania kluczy. Stosując metodę rusztu szukaliśmy i znaleźliśmy taki dzień, w którym bębenkiem *N* był jeden z dotychczasowych, a więc znanych bębenków. Potem zakładaliśmy, że spośród bębenków *L* i *M* jeden należał do znanych, a drugi do nie znanych i połączenia tego ostatniego znaleźliśmy w ten sam sposób, w jaki w roku 1932 znalazłem połączenia trzeciego, wówczas jeszcze nie znanego bębenka.

Tak więc byliśmy w posiadaniu połączeń wszystkich 5 bębenków i depesze należące do sieci SD nadal mogliśmy czytać. Jednak łatwe to nie było, bo chociaż dzięki metodzie zegara Różyckiego niekiedy wiedzieliśmy, który

bębenek znajduje się na miejscu N, to i tak metoda rusztu, jedyna, którą teraz do sieci SD mogliśmy stosować, niekiedy zawodziła, ponieważ z dniem 1 stycznia 1939 roku Niemcy ponownie zwiększyli liczbę liter zmienianych przez permutację S od 7 do 10 par. Faktem jednak jest, że depesze sieci SD czytaliśmy i nie miał racji wspomniany już Calvocoressi, że w tym czasie nikt nie świecie depesz zaszyfrowanych Enigmą o pięciu bębenkach nie mógł odczytać.

Inaczej przedstawiała się sprawa z czytaniem depesz formacji wojskowych. Chociaż znaliśmy dzięki sieci SD połączenia bębenków IV i V, to należało te bębenki zastosować do naszych bomb i do naszych arkuszy perforowanych. Fabryka AVA dostarczyła wprawdzie niewielką ilość bębenków IV i V do maszyn, którymi deszyfranci czytali depesze sieci SD, ale do bomb potrzebnych było po 36 bębenków IV i V, a praca przy bombach powinna trwać 24 godziny na dobę, więc należało by też zaangażować dodatkowo kilku operatorów.

A jeżeli chodzi o arkusze perforowane, to do naszych dwóch kompletów należałoby dorobić jeszcze 58 dalszych. Wypracowaliśmy wprawdzie metody, za pomocą których w pewnych wypadkach udawało się z wielkim prawdopodobieństwem ustalić, który bębenek znajduje się na miejscu N, niemniej jednak wszystkie komplety arkuszy były potrzebne. Sytuacja wyglądała więc w ten sposób, że pomijając sieć SD, depesze wojskowe czytaliśmy tylko wtedy, gdy w maszynie na osi znajdowały się przypadkowo tylko trzy pierwotne bębenki, co zdarzało się średnio jeden raz na dziesięć. Wprowadzenie zatem IV i V bębenka oznaczało tylko zmiany ilościowe, nie jakościowe w naszej pracy. Ale gdy z dniem 1 lipca 1939 roku także sieć SD przeszła na nowy sposób przekazywania kluczy depesz, metoda rusztu i tu przestała być aktualna.

Zakończenie. Tak przedstawiała się sytuacja, gdy w dniach 25 i 26 lipca 1939 roku zwołano z inicjatywy polskiej do Warszawy spotkanie przedstawicieli trzech wywiadów: angielskiego, francuskiego i polskiego.

Na spotkaniu tym powiedzieliśmy wszystko, co sami wiedzieliśmy, i pokazaliśmy wszystko, co mieliśmy do pokazania. Dwie Enigmy z pięcioma bębenkami, u nas wyprodukowane, dostarczyliśmy majorowi (później generałowi) Bertrandowi, który zobowiązał się, że jedną z tych maszyn przekaże potem Anglikom, co też uczynił. Od naszych gości nie dowiedzieliśmy się niczego. Ani Anglicy, ani Francuzi nie zdołali pokonać pierwszych trudności, nie mieli połączeń bębenków, nie mieli żadnych metod.

Spotkanie to miało jednak bardzo daleko idące skutki, bo gdy wkrótce potem Niemcy bez wypowiedzenia wojny wkroczyli do Polski i Sztab Główny, a z nim Biuro Szyfrów, ratowały się ucieczką do Rumunii, mjr Bertrand 15 pracowników tegoż Biura, w tym szefa i jego zastępcę oraz moich dwóch kolegów i mnie ściągnął do Francji, gdzie w zamku Vignolles,

odległym około 40 km od Paryża, stworzył nam warsztat pracy. Ale jak tu pracować, skoro wszystkie materiały, urządzenia, maszyny (z wyjątkiem dwóch Enigm przewiezionych przez granicę w samochodzie ppłk. Langera) jeszcze na terenie Polski bardzo starannie zniszczono, by żaden ślad naszej pracy nie wpadł w ręce niemieckie? Wtedy to przysłali nam Anglicy pełen zestaw 60 kompletów po 26 arkuszy perforowanych Zygalskiego.

Wykonanie tej olbrzymiej pracy w stosunkowo krótkim czasie nie było dla Brytyjczyków niczym nadzwyczajnym. Dysponowali przecież olbrzymimi zasobami ludzkimi. W Bletchley, miejscowości położonej około 60 km na północ od Londynu, w której wówczas mieściło się angielskie biuro szyfrów, już na samym początku wojny zatrudnionych było 60 kryptologów, później zaś daleko więcej. Nic więc dziwnego, że gdy korzystając z arkuszy perforowanych zaczęliśmy odtwarzać klucze dzienne i wzajemnie je sobie poprzez Kanał przesyłać, na każde 100 odnalezionych kluczy 83 pochodziło od Brytyjczyków, a tylko 17 od nas Polaków.

Gdy w czerwcu 1940 roku Francuzi podpisali zawieszenie broni z Niemcami, mjr Bertrand zorganizował nam ucieczkę do Algerii, a gdy w jesieni tego samego roku znów powróciliśmy do nieokupowanej strefy Francji, by działać konspiracyjnie pod kierunkiem mjra Bertranda, stwierdziliśmy, że Niemcy w międzyczasie ponownie zmienili sposób przekazywania kluczy depesz, wskutek czego również arkusze Zygalskiego stały się bezużyteczne. Zajmowaliśmy się rozwiązywaniem innych szyfrów, ale już nie Enigmą. Bo, jak słusznie stwierdził wzmiankowany już Calvocoressi, żeby ten rodzaj szyfru złamać, dwie rzeczy są potrzebne: matematyczna teoria i pomoc mechaniczna. A w miarę jak Niemcy doskonalili sposoby przekazywania depesz, pomoc mechaniczna konieczna dla złamania szyfru stawała się coraz bardziej skomplikowana i coraz kosztowniejsza. Równolegle wzrastała też ilość materiału podsłuchowego potrzebna dla uporania się z szyfrem. Tymczasem w warunkach, w jakich we Francji, w strefie wprawdzie nieokupowanej, jednak przez Niemców kontrolowanej, wówczas przebywaliśmy, materiału podsłuchowego otrzymywaliśmy niedużo, a o wykoncypowaniu, a tym bardziej zbudowaniu skomplikowanych i kosztownych maszyn, jakie wówczas byłyby potrzebne, nawet marzyć nie mogliśmy. Anglicy w Bletchley już w 1940 roku przerobili polskie „bomby" z 1938 roku odpowiednio do zmienionych potrzeb, zachowując nazwę „bombs" i ich charakter elektromechaniczny. Potem budowali dla potrzeb łamania szyfru Enigma maszyny coraz to bardziej skomplikowane, aż wreszcie jedna z nich, która weszła w użycie na sam koniec 1943 roku, była – jak Calvocoressiego zapewniono – pierwszym zbudowanym na świecie autentycznym elektronicznym komputerem.

Gdy 8 listopada 1942 roku alianci wylądowali w Afryce Północnej i Niemcy w odwecie wkroczyli do strefy nieokupowanej Francji, mjr Bertrand pospiesznie wyewakuował nas wszystkich nad Lazurowe Wybrzeże, by tam zorganizować nasz przerzut małymi partiami przez Pireneje do Hiszpanii

i dalej do Wielkiej Brytanii. Jednak przeprawa ta nie okazała się szczęśliwa. Przy przejściu przez granicę hiszpańską z osób wymienionych w niniejszym opracowaniu wpadli w ręce niemieckie ppłk Langer, mjr Ciężki i inż. Palluth. Inż. Palluth zginął 19 IV 1944 roku w obozie pracy, ugodzony odłamkiem bomby alianckiej zrzuconej w czasie nalotu na ten obóz. Ppłk Langer i mjr Ciężki zostali umieszczeni w obozach jenieckich, z których dopiero w maju 1945 roku uwolnieni zostali przez aliantów. Jerzy Różycki zginął już wcześniej, 9 stycznia 1942 roku, wskutek rozbicia się statku, na którym się znajdował w czasie przeprawy przez Morze Śródziemne. Tak więc do Wielkiej Brytanii dotarli tylko Henryk Zygalski i ja. Tutaj, wcieleni do polskich jednostek wojskowych, zajmowaliśmy się jeszcze przez pewien czas rozwiązywaniem niemieckich szyfrów (lecz nie szyfrem Enigma), dopóki na mocy odpowiednich porozumień radziecko-brytyjskich komórka nasza nie uległa likwidacji.

Bibliografia

[1] Gustave Bertrand, *Enigma ou la plus grande énigme de la guerre 1939–1945*, Paris 1973.
[2] Anthony Cave-Brown, *Bodyguard of Lies*, New York 1975.
[3] Peter Calvocoressi, *The Secrets of Enigma*, The Listener, London 20. I. 1977, 27. I. 1977, 3. II. 1977.
[4] Brian Johnson, *The Secret War*, London 1978.
[5] David Kahn, *The Code-Breakers*, New York 1968.
[6] Władysław Kozaczuk, *Bitwa o Tajemnice*, Warszawa 1967.
[7] – *Złamany szyfr*, Warszawa 1976.
[8] – *Wojna w eterze*, Warszawa 1977.
[9] – *W kręgu Enigmy*, Warszawa 1979.
[10] Ronald Lewin, *Ultra goes to War*, London 1978.
[11] Ilija Marinković, *„Enigma" do pobjede*, Zagreb 1977.
[12] M. Rejewski, *An application of the theory of permutations in breaking the Enigma cipher*, Applicationes Math. 16, zeszyt 4.
[13] William Stevenson, *A Man Intrepid*, New York 1976.
[14] Stanisław Strumph-Wojtkiewicz, *Sekret Enigmy*, Warszawa 1978.
[15] E. W. Winterbotham, *The Ultra Secret*, London 1974.
[16] F. H. Hinsley *et al.*, *British intelligence in the Second World War*, Vol. I, Appendix 1, *The Polish, French and British contributions to the breaking of the Enigma*, H.M.S.O., London 1979.
[17] Józef Garliński, *Intercept*, London 1979.
[18] Ralph Bennett, *Ultra in the West*, London 1979.
[19] T. Lisicki, *Die Leistung des polnischen Endzifferungsdienstes bei der Lösung des Verfahrens der deutschen „Enigma-Funkschlüsselmaschinen"*, w książce: J. Rohwer und E. Jäckel, *Die Funkaufklärung und ihre Rolle in Zweiten Weltkrieg*, Stuttgart 1979, str. 66–87.