Paweł Gładki

Jak matematycy polscy złamali szyfr Enigmy

1 Rys historyczny

Marian Rejewski urodził się 16 sierpnia 1905 r. w Bydgoszczy, ukończył tam w 1923 r. gimnazjum klasyczne. Studiował matematykę na Uniwersytecie Poznańskim otrzymując stopień magistra filozofii w 1929 r., po czym przebywał rok w Getyndze, specjalizując się w matematyce ubezpieczeniowej. Od września 1930 do września 1932 był młodszym asystentem w Instytucie Matematycznym Uniwersytetu Poznańskiego i jednocześnie pracownikiem poznańskiej filii Biura Szyfrów Sztabu Głównego WP. Przeniesiony do tegoż biura do Warszawy znalazł na przełomie lat 1932-1933 metodę odczytywania depesz zaszyfrowanych za pomocą niemieckiej Enigmy, a następnie - wraz ze swymi współpracownikami - wielokrotnie metodę tę doskonalił. Ewakuowany ze stolicy znalazł się 17. IX. 1939 w Rumunii, skąd dostał się 25.IX.1939 do Francji. Tam kontynuował swą dawną pracę włączony do grupy płk. Bertranda w Château Vignolles w Gretz-Armainvillers koło Paryża. Po inwazji niemieckiej i ewakuacji do Algierii wrócił potajemnie do nieokupowanej części Francji, by w pałacu Les Fouzes w Uzés dalej działać pod kierunkiem Bertranda aż do zajęcia południa Francji przez Niemców. 30.I.1943 przeszedł przez Pireneje do Hiszpanii, skąd po trzymiesięcznym pobycie w więzieniu dostał się przez Portugalię i Gibraltar do Anglii. Tam przydzielono go do oddziału radiowywiadowczego Polskich Sił Zbrojnych. 21 listopada 1946 wrócił do Polski, następnie przez 20 lat pracował jako urzędnik w różnych przedsiębiorstwach w Bydgoszczy, a w lutym 1967 przeszedł na rentę. Zmarł w Warszawie 13 lutego 1980 r.

2 Podstawowe wiadomości o budowie Enigmy

Maszyna 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 oznaczonymi tymi samymi literami co klawisze. Znajdowało się w niej także źródło prądu w postaci bateryjki.

Sercem maszyny były umieszczone na jednej osi i mogące się obracać, wzajemnie przestawialne trzy bębenki szyfrujące L, M, i N, oraz bębenek odwracający R, w modelu wojskowym nieruchomy. Każdy z bębenków miał pierścień z wyrytymi na obwodzie 26 literami alfabetu. Literę znajdującą się u góry widać było w okienku umieszczonym w metalowym wieku maszyny. Pierścień mógł zmieniać położenie w stosunku do reszty bębenka.

Środkową część bębenków stanowił ebonitowy krążek, w którym po jednej stronie znajdowało się koncentrycznie 26 kontaktów stałych, połączonych izolowanymi drucikami w sposób nieregularny ze znajdującymi się po drugiej stronie, też koncentrycznie umieszczonymi 26 kontaktami sprężynującymi. Bębenek

odwaracający miałpo jednej stronie 26 kontaktów sprężynujących, połączonych w sposób nieregularny między sobą.

Gdy naciśnięto klawisz, bębenek szyfrujący N wykonywał obrót o $\frac{1}{26}$ część obwodu, prąd od naciśniętego klawisza płynął poprzez trzy bębenki szyfrujące, przez bębenek odwracający, ponownie przez bębenki szyfrujące i zapalał którąś z żarówek. Zauważmy, że gdy w danym momencie nacisnęło się klawisz np. z literą u, zapalała się lampka z inną literą, zawsze różną od naciśniętej, np. z literą d. Przy następnym jednak naciśnięciu litery u, na skutek dokonywanego obrotu bębenków szyfrujących, zapalała się już inna literka.

Gdy wstukiwało siękolejne litery tekstu otwartego, zwanego klerem, wówczas litery zapalających się sukcesywanie żaróweczek tworzyły tekst zaszyfrowany. Gdy natomiast wstukiwało się kolejne litery szyfru, litery zapalających się kolejno żarówek tworzy y kler. Sprawiał to bębenek odwracający.

TWIERDZENIE **2.1** *Zbiór wszystkich transpozycji generuje grupę permutacji.*

Widzimy więc, że permutacja szyfrująca była inwolucją, będącą iloczynem 13 transpozycji.

Bębenków szyfrujących o różnych połączeniach można utowzyć:

$$26! = 403291461126605663558400000 0$$

Różnych bębenków odwracających zaś:

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

Zatem fabryka produkująca Enigmy mogła dostarczać każdemu odbiorcy zamówioną partię maszyn z odmiennymi połączeniami bębenków. Jednak wszystkie komplety bębenków maszyn wojskowych, których liczbę szacuje się na 100 do 200 tysięcy, miały te same połączenia, tak że szyfranci jakichkolwiek dwóch jednostek wojskowych mogli się porozumiewać za pomocątych maszyn.

Pod warunkiem wszakże, że mieli je nastawione na ten sam klucz. Albowiem klucz, obok połączeń bębenków, była to druga z tajemnic Enigmy. Każdy bębenek można bowiem nastawić na 26 sposobów, zatem 3 bębenki na $26^3 = 17576$ sposobów. Z kolei kolejność trzech bębenków na osi można jeszcze zmienić na sześć sposobów, razem więc mamy $6 \cdot 26^3 = 105456$ możliwości. Liczba ta wydała się jednak niemieckim specjalistom za mała. Do maszyn wojskowych dołączano więc łącznicę, coś w rodzaju centrali telefonicznej - dodatkowe urządzenie szyfrujące, które umożliwiało dodatkowe pozamienianie kolejności w dowolnych sześciu parach liter, co stworzyło dodatkowych $\frac{26!}{2^6 6!14!} = 100391791500$ możliwości.

Zestaw potrzebnych szyfrantom informacji, tj. ustawienie bębenków, ich kolejność i połączenia na łącznicy, nazywano **kluczem dziennym**. Klucz ten każdego dnia ulegał modyfikacji, choć pod koniec wojny niektóre jego elementy zmieniały się częściej niż co dobę.

Zaszyfrowanie wszystkich depesz danego dnia z tej samej pozycji bębenków oznaczałoby w praktyce dekonspirację tych depesz. Wówczas bowiem pierwsze litery wszystkich depesz stanowiłyby zwykłą literówkę - banalną do rozszyfrowania. Istniała zatem konieczność pozostawienia do decyzji szyfranta wyboru pozycji bębenków, od której zamierzał rozpocząć szyfrowanie danej depeszy. Wymagało to podania trzech zaszyfrowanych liter, a ponieważ droga radiowa nie zawsze zapewniała dobry odbiór, należało te litery - zaszyfrowane dwukrotnie - podać, po czym otrzymane w ten sposób sześć liter umieszczano na początku danej depeszy. Owe trzy litery nazywano **kluczem depeszy** i one to stanowiły trzecią tajemnicę Enigmy.

3 Klucze depeszy

To, że pierwsze sześć liter każdej depeszy rzucało się w oczy i nie będziemy się nad tym zastanawiać. Omówmy sposób w jaki złamano klucz depeszy, a potem uzasadnijmy poprawność przeprowadzonego rozumowania.

Wypiszmy oddzielnie sześć pierwszych liter wszystkich depesz danego dnia. Wszystkie klucze, które miały tę samą pierwszaą literę, miały oczywiście tę samą czwartą literę. To samo można powiedzieć o drugich i piątych oraz o trzecich i szóstych literach. Wybierzmy dowolny klucz i napiszmy pierwszą literę i obok czwartą literę. Potem wybierzmy klucz mający jako pierwszą literę - czwartą literę poprzedniego klucza, czwartą zaś literę napiszmy obok czwartej litery poprzedniego klucza. Postępując tak dalej dojdziemy w końcu do pierwszej napisanej litery. Drugi raz tej samej litery nie piszemy, lecz ujmijmy uzyskany wynik w nawias. Oto przykład. Niech:

$$dmq\ vbn$$

$$von\ puy$$

$$puc\ fmq$$

stanowią trzy zaszyfrowane klucze depesz danego dnia. Postępując w opisany sposób otrzymujemy:

$$dvpf$$

Przypuśćmy, że z dostarczonego materiału wynikałoby, że mamy cykl liter:

$$(dvpfkxgzyo)$$

Powiedzmy, że z pozostałych depesz powstałyby jeszcze dalsze cykle, tak że ogół cykli utworzonych z pierwszych i czwartych liter wyglądałby następująco:

$$AD = (dvpfkxbzyo)(eijmunqlht)(bc)(rw)(a)(s)$$

W ten sam sposób postąpimy z literami drugimi i piątymi oraz trzecimi i szóstymi. Otrzymamy układm który będzie wyglądał na przykład tak:

$$AD = (dvpfkxbzyo)(eijmunqlht)(bc)(rw)(a)(s)$$

$$BE = (blfqveoum)(hjpswizrn)(axt)(cgy)(d)(k)$$

$$CF = (abviktjgfcqny)(duzrehlxwpsmo)$$

Układ taki nazywać będziemy *charakterystyką* danego dnia.

Cykle tej samej d lugości występują zawsze w liczbie parzystej. Jak to można uzasadnić? Jeżeli naciśniemy kolejno wszystkie klawisze w ten sposób, że nastawienie bębenków się nie zmieni (np. przytrzymując jeden klawisz), to zapalać będą się coraz inne żarówki. Powstanie permutacja pewnych liter. Przy innym nastawieniu bębenków permutacja będzie oczywiście inna, ale za sprawą bębenka odwracającego , wszystkie permutacje będą składały się z samych transpozycji, bo np. jeżeli naciśnięcie d spowoduje zapalenie z, to naciśnięcie z spowoduje zapalenie d.

Jeżeli sześć kolejnych permutacji powstających podczas dwukrotnego szyfrowania kluczy depesz oznaczymy literami od A do F, to iloczyny tych permutacji AD, BE i CF będą identyczne z wyrażeniami tworzącymi charakterystykę dnia.

Ale dlaczego w tych wyrażeniach cykle tej samej długości występują zawsze w liczbie parzystej?. Wynika to z następującego twierdzenia:

TWIERDZENIE **3.1** *Jeżeli dwie permutacje X i Y tego samego stopnia składają się z samych transpozycji rozłącznych*

Prawdziwe jest też twierdzenie odwrotne:

TWIERDZENIE **3.2** *Jeśli 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*

Możemy też wykazać, że:

TWIERDZENIE **3.3** *(i) Litery wchodzące do jednej i tej samej transpozycji permutacji X lub Y wchodzą zawsze do dwóch różnych cykli tej samej permutacji XY.*

(ii) 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.

Wystarczy jeszcze znać zwyczaje szyfrantów, by całkowicie zrekonstruować wszystkie klucze depesz. Niech na przykład szyfranci lubią jako klucze wybierać trzy jednakowe litery jak *aaa*, *bbb* itp. Spójrzmy na przykładową charakterystykę. 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 winna być s. Przypuśćmy, że wśród zaszyfrowanych kluczy depesz danego dnia były trzy klucze rozpoczynające się na literę s:

$$sug\ smf$$

$$sjm\ spo$$

$$syx\ scw$$

Zaszyfrowan 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 trzyliterowych 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.

Konieczna oczywiście jest tutaj dobra znajomość zwyczajów szyfrantów. Hipoteza, że będzie dużo kluczy w rodzaju *aaa*, *bbb* itp. jest autentyczna - niemieccy szyfranci rzeczywiście mieli taki nawyk. Później bardzo uważnie śledzono ewolucję ich zwyczajów. Na przykład, kiedy zakazano szyfrantom stosowania kluczy *aaa*, *bbb* itp., odruchowo stosowali oni klucze, w których żadne litery się nie powtarzały.

4 Połączenia bębenków

Byłoby lepiej dla Niemców, gdyby kluczy depesz w ogóle nie szyfrowali. I tak nie ustrzegło ich to przed ich rozszyfrowaniem, a w dodatku dostarczyło informacji w postaci sześciu kolejnych permutacji od A do F.

Oznaczmy permutację spowodowaną przez łącznicę literą S, przez trzy bębenki szyfrujące literami L, M i N, a przez bębenek odwracający literą R. Dodatkowo wprowadźmy bębenek nieruchomy H pomiędzy łącznicą a bębenkiem N. Przbieg prądu można oznaczyć jako:

$$SHNMLRL^{-1}M^{-1}H^{-1}S^{-1}$$

Ponieważ po każdym naciśnięciu klawisza bębenek N obraca się o $\frac{1}{26}$, więc musimy wprowadzić dodatkową permutację P przesuwającą literki *a* na *b*, *b* na *c*, ..., *z* na *a*. Teraz znane nam permutacje od A do F można przedstawić w postaci równań:

$$A = SHPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}H^{-1}S^{-1}$$

$$B = SHP^2NP^{-2}MLRL^{-1}M^{-1}P^2N^{-1}P^{-2}H^{-1}S^{-1}$$

$$C = SHP^3NP^{-3}MLRL^{-1}M^{-1}P^3N^{-1}P^{-3}H^{-1}S^{-1}$$

$$D = SHP^4NP^{-4}MLRL^{-1}M^{-1}P^4N^{-1}P^{-4}H^{-1}S^{-1}$$

$$E = SHP^5NP^{-5}MLRL^{-1}M^{-1}P^5N^{-1}P^{-5}H^{-1}S^{-1}$$

$$F = SHP^6NP^{-6}MLRL^{-1}M^{-1}P^6N^{-1}P^{-6}H^{-1}S^{-1}$$

Zakładamy tu, że obracał się tylko bębenek prawy, czyli N, natomiast bębenki L i M podczas kolejnych sześciu uderzeń w klawisze nie obracały się. W praktyce zdarzało się to w 21 na 26 przypadków. Wówczas we wszystkich powyższych równaniach możemy dokonać następującego uproszczenia:

$$Q = MLRL^{-1}M^{-1}$$

Otrzymujemy więc układ 6 równań z 4 niewiadomymi permutacjami S, H, N i Q:

$$A = SHPNP^{-1}QPN^{-1}P^{-1}H^{-1}S^{-1}$$
$$B = SHP^2NP^{-2}QP^2N^{-1}P^{-2}H^{-1}S^{-1}$$
$$C = SHP^3NP^{-3}QP^3N^{-1}P^{-3}H^{-1}S^{-1}$$
$$D = SHP^4NP^{-4}QP^4N^{-1}P^{-4}H^{-1}S^{-1}$$
$$E = SHP^5NP^{-5}QP^5N^{-1}P^{-5}H^{-1}S^{-1}$$
$$F = SHP^6NP^{-6}QP^6N^{-1}P^{-6}H^{-1}S^{-1}$$

Będziemy zmierzali do zmniejszenia liczby niewiadomych.

Ponieważ w maszynie handlowej połączenia bębenka wstępnego miały postać:

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

więc matematycy przyjęli, że w maszynie wojskowej permutacja ta jest taka sama. Wprawdzie okazało się to błędne i przysporzyło nawet zupełnie niepotrzebnych komplikacji, ale przyjmijmy, że H jest znane.

Z pomocą przyszły służby wywiadowcze. 9 grudnia 1932 roku matematykom dostarczono fotokopię kluczy dziennych na wrzesień i październik 1932 roku. Ponieważ tablice te zawierały też codzienne zmiany połączeń łącznicy, więc permutację S udało się odtworzyć i jako znaną wraz z przyjętą za ananą H przenieść na drugą stronę równań. Otrzymujemy:

$$H^{-1}S^{-1}ASH = PNP^{-1}QPN^{-1}P^{-1}$$
$$H^{-1}S^{-1}BSH = P^2NP^{-2}QP^2N^{-1}P^{-2}$$
$$H^{-1}S^{-1}CSH = P^3NP^{-3}QP^3N^{-1}P^{-3}$$
$$H^{-1}S^{-1}DSH = P^4NP^{-4}QP^4N^{-1}P^{-4}$$
$$H^{-1}S^{-1}ESH = P^5NP^{-5}QP^5N^{-1}P^{-5}$$
$$H^{-1}S^{-1}BSH = P^6NP^{-6}QP^6N^{-1}P^{-6}$$

W takiej postaci wszystkie permutacje po lewej stronie są znane, a po prawej nie są znane tylko N i Q. Przekształćmy obie strony każdego z równań przez automorfizm wewnętrzny wyznaczony odpowiednio przez P, P^2, P^3, P^4, P^5 i P^6. Dla prostoty oznaczmy też lewe strony odpowiednio przez U, V, W, X, Y i Z. Mamy:

$$U = P^{-1}H^{-1}S^{-1}ASHP = NP^{-1}QPN^{-1}$$
$$V = P^{-2}H^{-1}S^{-1}BSHP^2 = NP^{-2}QP^2N^{-1}$$
$$W = P^{-3}H^{-1}S^{-1}BSHP^3 = NP^{-3}QP^3N^{-1}$$
$$X = P^{-4}H^{-1}S^{-1}BSHP^4 = NP^{-4}QP^4N^{-1}$$
$$Y = P^{-5}H^{-1}S^{-1}BSHP^5 = NP^{-5}QP^5N^{-1}$$
$$Z = P^{-6}H^{-1}S^{-1}BSHP^6 = NP^{-6}QP^6N^{-1}$$

Przemnóżmy po dwa kolejne z tych wyrażeń:

$$UV = NP^{-1}(QP^{-1}QP)PN^{-1}$$
$$VW = NP^{-2}(QP^{-1}QP)P^2N^{-1}$$
$$WX = NP^{-3}(QP^{-1}QP)P^3N^{-1}$$
$$XY = NP^{-4}(QP^{-1}QP)P^4N^{-1}$$
$$YZ = NP^{-5}(QP^{-1}QP)P^5N^{-1}$$

Eliminując wspólne wyrażenie $QP^{-1}QP$ otrzymujemy układ czterech równań z jedną niewiadomą NPN^{-1}:

$$VW = NP^{-1}N^{-1}(UV)NPN^{-1}$$
$$WX = NP^{-1}N^{-1}(VW)NPN^{-1}$$
$$XY = NP^{-1}N^{-1}(WX)NPN^{-1}$$
$$YZ = NP^{-1}N^{-1}(XY)NPN^{-1}$$

Widzimy, że wyrażenie VW jest przekształcone z UV za pomocą permutacji NPN^{-1}. Podpisując VW pod UV na wszystkie możliwe sposoby, a jest ich na ogół kilkadziesiąt, otrzymujemy kilkadziesiąt możliwych rozwiązań dla NPN^{-1}. Podobnie postępujemy dla pary WX i VW. Jedno z klikludziesięciu rozwiązań dla każdej pary powinno być identyczne w obu przypadkach. To właśnie jest nasze szukane NPN^{-1}. Dwa ostatnie równania są już zbyteczne.

Dalej jest już prosto. Wystarczy pod otrzymane wyrażenie NPN^{-1} podpisać znaną nam permutację P na wszystkie 26 sposobów, aby otrzymać 26 wariantów połączeń dla bębenka N. Który z nich wybierzemy, nie ma większego znaczenia, bo oznacza tylko większy lub mniejszy obrót w bębenku N strony z kontaktami stałymi w stosunku do strony z kontaktami sprężynującymi.

Tak to wygląda teoretycznie. W praktyce, w wyniku błędnych założeń co do bębenka H, iloczyny UV, VW, WX, XY i YZ były do siebie niepodobne i wskutek tego niemożliwe było podpisanie ich jednych pod drugimi.

Jakie więc były połączenia bębenka wstępnego? Opracowano potem dedukcyjną metodę ich znalezienia, nad którą nie będziemy się rozwodzić, po raz pierwszy wszakże znaleziono je metodą odgadnięcia. Okazało się, że permutacja ta była identycznościowa...

Połączenia pozostałych bębenków odkryto korzystając z faktu, że zmiana kolejności bębenków następowała co kwartał. Dostarczone przez wywiad materiały pochdziły z dwóch różnych kwartałów, więc tablice kluczy dziennych odzwierciedlały różną kolejność bębenków, przy czym po prawj stronie równań znajdowały się różne bębenki. W obu kwartałach można było więc zastosować taką samą metodę znalezienia ich połączeń. Znalezienie połączeń bębenka trzeciego oraz odwracającego nie stwarzało już większych trudności.

Połączenia bębenka wstępnego można znaleźć drogą dedukcyjną. A czy połączenia pozostałych bębenków też? Do dziś nie wiadomo, czy wypisany powyżej układ jest rozwiązalny. Można natomiast skonstruować inną metodę odtwarzania połączeń bębenków, ale nie będziemy się tym zajmować.

5 Klucze dzienne

Skoncentrowano się na fakcie, że permutacja S zamienia tylko sześć par liter, a 14 pozostawia niezmienionych. Rozważmy jeszcze raz układ:

$$A = SHPNP^{-1}QPN^{-1}P^{-1}H^{-1}S^{-1}$$
$$B = SHP^2NP^{-2}QP^2N^{-1}P^{-2}H^{-1}S^{-1}$$
$$C = SHP^3NP^{-3}QP^3N^{-1}P^{-3}H^{-1}S^{-1}$$
$$D = SHP^4NP^{-4}QP^4N^{-1}P^{-4}H^{-1}S^{-1}$$
$$E = SHP^5NP^{-5}QP^5N^{-1}P^{-5}H^{-1}S^{-1}$$
$$F = SHP^6NP^{-6}QP^6N^{-1}P^{-6}H^{-1}S^{-1}$$

Wiemy, że H jest identycznością, można ją więc opuścić. Przypuśćmy, że permutacja S jest również identycznościowa. Przenosząc wszystkie permutacje, za wyjątkiem niewiadomej Q, na lewą stronę otrzymujemy:

$$PN^{-1}P^{-1}APNP^{-1} = Q$$
$$P^2N^{-1}P^{-2}AP^2NP^{-2} = Q$$
$$P^3N^{-1}P^{-3}AP^3NP^{-3} = Q$$
$$P^4N^{-1}P^{-4}AP^4NP^{-4} = Q$$
$$P^5N^{-1}P^{-5}AP^5NP^{-5} = Q$$
$$P^6N^{-1}P^{-6}AP^6NP^{-6} = Q$$

Połącznie bębenka N są znane, ale nie znamy jego nastawienia. Poprawniej jest więc zapisać:

$$P^xN^{-1}P^{-x}AP^xNP^{-x} = Q$$
$$P^{x+1}N^{-1}P^{-x-1}AP^{x+1}NP^{-x-1} = Q$$
$$P^{x+2}N^{-1}P^{-x-2}AP^{x+2}NP^{-x-2} = Q$$
$$P^{x+3}N^{-1}P^{-x-3}AP^{x+3}NP^{-x-3} = Q$$
$$P^{x+4}N^{-1}P^{-x-4}AP^{x+4}NP^{-x-4} = Q$$
$$P^{x+5}N^{-1}P^{-x-5}AP^{x+5}NP^{-x-5} = Q$$

Gdyby permutacja S istotnie była identycznościowa, to podstawiając za x kolejno liczby od 1 do 26 otrzymalibyśmy przy pewnym określonym x to samo na wszystkie wyrażenia Q układu i w ten sposów znaleźlibyśmy nastawienie bębenka N. Ale tak nie jest, więc dla żadnego x wyrażenia Q nie będą równe między sobą, ale będą pomiędzy nimi pewne podobieństwa, jako że permutacja S wszystkich liter nie zamienia. Ta metoda byłaby jednak zbyt czasochłonna, opracowano więc tzw. **metodę rusztu**.

Wpisuje się dla każdego z trzech bębenków na stałe na arkuszu odpowiedniej wielkości 31 permutacji N, PNP^{-1}, P^2NP^{-2}, ..., $P^{25}NP^{-25}$, N, PNP^{-1}, ..., P^4NP^{-4} z połączeniami trzech bębenków w - przykładowo - następującej postaci:

N $\quad$ *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*

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

a na innej kartce z sześcioma otworami, zwanej rzusztem, wypisuje się poznane wcześniej permutacje od A do F w postaci:

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

$$\ldots$$

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

Następnie przesuwa sę ruszt po kartce z połączeniami bębenka N tak długo, aż trafi się na pozycję, w której odgaduje się pewne podobieństwa między poszczególnymi wyrażeniami Q. W tej pozycji należy wszystkie 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.

Pozostaje niewiadoma Q, $Q = MLRL^{-1}M^{-1}$. Znamy połączenia bębenków M, L i R, ale nie są znane pozycje M i L (R - nieruchomy). Należałoby więc napisać:

$$Q = P^yMP^{-y}P^zLP^{-z}RP^zL^{-1}P^{-z}P^yMP^{-y}$$

gdzie x i y przyjmują wartości od 1 do 26. Pierwsza znana metoda na znalezienie y i z polegała na codziennym przerabianiu możliwych $26^2 = 676$ pozycji na maszynie, dopóki nie trafiło się na właściwą.

Na obwodzie bębenków L, M i N umieszczone były przesuwalne pierścienie z wygrawerowanymi na nich iterami alfabetu. Trzeba było jeszcze odgadnąć ich ustawienia.

Z odczytanych depeszy dowiedziano się, że większość z nich zaczynała się od liter ANX (*an* - przyimek, x - oznaczenie spacji). Należało zatem wybrać odpowiednią depeszę zaczynającą się od liter np. *tuv* i stale przyciskając klawisz t obracać bębenkami i jednocześnie obserwować, kiedy zapali się lampka A. Wówczas powtórzyć operację dla literki u i potem jeszcze dla v. Jeśli otrzymamy rozwiązanie ANX, to mamy sporą szansę na to, że znaleźliśmy właściwe ustawienie. Jeśli nie - to szukamy dalej... Metoda ta, choć wymagająca maksymalnie $26^3 = 17576$ nastawień, okazała się skuteczna.

Tak oto złamano szyfr Enigmy.

6 Dalsze dzieje Enigmy

Ograniczone ramy tego referatu nie pozwalają na szczegółowe opisywanie wszystkich modyfikacji w budowie Enigmy oraz wprowadzanych udoskonaleń w rozszyfrowywaniu jej kodu. W latach 1933 - 1935 sporządzono katalog wszystkich możliwych permutacji Q. W tym samym okresie usprawniono metodę znajdowania nastawień pierścieni. Opracowano wtedy też tzw. **metodę zegara** umożliwiającą odgadywanie, który z bębenków danego dnia znajdował się po prawej stronie. Od roku 1936 zmodyfikowano konstrukcję łącznicy, która zmieniała już nie 6 par, ale 5 do 8 par liter. Utrudniło to posługiwanie się metodą rusztu, w zamian więc wymyślono przyrząd zwany **cyklometrem**, który pomagał odgadywać charakterystyki dnia. W 1937 roku Enigmami zaczęła posługiwać się niemiecka partyjna służba bezpieczeństwa, stosując pewien zmodyfikowany kod, który również został rozpracowany, co pomgło też w doskonaleniu metod nastawiania pierścieni. W 1938 roku zmieniono sposób nadawania kluczy depesz. Do ich rozkodowywania skonstruowano specjalną maszynęzwaną **bombą**. Pod koniec tego roku zmodyfikowano budowę Enigmy, stosując w miejsce 3 bębenków 5. W 1940 roku pracę nad Enigmami faktycznie przejęli Anglicy. Wykorzystując polskie osiągnięcia i modyfikując "bomby" zbudowali w 1943 roku - jak podaje Calvocoressi - coś na kształt pierwszego komputera.

References

[1] Gustave Bertrand, *Enigma ou la plus grande enigme 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] Władysław Kozaczuk, *Złamany szyfr*, Warszawa, 1976

[8] Władysław Kozaczuk, *Wojna w eterze*, Warszawa, 1977

[9] Władysław Kozaczuk, *W kręgu Enigmy*, Warszawa, 1979

[10] Ronald Lewin, *Ultra goes to War*, London, 1978

[11] Ilija Marinković, *"Enigma" do pobjede*, Zagreb, 1977

[12] Marian Rejewski, *An application of the theory of permutations in breaking the Enigma cipher*, Applicationes Mathematicae 16, zeszyt 4.

[13] Marian Rejewski, *Jak matematycy polscy rozszyfrowali Enigmę*, Wiadomości Matematyczne XXIII.1, (1980)

[14] William Stevenson, *A Man Intrepid*, New York, 1976

[15] Stanisław Strumph - Wojtkiewicz, *Sekret Enigmy*, Warszawa, 1978

[16] Ernest Winterbotham, *The Ultra Secret*, London, 1974

[17] Frank Hinsley i inni, *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

[18] Józef Garliński, *Intercept*, London, 1979

[19] Ralph Bennet, *Ultra in the West*, London, 1979

[20] Tomasz Lisicki, *Die Leistung des polnischen Endzifferungsdienstes bei der Lösung des Verfahrens der deutschen "Enigma - Funkschlüsselmaschinen"*, w książce: J. Rohwer, E. Jäckel, *Die Funkaufklärung und ihre Rolle in Zweiten Weltkrieg*, Stuttgart, 1979, str. 66-87