Jest to zapis odczytu wygłoszonego na XXXIX Szkole Matematyki Poglądowej *Domniemanie – Hipoteza – Dowód*, Sierpień 2007

# ENIGMA

*Wojciech GUZICKI, Warszawa*

W ostatnich dniach grudnia 2007 roku minęło 75 lat od jednego z największych osiągnięć w kryptografii, złamania budowy maszyny szyfrującej *Enigma* przez Mariana Rejewskiego. Osiągnięcie to ma dla nas, matematyków, szczególne znaczenie, gdyż złamanie budowy tej maszyny odbyło się za pomocą metod czysto matematycznych. W tym artykule zostanie przedstawione rozumowanie Mariana Rejewskiego, będące początkiem długiej historii łamania szyfrów *Enigmy*, najpierw przez matematyków polskich, a od wybuchu II Wojny Światowej, także matematyków angielskich (wśród nich Alana Turinga).

Maszyna szyfrująca *Enigma* została wprowadzona do użytku przez Niemców w końcu lat dwudziestych. Wywiad Wojska Polskiego dość szybko zdał sobie sprawę z tego, że Niemcy używają szyfrów zupełnie nowego typu, niepodatnych na dotychczasowe metody kryptoanalizy. O niezwykłej intuicji osób kierujących wywiadem świadczy to, że zorganizowali kurs kryptografii dla studentów matematyki Uniwersytetu Poznańskiego, zdając sobie sprawę, że wiedza matematyczna połączona z dobrą znajomością niemieckiego może okazać się konieczna do złamania tych szyfrów. Marian Rejewski był jednym z absolwentów tego kursu i jesienią 1932 roku rozpoczął pracę w Biurze Szyfrów w Warszawie. Po przekonaniu się o jego wyjątkowych zdolnościach do analizy szyfrów zlecono mu rozpracowanie maszyny *Enigma*. Mimo wielkich trudności i okresów zastoju, gdy nawet zastanawiano się, czy nie przerwać pracy nad *Enigmą*, Rejewskiemu udało się rozwiązać pierwszy i chyba najważniejszy problem – budowę wewnętrzną maszyny – przed końcem 1932 roku. Od tej chwili trzyosobowy zespół kryptologów, Marian Rejewski, Jerzy Różycki i Henryk Zygalski, mogli poświęcić się metodom poszukiwania kluczy dziennych i kryptoanalizie zaszyfrowanych niemieckich depesz.

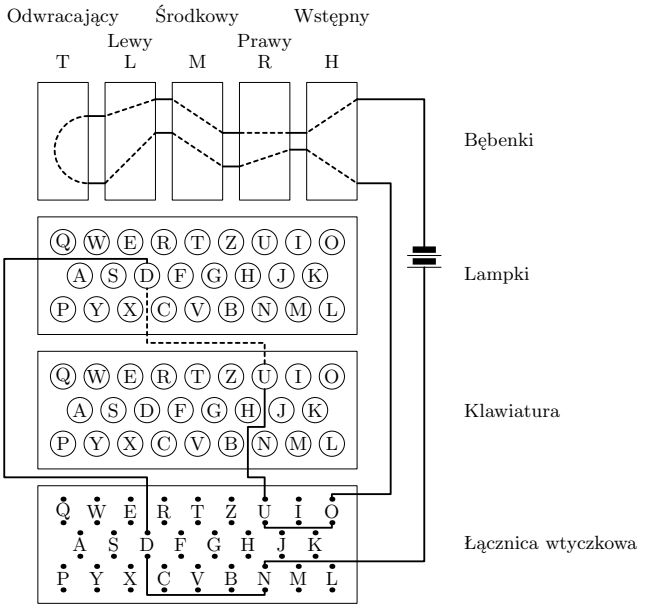
W tym artykule ograniczymy się tylko do pierwszych dwóch problemów *Enigmy*: poszukiwania tzw. kluczy depesz i odtworzenia wewnętrznych połączeń bębenków szyfrujących – serca maszyny szyfrującej. O trzecim wielkim problemie, znajdowaniu kluczy dziennych, a także o historii polskiej i brytyjskiej kryptografii związanej z *Enigmą* można przeczytać w licznych publikacjach na ten temat (por. zwłaszcza trzy książki historyczne [5], [6] i [7], dwa artykuły Rejewskiego [8] i [9], a także książkę [4] poświęconą w całości opisowi matematycznych metod użytych w kryptoanalizie *Enigmy*). Zaczniemy od opisu maszyny *Enigma*.

**Opis maszyny szyfrującej Enigma**

Maszyna *Enigma* składała się z czterech zasadniczych części. Pierwszą była klawiatura podobna do klawiatury maszyny do pisania (z niemieckim układem klawiszy). Nie było jednak czcionek, zamiast nich w *Enigmie* były lampki. Za klawiaturą (patrząc od strony piszącego) znajdowała się bowiem druga ważna część maszyny: układ (taki sam jak klawiszy) lampek. Po naciśnięciu klawisza zapalała się jedna lampka: była to litera kryptogramu odpowiadająca literze znajdującej się na naciśniętym klawiszu. Trzecią część maszyny stanowił układ pięciu bębenków szyfrujących. Trzy bębenki były ruchome. Po naciśnięciu klawisza prawy z owych trzech bębenków przekręcał się o jedną pozycję. Gdy dokonał on pełnego obrotu, bębenek środkowy obracał się o jedną pozycję. Wreszcie, gdy bębenek środkowy obrócił się o kąt pełny, obracał się o jedną pozycję również bębenek lewy. Układ tych trzech bębenków zachowywał się zatem w taki sposób, jak mechaniczny licznik kilometrów w samochodzie. Każdy z tych trzech bębenków miał 26 możliwych pozycji w maszynie; odpowiadały one literom alfabetu. Każdy bębenek był otoczony pierścieniem z zaznaczonymi na nim literami. Bębenki te można było w maszynie obracać ręcznie, ustawiając je na dowolnej z $26^3$ pozycji. Bębenki te można było wyjmować z maszyny i wkładać w dowolnej kolejności. Łącznie dawało to $6 \cdot 26^3 = 105456$ możliwych ustawień początkowych trzech bębenków. Każdy bębenek miał z obu stron styki, przez które prąd elektryczny

mógł przepływać z jednego bębenka do następnego. Na prawo od trzech ruchomych bębenków znajdował się tzw. bębenek wstępny, o identycznej budowie jak te trzy bębenki ruchome, ale ustawiony nieruchomo w jednej ustalonej pozycji. Na lewo od ruchomych bębenków znajdował się tzw. bębenek odwracający. Był on nieruchomy i miał styki tylko po jednej stronie, kontaktujące ze stykami lewego ruchomego bębenka. Prąd elektryczny przepływał przez bębenki w następujący sposób: po naciśnięciu klawisza prąd przepływał do odpowiadającego tej literze miejsca na prawej powierzchni bębenka wstępnego, następnie wewnątrz bębenka wstępnego do jednego ze styków na jego lewej powierzchni. Ten styk kontaktował się z położonym naprzeciw niego stykiem na prawej powierzchni prawego bębenka ruchomego. Prąd przepływał do tego bębenka, a następnie wewnątrz niego do odpowiedniego styku na lewej powierzchni. Ten styk kontaktował się z jednym ze styków na prawej powierzchni bębenka środkowego i tak dalej. Prąd przepływał przez wszystkie bębenki ruchome, wpływał do bębenka odwracającego (jednym ze styków na jego prawej powierzchni), przepływał wewnątrz tego bębenka do innego styku na prawej powierzchni i wracał do bębenka lewego. Przepływał następnie inną drogą przez wszystkie bębenki ruchome i bębenek wstępny, opuszczając w ten sposób układ pięciu bębenków. Czwartą część maszyny stanowiła tzw. łącznica wtyczkowa podobna do dawnych central telefonicznych. Każdej literze alfabetu odpowiadało gniazdko elektryczne. Parę takich gniazdek można było połączyć przewodem elektrycznym, powodując w ten sposób zamianę dwóch liter.

Teraz możemy już opisać dokładnie przebieg prądu w całej maszynie. Po naciśnięciu klawisza, np. z literą `U` następował opisany wyżej obrót bębenków ruchomych i prąd przepływał do litery `U` w łącznicy wtyczkowej. Przypuśćmy, że literę `U` połączono przewodem z literą `O`. Prąd przepływał do gniazdka litery `O` i z niego do odpowiadającego tej literze styku bębenka wstępnego. (Gdyby gniazdko litery `U` nie było połączone z żadnym innym gniazdkiem, to prąd popłynąłby do styku odpowiadającego literze `U`.) Następnie prąd przepływał w obie strony przez cały układ bębenków i powracał do łącznicy wtyczkowej. Przypuśćmy, że układ bębenków i ich połączenia wewnętrzne powodowały w danym momencie, że z układu bębenków prąd wypływał stykiem litery `N` bębenka wstępnego. Wówczas prąd dopływał do gniazdka `N` łącznicy wtyczkowej. Załóżmy, że to gniazdko było połączone z gniazdkiem `D`. Wtedy prąd wypływał z łącznicy do lampki `D` i właśnie ta lampka zapalała się. Oznaczało to, że literze `U` tekstu otwartego odpowiadała w danym momencie litera `D` kryptogramu. Maszynę obsługiwało zazwyczaj dwóch szyfrantów. Jeden naciskał klawisze odpowiadające kolejnym literom tekstu otwartego, drugi zaś spisywał litery na zapalających się lampkach; były to kolejne litery kryptogramu.




Należy jeszcze powiedzieć, że maszyny *Enigma* były produkowane w dwóch wersjach: handlowej i wojskowej. Wersje handlowe były produkowane parami: tylko te dwie maszyny mogły się ze sobą komunikować. Każda para miała własne indywidualne połączenia wewnętrzne bębenków ruchomych i bębenka odwracającego. Połączenia bębenka wstępnego były jednakowe we wszystkich maszynach typu handlowego. Maszyny handlowe nie miały też łącznicy wtyczkowej. Druga wersja *Enigmy*, maszyna wojskowa, miała inne połączenia bębenków, jednakowe we wszystkich maszynach. W ten sposób każda maszyna wojskowa mogła się komunikować z każdą inną maszyną wojskową. Niemcy uważali, że ogromna liczba możliwych połączeń wewnętrznych bębenków oraz wielka liczba kluczy (ustawienia bębenków i połączenia łącznicy wtyczkowej) gwarantują bezpieczeństwo szyfru.

Opisany wyżej przebieg prądu możemy obejrzeć na szkicu.

**Szyfrowanie i rozszyfrowywanie**

Przed przystąpieniem do szyfrowania szyfrant sprawdzał w specjalnych tablicach tzw. klucz dzienny. Opisywał on kolejność bębenków ruchomych (zmienianą raz na kwartał) i pozycje początkowe bębenków (zmieniane codziennie). Bębenki ruchome miały jeszcze jedną cechę. Mianowicie można było obracać względem siebie powierzchnię lewą i prawą. Przy jednej literze znajdował się znacznik określający tzw. „pozycję zerową". Naprzeciw niego mnożna było ustawić dowolną literę drugiej powierzchni bębenka. W ten sposób ustawiano tzw. skręcenie bębenka, podawane również w tabeli kluczy dziennych. Wreszcie częścią klucza dziennego było sześć par liter, które należało połączyć ze sobą w łącznicy wtyczkowej.

Szyfrant ustawiał maszynę zgodnie z tablicą kluczy dziennych i wybierał trzyliterowy klucz depeszy. Dwukrotnie szyfrował ten klucz depeszy za pomocą maszyny ustawionej na dany klucz dzienny i przestawiał bębenki na swój klucz depeszy. Nie zmieniał kolejności bębenków ani ich skręceń i nie zmieniał połączeń w łącznicy wtyczkowej. Jedynie przekręcał bębenki ruchome na wybrane przez siebie pozycje. Wtedy maszyna była gotowa do szyfrowania depeszy.

Odszyfrowywanie odbywało się w taki sam sposób. Szyfrant ustawiał maszynę na dany klucz dzienny, rozszyfrowywał dwukrotnie zaszyfrowany klucz depeszy, przestawiał bębenki na ten klucz i rozszyfrowywał depeszę. Cechą konstrukcyjną *Enigmy*, za którą odpowiadał bębenek odwracający, było to, że jeśli naciśnięcie np. litery `U` powodowało zapalenie się lampki `D`, to przy tym samym ustawieniu maszyny naciśnięcie litery `D` powodowało zapalenia się lampki `U`. A więc wystukiwanie kolejnych liter tekstu otwartego dawało tekst zaszyfrowany, a wystukiwanie w tym samym ustawieniu kolejnych liter tekstu zaszyfrowanego dawało tekst otwarty. Niewątpliwie ułatwiało to pracę szyfrantom, ale też przyczyniło się do złamania szyfru.

**Przykład szyfrowania**

W Internecie można znaleźć wiele symulatorów *Enigmy* (np. [1]). Za pomocą symulatora [1] możemy uzyskać następujący przykład kryptogramu. A oto ustawienia maszyny (podawane szyfrantom w wykazie kluczy dziennych):

Bębenek prawy (Eingangswalze): II,
Bębenek środkowy (Mittelwalze): I,
Bębenek lewy (Endwalze): III,
Bębenek odwracający (Umkehrwalze): B,
Usytuowanie pierścieni, czyli skręcenie bębenków (Ringstellung): V, I, M,
Pierwotne pozycje bębenków (Grundstellung): J, W, S,
Połączenia łącznicy wtyczkowej (Steckverbindungen): (A,S), (E,Z), (G,L), (P,R), (T,X), (V,Y).

Tekst otwarty i odpowiadający mu kryptogram:

`MECMECGRZEGORZEWICE`

`RCGROKWHUBUFNHRDBIX`

Po pierwszych sześciu literach tekstu otwartego szyfrant zmienia pozycje bębenków na MEC i wpisuje dalszy tekst. Podczas rozszyfrowywania szyfrant rozszyfrowuje dwukrotnie zaszyfrowany klucz MEC, przestawia pozycje bębenków na MEC i kontynuuje rozszyfrowywanie kryptogramu.

**Odczytanie kluczy depesz**

W każdym momencie przypiszemy maszynie pewną permutację. Mianowicie, jeśli w danym ustawieniu maszyny litera $\alpha$ jest szyfrowana jako $\beta$, to ta permutacja przyporządkowuje literze $\alpha$ literę $\beta$. A więc z każdym ustawieniem maszyny związana jest permutacja pokazująca, w jaki sposób są szyfrowane wszystkie litery. Zauważmy też, że naciśnięcie każdego klawisza powodowało zmianę ustawienia maszyny: prawy bębenek obracał się o jedną pozycję, a w niektórych przypadkach obracał się również bębenek środkowy lub oba pozostałe

bębenki, środkowy i lewy. Zatem po każdym naciśnięciu klawisza dostajemy nową permutację opisującą stan maszyny i sposób szyfrowania wszystkich liter. Pierwszy krok na drodze prowadzącej do złamania szyfru Enigmy polegał na znalezieniu tych permutacji dla pierwszych kilku ustawień maszyny danego dnia. Popatrzmy teraz, w jaki sposób Rejewski znalazł te permutacje. Wiadomo było tylko, że w *Enigmach* typu handlowego taka permutacja jest iloczynem rozłącznych transpozycji. Czy tak też było w *Enigmach* typu wojskowego? Oddajmy głos Rejewskiemu:

„To, że pierwsze sześć liter każdej depeszy stanowiły jej trzyliterowy klucz dwukrotnie zaszyfrowany, rzucało się w oczy i nad tym nie będę się zatrzymywał."

Nie zatrzymujmy się zatem i my. Popatrzmy natomiast na przykładowy zestaw sześcioliterowych początków 64 depesz z jednego dnia (a więc zaszyfrowanych za pomocą maszyn ustawionych tak samo).

| Nr | 6 liter | Nr | 6 liter | Nr | 6 liter | Nr | 6 liter |
|---|---|---|---|---|---|---|---|
| 1. | AKF NEV | 17. | IEG JWK | 33. | ORM XPB | 49. | SYJ HLS |
| 2. | AKF NEV | 18. | IZW JMF | 34. | ORM XPB | 50. | TLC UIY |
| 3. | BAI GSA | 19. | JNA ODT | 35. | OTG XJK | 51. | TZM UMB |
| 4. | BAI GSA | 20. | KJX WYR | 36. | OTG XJK | 52. | TZM UMB |
| 5. | BGQ GQN | 21. | KJX WYR | 37. | OTG XJK | 53. | UQV FBC |
| 6. | COA VRT | 22. | KPT WHG | 38. | PMD ETU | 54. | VCW BOF |
| 7. | DDZ SUM | 23. | KXW WCF | 39. | PTR EJD | 55. | VCW BOF |
| 8. | ETS IJX | 24. | LCB QOQ | 40. | PTR EJD | 56. | VSY BKL |
| 9. | FRN TPH | 25. | MBU MNW | 41. | PTR EJD | 57. | VSY BKL |
| 10. | GGT LQG | 26. | MLK MIO | 42. | PTR EJD | 58. | WFA YGT |
| 11. | GGT LQG | 27. | NQH CBI | 43. | QOV ZRC | 59. | WFA YGT |
| 12. | HHZ DZM | 28. | OPL XHP | 44. | QOV ZRC | 60. | XHP KZJ |
| 13. | HIE DXZ | 29. | OPL XHP | 45. | RND RDU | 61. | YUH PAI |
| 14. | HVF DFV | 30. | OPL XHP | 46. | RND RDU | 62. | YYC PLY |
| 15. | IEG JWK | 31. | OPL XHP | 47. | SLO HIE | 63. | ZWQ AVN |
| 16. | IEG JWK | 32. | OPL XHP | 48. | SLO HIE | 64. | ZWQ AVN |

Literami $A$, $B$, $C$, $D$, $E$ i $F$ oznaczmy permutacje związane z pierwszymi sześcioma ustawieniami maszyny danego dnia. Popatrzmy na pierwszą pozycję w powyższej tabeli: `AKF NEV`. Pierwsza litera `A` i czwarta litera `N` powstały z zaszyfrowania tej samej litery $\alpha$ w dwóch różnych ustawieniach maszyny (opisanych przez permutacje $A$ i $D$). Jeśli słuszne jest przypuszczenie, że w Enigmie typu wojskowego wszystkie rozważane permutacje są iloczynami rozłącznych transpozycji, to w permutacji $A$ występuje transpozycja $(\alpha, \texttt{A})$, a w permutacji $D$ występuje transpozycja $(\alpha, \texttt{N})$. Zatem permutacja $AD$ przeprowadza literę `A` na literę `N`.

**Uwaga.** Jeśli dane są permutacje $\sigma$ i $\pi$ to symbolem $\sigma\pi$ oznaczamy złożenie $\pi \circ \sigma$. Inaczej mówiąc, w złożeniach zapisujemy permutacie w kolejności składania (licząc od lewej strony).

Przyglądając się parom: pierwsza litera – czwarta litera w pozostałych depeszach, możemy odtworzyć w ten sposób całą permutację $AD$, a także całe permutacje $BE$ i $CF$. Oto one:

$AD =$ `(A,N,C,V,B,G,L,Q,Z)(E,I,J,O,X,K,W,Y,P)(D,S,H)(F,T,U)(M)(R)`

$BE =$ `(A,S,K,E,W,V,F,G,Q,B,N,D,U)(C,O,R,P,H,Z,M,T,J,Y,L,I,X)`

$CF =$ `(A,T,G,K,O,E,Z,M,B,Q,N,H,I)(C,Y,L,P,J,S,X,R,D,U,W,F,V)`

Znalezione permutacje $AD$, $BE$ i $CF$ miały wspólną cechę: cykle tej samej długości występowały parami. Wynika to bowiem z następującego twierdzenia:

**Twierdzenie 1.** Jeśli każda z permutacji $P$ i $Q$ jest iloczynem rozłącznych transpozycji, to ich złożenie $PQ$ jest permutacją, w której liczby cykli tej samej długości są liczbami parzystymi.

**Dowód.** Przypuśćmy najpierw, że w permutacjach $P$ i $Q$ występuje ta sama transpozycja:

$$P = (a, b)P', \quad Q = (a, b)Q',$$

dla pewnych permutacji $P'$ i $Q'$. Wtedy

$$PQ = (a)(b)P'Q',$$

przy czym możemy założyć (indukcja!), że złożenie $P'Q'$ ma żądaną własność. Ponieważ doszły dwa cykle długości 1, więc złożenie $PQ$ ma też tę własność. Przypuśćmy zatem, że permutacje $P$ i $Q$ nie mają wspólnej transpozycji. Weźmy pewną transpozycję $(a_1, a_2)$ permutacji $P$. Istnieje element $a_3$ taki, że w permutacji $Q$ występuje transpozycja $(a_2, a_3)$. Następnie znajdujemy transpozycję $(a_3, a_4)$ permutacji $P$, transpozycję $(a_4, a_5)$ permutacji $Q$ i tak dalej. Mamy zatem

$$P = (a_1, a_2)(a_3, a_4) \dots (a_{2m-1}, a_{2m})P',$$
$$Q = (a_2, a_3)(a_4, a_5) \dots (a_{2m-2}, a_{2m-1})(a_{2m}, a_1)Q'$$

dla pewnych permutacji $P'$ i $Q'$. Wówczas

$$PQ = (a_1, a_3, a_5, \dots, a_{2m-1})(a_{2m}, a_{2m-2}, \dots, a_6, a_4, a_2)P'Q'$$

i podobnie jak wyżej stwierdzamy, że złożenie $P'Q'$ ma żądaną własność. Tym razem doszły dwa cykle długości $m$, więc żądaną postać ma też permutacja $PQ$, c. b. d. o.

**Przykład.** Niech

$$P = (\mathtt{A}, \mathtt{J})(\mathtt{B}, \mathtt{E})(\mathtt{C}, \mathtt{H})(\mathtt{D}, \mathtt{F})(\mathtt{G}, \mathtt{K})(\mathtt{I}, \mathtt{L}),$$
$$Q = (\mathtt{J}, \mathtt{B})(\mathtt{E}, \mathtt{C})(\mathtt{H}, \mathtt{D})(\mathtt{F}, \mathtt{A})(\mathtt{K}, \mathtt{I})(\mathtt{L}, \mathtt{G}) = (\mathtt{A}, \mathtt{F})(\mathtt{B}, \mathtt{J})(\mathtt{C}, \mathtt{E})(\mathtt{D}, \mathtt{H})(\mathtt{G}, \mathtt{L})(\mathtt{I}, \mathtt{K}).$$

Wtedy

$$PQ = (\mathtt{A}, \mathtt{B}, \mathtt{C}, \mathtt{D})(\mathtt{F}, \mathtt{H}, \mathtt{E}, \mathtt{J})(\mathtt{G}, \mathtt{I})(\mathtt{L}, \mathtt{K}) = (\mathtt{A}, \mathtt{B}, \mathtt{C}, \mathtt{D})(\mathtt{E}, \mathtt{J}, \mathtt{F}, \mathtt{H})(\mathtt{G}, \mathtt{I})(\mathtt{K}, \mathtt{L}).$$

Prawdziwe jest też twierdzenie odwrotne:

**Twierdzenie 2.** Jeśli permutacja $R$ ma tę własność, że liczby cykli wszystkich długości są parzyste, to istnieją permutacje $P$ i $Q$ będące iloczynami rozłącznych transpozycji takie, że $PQ = R$.

**Dowód.** Przypuśćmy, że

$$R = (a_1, a_2, \dots, a_{m-1}, a_m)(b_1, b_2, \dots, b_{m-1}, b_m)R'$$

dla pewnej pemutacji $R'$. Możemy założyć (indukcja!), że $R' = P'Q'$ dla pewnych permutacji $P'$ i $Q'$ żądanej postaci. Przyjmijmy teraz

$$P = (a_1, b_m)(a_2, b_{m-1}) \dots (a_{m-1}, b_2)(a_m, b_1)P',$$
$$Q = (a_1, b_1)(a_2, b_m)(a_3, b_{m-1}) \dots (a_{m-1}, b_3)(a_m, b_2)Q'.$$

Nietrudno zauważyć, że wówczas $PQ = R$, c. b. d. o.

**Przykład.** Z dowodu twierdzenia 2 wynika, że permutację $P$ znajdujemy podpisując pod sobą cykle tej samej długości permutacji $R$, z tym tylko, że w dolnym wierszu odwracamy kolejność elementów cyklu. Permutację $Q$ otrzymujemy analogicznie, z tym tylko, że w dolnym wierszu elementy każdego cyklu przesuwamy o jedną pozycję w prawo. Permutacje te nie są zatem wyznaczone jednoznacznie. Mamy tyle rozwiązań, ile jest sposobów podpisania w ten sposób permutacji pod sobą. Zobaczmy, jak to wygląda w praktyce. Niech

$$R = (\mathtt{A}, \mathtt{B}, \mathtt{C}, \mathtt{D})(\mathtt{E}, \mathtt{J}, \mathtt{F}, \mathtt{H})(\mathtt{G}, \mathtt{I})(\mathtt{K}, \mathtt{L}).$$

Mamy 8 sposobów podpisania pod sobą cykli tej samej długości:

1) Z pierwszego sposobu podpisania

$$(\mathtt{A}, \mathtt{B}, \mathtt{C}, \mathtt{D})\ (\mathtt{G}, \mathtt{I})$$
$$(\mathtt{H}, \mathtt{F}, \mathtt{J}, \mathtt{E})\ (\mathtt{K}, \mathtt{L})$$

otrzymujemy najpierw permutację $P$:

$$P = (\mathtt{A}, \mathtt{H})(\mathtt{B}, \mathtt{F})(\mathtt{C}, \mathtt{J})(\mathtt{D}, \mathtt{E})(\mathtt{G}, \mathtt{K})(\mathtt{I}, \mathtt{L}),$$

a następnie przesuwając jak wyżej elementy cykli w dolnym wierszu:

$$(\mathtt{A}, \mathtt{B}, \mathtt{C}, \mathtt{D})(\mathtt{G}, \mathtt{I})$$
$$(\mathtt{E}, \mathtt{H}, \mathtt{F}, \mathtt{J})(\mathtt{L}, \mathtt{K})$$

otrzymujemy permutację $Q$:

$$Q = (\mathtt{A},\mathtt{E})(\mathtt{B},\mathtt{H})(\mathtt{C},\mathtt{F})(\mathtt{D},\mathtt{J})(\mathtt{G},\mathtt{L})(\mathtt{I},\mathtt{K}).$$

2) Możemy cykl długości 4 zapisać inaczej:

$$(\mathtt{A},\mathtt{B},\mathtt{C},\mathtt{D})\ (\mathtt{G},\mathtt{I})$$
$$(\mathtt{F},\mathtt{J},\mathtt{E},\mathtt{H})\ (\mathtt{K},\mathtt{L})$$

otrzymując permutacje:

$$P = (\mathtt{A},\mathtt{F})(\mathtt{B},\mathtt{J})(\mathtt{C},\mathtt{E})(\mathtt{D},\mathtt{H})(\mathtt{G},\mathtt{K})(\mathtt{I},\mathtt{L}),$$
$$Q = (\mathtt{A},\mathtt{H})(\mathtt{B},\mathtt{F})(\mathtt{C},\mathtt{J})(\mathtt{D},\mathtt{E})(\mathtt{G},\mathtt{L})(\mathtt{I},\mathtt{K}).$$

3) Możemy też zapisać odwrotnie cykl długości 2:

$$(\mathtt{A},\mathtt{B},\mathtt{C},\mathtt{D})\ (\mathtt{G},\mathtt{I})$$
$$(\mathtt{H},\mathtt{F},\mathtt{J},\mathtt{E})\ (\mathtt{L},\mathtt{K})$$

otrzymując tym razem następujące permutacje:

$$P = (\mathtt{A},\mathtt{H})(\mathtt{B},\mathtt{F})(\mathtt{C},\mathtt{J})(\mathtt{D},\mathtt{E})(\mathtt{G},\mathtt{L})(\mathtt{I},\mathtt{K}),$$
$$Q = (\mathtt{A},\mathtt{E})(\mathtt{B},\mathtt{H})(\mathtt{C},\mathtt{F})(\mathtt{D},\mathtt{J})(\mathtt{G},\mathtt{K})(\mathtt{I},\mathtt{L}).$$

4) Możemy wybrać drugi sposób zapisu cyklu długości 4 oraz zapisać odwrotnie cykl długości 2:

$$(\mathtt{A},\mathtt{B},\mathtt{C},\mathtt{D})\ (\mathtt{G},\mathtt{I})$$
$$(\mathtt{F},\mathtt{J},\mathtt{E},\mathtt{H})\ (\mathtt{L},\mathtt{K})$$

otrzymując permutacje:

$$P = (\mathtt{A},\mathtt{F})(\mathtt{B},\mathtt{J})(\mathtt{C},\mathtt{E})(\mathtt{D},\mathtt{H})(\mathtt{G},\mathtt{L})(\mathtt{I},\mathtt{K}),$$
$$Q = (\mathtt{A},\mathtt{H})(\mathtt{B},\mathtt{F})(\mathtt{C},\mathtt{J})(\mathtt{D},\mathtt{E})(\mathtt{G},\mathtt{K})(\mathtt{I},\mathtt{L}).$$

Wypisanie pozostałych czterech przypadków pozostawimy jako ćwiczenie (mamy jeszcze dwa sposoby podpisania pod sobą cykli długości 4 i do każdego z nich dwa pokazane wyżej sposoby podpisania cykli długości 2).

Przypuszczenie, że w *Enigmach* typu wojskowego każda permutacja odpowiadająca jednemu ustawieniu maszyny jest, podobnie jak w *Enigmach* typu handlowego, iloczynem rozłącznych transpozycji, uzyskało potwierdzenie. Ale czy można znaleźć same permutacje $A$, $B$, $C$, $D$, $E$ i $F$? Cykle permutacji $AD$ można podpisać pod sobą na 27 sposobów; cykle permutacji $BE$ i $CF$ na 13 sposobów. Łącznie dałoby to 4563 różne rozwiązania. Czy można wybrać z nich to jedyne właściwe?

Rejewski założył, że wielu szyfrantów będzie wybierać łatwe do zapamiętania klucze: trzy jednakowe litery, kolejne litery alfabetu, trzy kolejne klawisze na klawiaturze itp. Zobaczmy, co wynika z przypuszczenia, że najczęściej występująca szóstka liter `OPL XHP` odpowiada kluczowi `AAA`. Wówczas w permutacji $A$ litera `A` przechodzi na `O`, a w permutacji $D$ litera `O` przechodzi na `N`. Podpisujemy pod sobą cykle permutacji $A$:

```
(A,N,C,V,B,G,L,Q,Z)(D,S,H)(M)
(O,J,I,E,P,Y,W,K,X)(?,?,?)(R)
```

W drugim cyklu mamy trzy możliwości podpisania. Możemy spróbować wszystkich trzech możliwości i o wyborze właściwej zadecyduje ostateczny wynik. Okaże się, że właściwą kolejnością jest `(T,F,U)`. Zatem

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

i stąd dostajemy także

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

W permutacji $B$ litera `A` przechodzi na `P`. Podpisujemy pod sobą cykle permutacji $B$:

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

Permutacja $B$ ma zatem postać

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

i stąd dostajemy również permutację $E$:

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

Wreszcie w permutacji $C$ litera A przechodzi na L. Podpisujemy pod sobą cykle permutacji $C$:

(A,T,G,K,O,E,Z,M,B,Q,N,H,I)

(L,Y,C,V,F,W,U,D,R,X,S,J,P)

i dostajemy permutację $C$

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

oraz F:

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

Podsumowując:

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

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

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

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

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

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

O słuszności przyjętych hipotez przekonuje nas otrzymana z tych permutacji tabela kluczy depesz:

| Nr | klucz | Nr | klucz | Nr | klucz | Nr | klucz |
|---|---|---|---|---|---|---|---|
| 1. | OOO | 17. | CCC | 33. | ASD | 49. | FGH |
| 2. | OOO | 18. | CDE | 34. | ASD | 50. | DFG |
| 3. | PPP | 19. | NML | 35. | ABC | 51. | DDD |
| 4. | PPP | 20. | QQQ | 36. | ABC | 52. | DDD |
| 5. | PYX | 21. | QQQ | 37. | ABC | 53. | HJK |
| 6. | IKL | 22. | QAY | 38. | BNM | 54. | EEE |
| 7. | TZU | 23. | QWE | 39. | BBB | 55. | EEE |
| 8. | VBN | 24. | WER | 40. | BBB | 56. | ERT |
| 9. | SSS | 25. | RTZ | 41. | BBB | 57. | ERT |
| 10. | YYY | 26. | RFV | 42. | BBB | 58. | LLL |
| 11. | YYY | 27. | JJJ | 43. | KKK | 59. | LLL |
| 12. | UUU | 28. | AAA | 44. | KKK | 60. | ZUI |
| 13. | UVW | 29. | AAA | 45. | MMM | 61. | GHJ |
| 14. | UIO | 30. | AAA | 46. | MMM | 62. | GGG |
| 15. | CCC | 31. | AAA | 47. | FFF | 63. | XXX |
| 16. | CCC | 32. | AAA | 48. | FFF | 64. | XXX |

Oddajmy znów głos Rejewskiemu:

„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."

Dalej Rejewski pisze:

„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 $F$."

**Rekonstrukcja maszyny szyfrującej** *Enigma*

Drugą tajemnicą *Enigmy* były połączenia wewnętrzne bębenków. Zanim przyjrzymy się, w jaki sposób Rejewski odnalazł te połączenia, przyjrzymy się postaci permutacji sprzężonej oraz rozwiązaniom pewnych równań i układów równań, w których niewiadomymi są permutacje.

**Definicja.** Permutacje $P$ i $Q$ nazywamy **podobnymi**, jeśli mają tyle samo cykli każdej długości. Na przykład, permutacje

$$P = (\mathtt{A},\mathtt{C},\mathtt{G},\mathtt{I},\mathtt{K})(\mathtt{B},\mathtt{H},\mathtt{J},\mathtt{L})(\mathtt{D},\mathtt{F})(\mathtt{E})$$

oraz

$$Q = (\mathtt{A},\mathtt{F},\mathtt{I},\mathtt{K})(\mathtt{B},\mathtt{E},\mathtt{G},\mathtt{C},\mathtt{L})(\mathtt{D},\mathtt{J})(\mathtt{H})$$

są podobne: obie mają po jednym cyklu długości 5, 4, 2 i 1.

**Definicja.** Dla danych permutacji $P$ i $X$ permutację $Q = X^{-1}PX$ nazywamy permutacją **sprzężoną** z permutacją $X$.

**Twierdzenie 3.** Permutacja sprzężona z daną permutacją jest do niej podobna. Odwrotnie, każde dwie permutacje podobne są sprzężone.

Zamiast prostego dowodu pokażemy jeden przykład.

**Przykład.** Dane są permutacje

$$P = (\mathtt{A},\mathtt{C},\mathtt{G},\mathtt{I},\mathtt{K})(\mathtt{B},\mathtt{H},\mathtt{J},\mathtt{L})(\mathtt{D},\mathtt{F})(\mathtt{E})$$

oraz

$$X = (\mathtt{A},\mathtt{B},\mathtt{F},\mathtt{J},\mathtt{K},\mathtt{L})(\mathtt{C},\mathtt{E},\mathtt{H},\mathtt{I})(\mathtt{D})(\mathtt{G}).$$

Rozkład permutacji $Q = X^{-1}PX$ na cykle otrzymujemy w następujący sposób. Permutację $X$ zapisujemy w postaci

$$X = \begin{pmatrix} \mathtt{A} & \mathtt{B} & \mathtt{C} & \mathtt{D} & \mathtt{E} & \mathtt{F} & \mathtt{G} & \mathtt{H} & \mathtt{I} & \mathtt{J} & \mathtt{K} & \mathtt{L} \\ \mathtt{B} & \mathtt{F} & \mathtt{E} & \mathtt{D} & \mathtt{H} & \mathtt{J} & \mathtt{G} & \mathtt{I} & \mathtt{C} & \mathtt{K} & \mathtt{L} & \mathtt{A} \end{pmatrix}$$
$$= \begin{pmatrix} \mathtt{A} & \mathtt{C} & \mathtt{G} & \mathtt{I} & \mathtt{K} & \mathtt{B} & \mathtt{H} & \mathtt{J} & \mathtt{L} & \mathtt{D} & \mathtt{F} & \mathtt{E} \\ \mathtt{B} & \mathtt{E} & \mathtt{G} & \mathtt{C} & \mathtt{L} & \mathtt{F} & \mathtt{I} & \mathtt{K} & \mathtt{A} & \mathtt{D} & \mathtt{J} & \mathtt{H} \end{pmatrix}.$$

Teraz dostajemy:

$$Q = (\mathtt{B},\mathtt{E},\mathtt{G},\mathtt{C},\mathtt{L})(\mathtt{F},\mathtt{I},\mathtt{K},\mathtt{A})(\mathtt{D},\mathtt{J})(\mathtt{H}),$$

czyli

$$Q = (\mathtt{A},\mathtt{F},\mathtt{I},\mathtt{K})(\mathtt{B},\mathtt{E},\mathtt{G},\mathtt{C},\mathtt{L})(\mathtt{D},\mathtt{J})(\mathtt{H}).$$

Inaczej mówiąc, w każdym cyklu permutacji $P$ kolejne elementy zastępujemy elementami, na które przeprowadza je permutacja $X$ (a potem ewentualnie porządkujemy cykle). Korzystając z tej reguły możemy znaleźć nieznaną permutację $X$. Mianowicie podpisujemy pod sobą permutacje $P$ i $Q$ z zachowaniem długości cykli

$$P = (\mathtt{A},\mathtt{C},\mathtt{G},\mathtt{I},\mathtt{K})(\mathtt{B},\mathtt{H},\mathtt{J},\mathtt{L})(\mathtt{D},\mathtt{F})(\mathtt{E})$$
$$Q = (\mathtt{B},\mathtt{E},\mathtt{G},\mathtt{C},\mathtt{L})(\mathtt{A},\mathtt{F},\mathtt{I},\mathtt{K})(\mathtt{D},\mathtt{J})(\mathtt{H})$$

i znajdujemy jedną z możliwych permutacji $X$:

$$X = \begin{pmatrix} \mathtt{A} & \mathtt{C} & \mathtt{G} & \mathtt{I} & \mathtt{K} & \mathtt{B} & \mathtt{H} & \mathtt{J} & \mathtt{L} & \mathtt{D} & \mathtt{F} & \mathtt{E} \\ \mathtt{B} & \mathtt{E} & \mathtt{G} & \mathtt{C} & \mathtt{L} & \mathtt{A} & \mathtt{F} & \mathtt{I} & \mathtt{K} & \mathtt{D} & \mathtt{J} & \mathtt{H} \end{pmatrix} =$$
$$= (\mathtt{A},\mathtt{B})(\mathtt{C},\mathtt{E},\mathtt{H},\mathtt{F},\mathtt{J},\mathtt{I})(\mathtt{D})(\mathtt{G})(\mathtt{K},\mathtt{L}).$$

Naszą wyjściową permutację $X$ otrzymujemy podpisując permutacje $P$ i $Q$ w następujący sposób:

$$P = (\mathtt{A},\mathtt{C},\mathtt{G},\mathtt{I},\mathtt{K})(\mathtt{B},\mathtt{H},\mathtt{J},\mathtt{L})(\mathtt{D},\mathtt{F})(\mathtt{E})$$
$$Q = (\mathtt{B},\mathtt{E},\mathtt{G},\mathtt{C},\mathtt{L})(\mathtt{F},\mathtt{I},\mathtt{K},\mathtt{A})(\mathtt{D},\mathtt{J})(\mathtt{H}).$$

W naszym przykładzie istnieje 5 sposobów podpisania pod sobą cykli długości 5, 4 sposoby podpisania cykli długości 4 i 2 sposoby podpisania cykli długości 2. Stąd wynika, że równanie $Q = X^{-1}PX$ z niewiadomą permutacją $X$ ma $5 \cdot 4 \cdot 2 = 40$ rozwiązań.

**Przykład.** W podobny sposób rozwiązujemy układy równań postaci

$$\begin{cases} Q = X^{-1}PX, \\ R = X^{-1}QX, \end{cases}$$

gdzie $P$, $Q$ i $R$ są danymi permutacjami podobnymi (wspólną niewiadomą jest permutacja $X$). Jeden sposób polega na tym, by na wszystkie możliwe sposoby podpisać pod sobą permutacje $P$ i $Q$, a następnie permutacje $Q$ i $R$, i wybrać te sposoby, które dają w wyniku tę samą permutację $X$. Nieco inny sposób, wykorzystujący specjalną postać permutacji $P$, $Q$ i $R$, zobaczymy poniżej. Mamy dane permutacje podobne

$$P = (\mathtt{A},\mathtt{C},\mathtt{G},\mathtt{I},\mathtt{K})(\mathtt{B},\mathtt{H},\mathtt{J},\mathtt{L})(\mathtt{D},\mathtt{F})(\mathtt{E}),$$
$$Q = (\mathtt{A},\mathtt{F},\mathtt{I},\mathtt{K})(\mathtt{B},\mathtt{E},\mathtt{G},\mathtt{C},\mathtt{L})(\mathtt{D},\mathtt{J})(\mathtt{H}),$$
$$R = (\mathtt{A},\mathtt{F},\mathtt{H},\mathtt{G},\mathtt{E})(\mathtt{B},\mathtt{H},\mathtt{J},\mathtt{L})(\mathtt{D},\mathtt{K})(\mathtt{I}).$$

Podpisujemy je w następujący sposób:

$$P = (\mathtt{A},\mathtt{C},\mathtt{G},\mathtt{I},\mathtt{K})(\mathtt{B},\mathtt{H},\mathtt{J},\mathtt{L})(\mathtt{D},\mathtt{F})(\mathtt{E}),$$
$$Q = (\ ,\ ,\ ,\ ,\ )(\ ,\ ,\ ,\ )(\ ,\ )(\mathtt{H}),$$
$$R = (\ ,\ ,\ ,\ ,\ )(\ ,\ ,\ ,\ )(\ ,\ )(\mathtt{I}).$$

Widzimy zatem, że permutacja $X$ przeprowadza $\mathtt{E}$ na $\mathtt{H}$ oraz $\mathtt{H}$ na $\mathtt{I}$. Wykorzystamy teraz drugą z tych informacji do podpisania permutacji $P$ i $Q$:

$$P = (\mathtt{A},\mathtt{C},\mathtt{G},\mathtt{I},\mathtt{K})(\mathtt{B},\mathtt{H},\mathtt{J},\mathtt{L})(\mathtt{D},\mathtt{F})(\mathtt{E}),$$
$$Q = (\ ,\ ,\ ,\ ,\ )(\mathtt{F},\mathtt{I},\mathtt{K},\mathtt{A})(\ ,\ )(\mathtt{H}).$$

Otrzymaliśmy trzy nowe informacje o permutacji $X$: $\mathtt{B} \to \mathtt{F}$, $\mathtt{J} \to \mathtt{K}$ oraz $\mathtt{L} \to \mathtt{A}$. Wykorzystamy teraz wszystkie dotychczas otrzymane informacje do podpisania permutacji $Q$ i $R$:

$$Q = (\mathtt{B},\mathtt{E},\mathtt{G},\mathtt{C},\mathtt{L})(\mathtt{F},\mathtt{I},\mathtt{K},\mathtt{A})(\mathtt{D},\mathtt{J})(\mathtt{H}),$$
$$R = (\mathtt{F},\mathtt{H},\mathtt{G},\mathtt{E},\mathtt{A})(\ ,\ ,\ ,\ )(\mathtt{D},\mathtt{K})(\mathtt{I}).$$

Otrzymaliśmy trzy nowe informacje: $\mathtt{G} \to \mathtt{G}$, $\mathtt{C} \to \mathtt{E}$ oraz $\mathtt{D} \to \mathtt{D}$. Pozwalają one w całości podpisać pod sobą permutacje $P$ i $Q$:

$$P = (\mathtt{A},\mathtt{C},\mathtt{G},\mathtt{I},\mathtt{K})(\mathtt{B},\mathtt{H},\mathtt{J},\mathtt{L})(\mathtt{D},\mathtt{F})(\mathtt{E}),$$
$$Q = (\mathtt{B},\mathtt{E},\mathtt{G},\mathtt{C},\mathtt{L})(\mathtt{F},\mathtt{I},\mathtt{K},\mathtt{A})(\mathtt{D},\mathtt{J})(\mathtt{H}).$$

To już wyznacza w całości permutację $X$ i wystarczy sprawdzić, że spełnia ona także drugie równanie.

W dalszym ciągu potrzebna będzie permutacja przeprowadzająca każdą literę na następną w alfabecie (odpowiadająca obrotowi prawego bębenka o jedną pozycję), a także kilka jej iteracji:

$$Q = (\mathtt{A},\mathtt{B},\mathtt{C},\mathtt{D},\mathtt{E},\mathtt{F},\mathtt{G},\mathtt{H},\mathtt{I},\mathtt{J},\mathtt{K},\mathtt{L},\mathtt{M},\mathtt{N},\mathtt{O},\mathtt{P},\mathtt{Q},\mathtt{R},\mathtt{S},\mathtt{T},\mathtt{U},\mathtt{V},\mathtt{W},\mathtt{X},\mathtt{Y},\mathtt{Z})$$
$$Q^2 = (\mathtt{A},\mathtt{C},\mathtt{E},\mathtt{G},\mathtt{I},\mathtt{K},\mathtt{M},\mathtt{O},\mathtt{Q},\mathtt{S},\mathtt{U},\mathtt{W},\mathtt{Y})(\mathtt{B},\mathtt{D},\mathtt{F},\mathtt{H},\mathtt{J},\mathtt{L},\mathtt{N},\mathtt{P},\mathtt{R},\mathtt{T},\mathtt{V},\mathtt{X},\mathtt{Z})$$
$$Q^3 = (\mathtt{A},\mathtt{D},\mathtt{G},\mathtt{J},\mathtt{M},\mathtt{P},\mathtt{S},\mathtt{V},\mathtt{Y},\mathtt{B},\mathtt{E},\mathtt{H},\mathtt{K},\mathtt{N},\mathtt{Q},\mathtt{T},\mathtt{W},\mathtt{Z},\mathtt{C},\mathtt{F},\mathtt{I},\mathtt{L},\mathtt{O},\mathtt{R},\mathtt{U},\mathtt{X})$$
$$Q^4 = (\mathtt{A},\mathtt{E},\mathtt{I},\mathtt{M},\mathtt{Q},\mathtt{U},\mathtt{Y},\mathtt{C},\mathtt{G},\mathtt{K},\mathtt{O},\mathtt{S},\mathtt{W})(\mathtt{B},\mathtt{F},\mathtt{J},\mathtt{N},\mathtt{R},\mathtt{V},\mathtt{Z},\mathtt{D},\mathtt{H},\mathtt{L},\mathtt{P},\mathtt{T},\mathtt{X})$$
$$Q^5 = (\mathtt{A},\mathtt{F},\mathtt{K},\mathtt{P},\mathtt{U},\mathtt{Z},\mathtt{E},\mathtt{J},\mathtt{O},\mathtt{T},\mathtt{Y},\mathtt{D},\mathtt{I},\mathtt{N},\mathtt{S},\mathtt{X},\mathtt{C},\mathtt{H},\mathtt{M},\mathtt{R},\mathtt{W},\mathtt{B},\mathtt{G},\mathtt{L},\mathtt{Q},\mathtt{V})$$
$$Q^7 = (\mathtt{A},\mathtt{H},\mathtt{O},\mathtt{V},\mathtt{C},\mathtt{J},\mathtt{Q},\mathtt{X},\mathtt{E},\mathtt{L},\mathtt{S},\mathtt{Z},\mathtt{G},\mathtt{N},\mathtt{U},\mathtt{B},\mathtt{I},\mathtt{P},\mathtt{W},\mathtt{D},\mathtt{K},\mathtt{R},\mathtt{Y},\mathtt{F},\mathtt{M},\mathtt{T})$$

Literą $S$ oznaczymy permutację związaną z łącznicą wtyczkową:

$$S = \mathtt{(A,S)(E,Z)(G,L)(P,R)(X,T)(Y,V)}.$$

Następnie literami $L$, $M$ i $R$ oznaczymy permutacje związane z trzema ruchomymi bębenkami: lewym, środkowym i prawym. Literą $H$ oznaczymy

permutację bębenka wstępnego, a literą $T$ permutację bębenka odwracającego. Do opisu permutacji szyfrowania w dowolnym ustawieniu parametrów *Enigmy* potrzebne będą jeszcze liczby określające usytuowanie pierścieni i pierwotne pozycje bębenków.

Dla dowolnej litery $\alpha$ niech $n(\alpha)$ oznacza numer tej litery w alfabecie pomniejszony o 1. Na przykład:

$$n(\mathtt{A}) = 0,\ n(\mathtt{B}) = 1,\ n(\mathtt{C}) = 2, \ldots$$

Jeśli $\alpha$ oznacza usytuowanie pierścienia, a $\beta$ pierwotną pozycję bębenka, to liczba $(n(\beta) - n(\alpha)) \bmod 26$ określa skręcenie bębenka w stosunku do pewnej ustalonej pozycji, tzw. „pozycji zerowej". Przyjmijmy oznaczenia: $x$ będzie skręceniem bębenka lewego, $y$ bębenka środkowego i $z$ skręceniem bębenka prawego (dokładniej: liczbę $z$ otrzymujemy dodając 1 modulo 26 do skręcenia bębenka prawego; jest to związane z tym, że po naciśnięciu klawisza najpierw bębenek prawy obraca się o jedną pozycję i dopiero po tym obrocie następuje szyfrowanie). Permutacje wyznaczone przez obrócone bębenki, lewy środkowy i prawy, mają więc postać:

$$L_x = Q^x L Q^{-x}, \quad M_y = Q^y M Q^{-y}, \quad R_z = Q^z R Q^{-z}.$$

Zauważmy, że wtedy

$$L_x^{-1} = Q^x L^{-1} Q^{-x}, \quad M_y^{-1} = Q^y M^{-1} Q^{-y}, \quad R_z^{-1} = Q^z R^{-1} Q^{-z}.$$

Możemy teraz opisać permutacje od $A$ do $F$, przy założeniu, że w czasie szyfrowania pierwszych sześciu liter obracał się tylko prawy bębenek:

$$\begin{aligned}
A &= SH\ \ R_z\ \ M_y L_x T L_x^{-1} M_y^{-1}\ \ R_z^{-1}\ \ H^{-1}S^{-1},\\
B &= SHQ\ \ R_z^{-1}Q^{-1} M_y L_x T L_x^{-1} M_y^{-1} Q\ \ R_z^{-1}Q^{-1}H^{-1}S^{-1},\\
C &= SHQ^2 R_z^{-1}Q^{-2} M_y L_x T L_x^{-1} M_y^{-1} Q^2 R_z^{-1}Q^{-2}H^{-1}S^{-1},\\
D &= SHQ^3 R_z^{-1}Q^{-3} M_y L_x T L_x^{-1} M_y^{-1} Q^3 R_z^{-1}Q^{-3}H^{-1}S^{-1},\\
E &= SHQ^4 R_z^{-1}Q^{-4} M_y L_x T L_x^{-1} M_y^{-1} Q^4 R_z^{-1}Q^{-4}H^{-1}S^{-1},\\
F &= SHQ^5 R_z^{-1}Q^{-5} M_y L_x T L_x^{-1} M_y^{-1} Q^5 R_z^{-1}Q^{-5}H^{-1}S^{-1},
\end{aligned}$$

Oznaczmy wreszcie literą $P$ permutację $M_y L_x T L_x^{-1} M_y^{-1}$. Powyższe równania przyjmą postać

$$\begin{aligned}
A &= SH\ \ R_z\ \ P\ \ R_z^{-1}\ \ H^{-1}S^{-1},\\
B &= SHQ\ \ R_z^{-1}Q^{-1} P Q\ \ R_z^{-1}Q^{-1}H^{-1}S^{-1},\\
C &= SHQ^2 R_z^{-1}Q^{-2} P Q^2 R_z^{-1}Q^{-2}H^{-1}S^{-1},\\
D &= SHQ^3 R_z^{-1}Q^{-3} P Q^3 R_z^{-1}Q^{-3}H^{-1}S^{-1},\\
E &= SHQ^4 R_z^{-1}Q^{-4} P Q^4 R_z^{-1}Q^{-4}H^{-1}S^{-1},\\
F &= SHQ^5 R_z^{-1}Q^{-5} P Q^5 R_z^{-1}Q^{-5}H^{-1}S^{-1},
\end{aligned}$$

Ponieważ permutacje od $A$ do $F$ są znane, więc mamy tu do czynienia z układem sześciu równań z czterema niewiadomymi: permutacjami $S$, $H$, $R_z$ i $P$. Ten układ ma oczywiście rozwiązanie, jednak znalezienie go może w praktyce okazać się niemożliwe.

Pomógł przypadek. Wywiad francuski dostarczył Rejewskiemu tablicę kluczy dziennych za dwa miesiące: wrzesień i październik 1932 roku. To pozwoliło poznać permutację $S$. Wprawdzie w tablicy kluczy dziennych podane były skręcenia bębenków, lecz wobec tego, że nieznane było położenie „pozycji zerowej", więc liczby $x$, $y$ i $z$ też nie były znane. Poznanie ich można było jednak odłożyć na później. Następnie Rejewski przyjął hipotezę, że permutacja $H$ jest taka sama jak w maszynach typu handlowego. Zatem niewiadomymi okazały się tylko permutacje $R_z$ i $P$. Ważniejsze było poznanie permutacji $R_z$, gdyż zdradzała ona wewnętrzne połączenia bębenka prawego.

Przyjmijmy teraz oznaczenia:

$$\begin{aligned}
U &= \ \ H^{-1}S^{-1}ASH\ \ ,\\
V &= Q^{-1}H^{-1}S^{-1}BSHQ\ ,\\
W &= Q^{-2}H^{-1}S^{-1}CSHQ^2,
\end{aligned}$$

$$X = Q^{-3}H^{-1}S^{-1}DSHQ^3,$$
$$Y = Q^{-4}H^{-1}S^{-1}ESHQ^4,$$
$$Z = Q^{-5}H^{-1}S^{-1}FSHQ^5.$$

Ponieważ po prawej stronie każdej z tych równości występują wyłącznie znane permutacje, więc Rejewski mógł wyznaczyć te sześć permutacji. Mamy teraz układ równań:

$$U = R_z \quad P \quad R_z^{-1},$$
$$V = R_zQ^{-1}PQ \; R_z^{-1},$$
$$W = R_zQ^{-2}PQ^2R_z^{-1},$$
$$X = R_zQ^{-3}PQ^3R_z^{-1},$$
$$Y = R_zQ^{-4}PQ^4R_z^{-1},$$
$$Z = R_zQ^{-5}PQ^5R_z^{-1}.$$

Następnie mnożymy stronami każde równanie przez następne:

$$UV = R_z \quad (PQ^{-1}PQ) \quad R_z^{-1},$$
$$VW = R_zQ^{-1}(PQ^{-1}PQ)Q \; R_z^{-1},$$
$$WX = R_zQ^{-2}(PQ^{-1}PQ)Q^2R_z^{-1},$$
$$XY = R_zQ^{-3}(PQ^{-1}PQ)Q^3R_z^{-1},$$
$$YZ = R_zQ^{-4}(PQ^{-1}PQ)Q^4R_z^{-1}.$$

Możemy teraz wyeliminować wyrażenie w nawiasie (a więc wyeliminować niewiadomą permutację $P$):

$$VW = (R_zQR_z^{-1})^{-1}U\ V\ (R_zQR_z^{-1}),$$
$$WX = (R_zQR_z^{-1})^{-1}V\ W(R_zQR_z^{-1}),$$
$$XY = (R_zQR_z^{-1})^{-1}WX\ (R_zQR_z^{-1}),$$
$$YZ = (R_zQR_z^{-1})^{-1}X\,Y\ (R_zQR_z^{-1}).$$

Taki układ równań umiemy już rozwiązywać. Wystarczą nawet tylko pierwsze dwa równania, dwa następne będą tylko służyć do sprawdzenia rozwiązania. Ponieważ niewiadoma permutacja $R_zQR_z^{-1}$ jest permutacją sprzężoną do permutacji $Q$, więc ma tylko jeden cykl. Musimy więc szukać rozwiązania tej postaci.

Spróbujmy zatem znaleźć takie rozwiązanie. Najpierw musimy wyznaczyć permutacje $U$, $V$, $W$, $X$, $Y$ i $Z$. Permutacja $S$ jest znana z tablicy kluczy dziennych. Permutacja $H$ pochodzi z maszyny handlowej. Tam miała ona następującą postać:

$$H = \begin{pmatrix} \mathtt{Q} & \mathtt{W} & \mathtt{E} & \mathtt{R} & \mathtt{T} & \mathtt{Z} & \mathtt{U} & \mathtt{I} & \mathtt{O} & \mathtt{A} & \mathtt{S} & \mathtt{D} & \mathtt{F} & \mathtt{G} & \mathtt{H} & \mathtt{J} & \mathtt{K} & \mathtt{P} & \mathtt{Y} & \mathtt{X} & \mathtt{C} & \mathtt{V} & \mathtt{B} & \mathtt{N} & \mathtt{M} & \mathtt{L} \\ \mathtt{A} & \mathtt{B} & \mathtt{C} & \mathtt{D} & \mathtt{E} & \mathtt{F} & \mathtt{G} & \mathtt{H} & \mathtt{I} & \mathtt{J} & \mathtt{K} & \mathtt{L} & \mathtt{M} & \mathtt{N} & \mathtt{O} & \mathtt{P} & \mathtt{Q} & \mathtt{R} & \mathtt{S} & \mathtt{T} & \mathtt{U} & \mathtt{V} & \mathtt{W} & \mathtt{X} & \mathtt{Y} & \mathtt{Z} \end{pmatrix}$$
$$= (\mathtt{A},\mathtt{J},\mathtt{P},\mathtt{R},\mathtt{D},\mathtt{L},\mathtt{Z},\mathtt{F},\mathtt{M},\mathtt{Y},\mathtt{S},\mathtt{K},\mathtt{Q})(\mathtt{B},\mathtt{W})(\mathtt{C},\mathtt{U},\mathtt{G},\mathtt{N},\mathtt{X},\mathtt{T},\mathtt{E})(\mathtt{H},\mathtt{O},\mathtt{I})(\mathtt{V}).$$

Nietrudne obliczenia dają:

$$U = (\mathtt{A},\mathtt{Q})(\mathtt{B},\mathtt{N})(\mathtt{C},\mathtt{E})(\mathtt{D},\mathtt{W})(\mathtt{F},\mathtt{S})(\mathtt{G},\mathtt{O})(\mathtt{H},\mathtt{U})(\mathtt{I},\mathtt{K})(\mathtt{J},\mathtt{M})(\mathtt{L},\mathtt{T})(\mathtt{P},\mathtt{X})(\mathtt{R},\mathtt{Y})(\mathtt{V},\mathtt{Z}),$$
$$V = (\mathtt{A},\mathtt{W})(\mathtt{B},\mathtt{Q})(\mathtt{C},\mathtt{F})(\mathtt{D},\mathtt{M})(\mathtt{E},\mathtt{L})(\mathtt{G},\mathtt{V})(\mathtt{H},\mathtt{P})(\mathtt{I},\mathtt{T})(\mathtt{J},\mathtt{R})(\mathtt{K},\mathtt{S})(\mathtt{N},\mathtt{O})(\mathtt{U},\mathtt{X})(\mathtt{Y},\mathtt{Z}),$$
$$W = (\mathtt{A},\mathtt{N})(\mathtt{B},\mathtt{W})(\mathtt{C},\mathtt{G})(\mathtt{D},\mathtt{H})(\mathtt{E},\mathtt{I})(\mathtt{F},\mathtt{J})(\mathtt{K},\mathtt{O})(\mathtt{L},\mathtt{Z})(\mathtt{M},\mathtt{P})(\mathtt{Q},\mathtt{R})(\mathtt{S},\mathtt{U})(\mathtt{T},\mathtt{Y})(\mathtt{V},\mathtt{X}).$$

Dalsze obliczenia są niepotrzebne, gdyż okazuje się, że permutacje

$$UV = (\mathtt{A},\mathtt{B},\mathtt{O},\mathtt{V},\mathtt{Y},\mathtt{J},\mathtt{D})(\mathtt{C},\mathtt{L},\mathtt{I},\mathtt{S})(\mathtt{E},\mathtt{F},\mathtt{K},\mathtt{T})(\mathtt{G},\mathtt{N},\mathtt{Q},\mathtt{W},\mathtt{M},\mathtt{R},\mathtt{Z})(\mathtt{H},\mathtt{X})(\mathtt{P},\mathtt{U})$$

oraz

$$VW = (\mathtt{A},\mathtt{B},\mathtt{R},\mathtt{F},\mathtt{G},\mathtt{X},\mathtt{S},\mathtt{O})(\mathtt{C},\mathtt{J},\mathtt{Q},\mathtt{W},\mathtt{N},\mathtt{K},\mathtt{U},\mathtt{V})(\mathtt{D},\mathtt{P})(\mathtt{E},\mathtt{Z},\mathtt{T})(\mathtt{H},\mathtt{M})(\mathtt{I},\mathtt{Y},\mathtt{L})$$

nie są podobne. Zatem rozwiązanie nie istnieje. Gdzieś w rozumowaniu tkwił błąd. Rejewski dość szybko zrozumiał, gdzie błąd popełnił: przyjął, że znana jest permutacja $H$. W maszynie typu wojskowego musiał być zainstalowany inny bębenek wstępny. Rejewski po prostu odgadł jaki. Przyjął rozwiązanie najprostsze: permutacja $H$ jest identycznościowa. Przeprowadźmy jeszcze raz potrzebne obliczenia:

$$U = (\mathtt{A},\mathtt{F})(\mathtt{B},\mathtt{R})(\mathtt{C},\mathtt{I})(\mathtt{D},\mathtt{X})(\mathtt{E},\mathtt{T})(\mathtt{G},\mathtt{W})(\mathtt{H},\mathtt{U})(\mathtt{J},\mathtt{N})(\mathtt{K},\mathtt{Q})(\mathtt{L},\mathtt{V})(\mathtt{M},\mathtt{P})(\mathtt{O},\mathtt{S})(\mathtt{Y},\mathtt{Z}),$$
$$V = (\mathtt{A},\mathtt{D})(\mathtt{B},\mathtt{Q})(\mathtt{C},\mathtt{Y})(\mathtt{E},\mathtt{F})(\mathtt{G},\mathtt{H})(\mathtt{I},\mathtt{V})(\mathtt{J},\mathtt{Z})(\mathtt{K},\mathtt{R})(\mathtt{L},\mathtt{P})(\mathtt{M},\mathtt{W})(\mathtt{N},\mathtt{O})(\mathtt{S},\mathtt{T})(\mathtt{U},\mathtt{X}),$$
$$W = (\mathtt{A},\mathtt{M})(\mathtt{B},\mathtt{Y})(\mathtt{C},\mathtt{P})(\mathtt{D},\mathtt{R})(\mathtt{E},\mathtt{N})(\mathtt{F},\mathtt{O})(\mathtt{G},\mathtt{W})(\mathtt{H},\mathtt{Q})(\mathtt{I},\mathtt{U})(\mathtt{J},\mathtt{L})(\mathtt{K},\mathtt{T})(\mathtt{S},\mathtt{V})(\mathtt{X},\mathtt{Z}),$$
$$X = (\mathtt{A},\mathtt{D})(\mathtt{B},\mathtt{L})(\mathtt{C},\mathtt{E})(\mathtt{F},\mathtt{M})(\mathtt{G},\mathtt{X})(\mathtt{H},\mathtt{N})(\mathtt{I},\mathtt{K})(\mathtt{J},\mathtt{Y})(\mathtt{O},\mathtt{U})(\mathtt{P},\mathtt{S})(\mathtt{Q},\mathtt{R})(\mathtt{T},\mathtt{Z})(\mathtt{V},\mathtt{W}),$$
$$Y = (\mathtt{A},\mathtt{G})(\mathtt{B},\mathtt{R})(\mathtt{C},\mathtt{X})(\mathtt{D},\mathtt{S})(\mathtt{E},\mathtt{V})(\mathtt{F},\mathtt{N})(\mathtt{H},\mathtt{Q})(\mathtt{I},\mathtt{Y})(\mathtt{J},\mathtt{M})(\mathtt{K},\mathtt{P})(\mathtt{L},\mathtt{W})(\mathtt{O},\mathtt{T})(\mathtt{U},\mathtt{Z}),$$
$$Z = (\mathtt{A},\mathtt{Q})(\mathtt{B},\mathtt{J})(\mathtt{C},\mathtt{L})(\mathtt{D},\mathtt{T})(\mathtt{E},\mathtt{K})(\mathtt{F},\mathtt{M})(\mathtt{G},\mathtt{I})(\mathtt{H},\mathtt{P})(\mathtt{N},\mathtt{O})(\mathtt{R},\mathtt{Z})(\mathtt{S},\mathtt{Y})(\mathtt{U},\mathtt{V})(\mathtt{W},\mathtt{X}).$$

Następnie

$$UV = (\mathtt{A},\mathtt{E},\mathtt{S},\mathtt{N},\mathtt{Z},\mathtt{C},\mathtt{V},\mathtt{P},\mathtt{W},\mathtt{H},\mathtt{X})(\mathtt{B},\mathtt{K})(\mathtt{D},\mathtt{U},\mathtt{G},\mathtt{M},\mathtt{L},\mathtt{I},\mathtt{Y},\mathtt{J},\mathtt{O},\mathtt{T},\mathtt{F})(\mathtt{Q},\mathtt{R}),$$
$$VW = (\mathtt{A},\mathtt{R},\mathtt{T},\mathtt{V},\mathtt{U},\mathtt{Z},\mathtt{L},\mathtt{C},\mathtt{B},\mathtt{H},\mathtt{W})(\mathtt{D},\mathtt{M},\mathtt{G},\mathtt{Q},\mathtt{Y},\mathtt{P},\mathtt{J},\mathtt{X},\mathtt{I},\mathtt{S},\mathtt{K})(\mathtt{E},\mathtt{O})(\mathtt{F},\mathtt{N}),$$
$$WX = (\mathtt{A},\mathtt{F},\mathtt{U},\mathtt{K},\mathtt{Z},\mathtt{G},\mathtt{V},\mathtt{P},\mathtt{E},\mathtt{H},\mathtt{R})(\mathtt{B},\mathtt{J})(\mathtt{C},\mathtt{S},\mathtt{W},\mathtt{X},\mathtt{T},\mathtt{I},\mathtt{O},\mathtt{M},\mathtt{D},\mathtt{Q},\mathtt{N})(\mathtt{L},\mathtt{Y}),$$
$$XY = (\mathtt{A},\mathtt{S},\mathtt{K},\mathtt{Y},\mathtt{M},\mathtt{N},\mathtt{Q},\mathtt{B},\mathtt{W},\mathtt{E},\mathtt{X})(\mathtt{C},\mathtt{V},\mathtt{L},\mathtt{R},\mathtt{H},\mathtt{F},\mathtt{J},\mathtt{I},\mathtt{P},\mathtt{D},\mathtt{G})(\mathtt{O},\mathtt{Z})(\mathtt{T},\mathtt{U}),$$
$$YZ = (\mathtt{A},\mathtt{I},\mathtt{S},\mathtt{T},\mathtt{N},\mathtt{M},\mathtt{B},\mathtt{Z},\mathtt{V},\mathtt{K},\mathtt{H})(\mathtt{C},\mathtt{W})(\mathtt{D},\mathtt{Y},\mathtt{G},\mathtt{Q},\mathtt{P},\mathtt{E},\mathtt{U},\mathtt{R},\mathtt{J},\mathtt{F},\mathtt{O})(\mathtt{L},\mathtt{X}).$$

Permutacje te są podobne, więc możemy spróbować podpisać je pod sobą w taki sposób, by permutacja przeprowadzająca je na siebie miała jeden cykl 26-literowy. Nad cyklem $(\mathtt{E},\mathtt{O})$ permutacji $VW$ możemy napisać cztery cykle: $(\mathtt{Q},\mathtt{R})$, $(\mathtt{R},\mathtt{Q})$, $(\mathtt{B},\mathtt{K})$ i $(\mathtt{K},\mathtt{B})$. Każda z tych możliwości wymusza pewien sposób podpisania długich cykli permutacji $WX$ pod permutacją $VW$. Popatrzmy na te możliwości. Oto pierwsza z nich:

$$UV = (\mathtt{Q},\mathtt{R})$$
$$VW = (\mathtt{E},\mathtt{O})(\mathtt{F},\mathtt{N})(\mathtt{A},\mathtt{R},\mathtt{T},\mathtt{V},\mathtt{U},\mathtt{Z},\mathtt{L},\mathtt{C},\mathtt{B},\mathtt{H},\mathtt{W})(\mathtt{D},\mathtt{M},\mathtt{G},\mathtt{Q},\mathtt{Y},\mathtt{P},\mathtt{J},\mathtt{X},\mathtt{I},\mathtt{S},\mathtt{K})$$
$$WX = (\ ,\ )(\ ,\ )(\mathtt{I},\mathtt{O},\mathtt{M},\mathtt{D},\mathtt{Q},\mathtt{N},\mathtt{C},\mathtt{S},\mathtt{W},\mathtt{X},\mathtt{T})(\mathtt{G},\mathtt{V},\mathtt{P},\mathtt{E},\mathtt{H},\mathtt{R},\mathtt{A},\mathtt{F},\mathtt{U},\mathtt{K},\mathtt{Z})$$

Otrzymaliśmy sprzeczność: Szukana permutacja przeprowadza `X` na `F`, ale w permutacji $UV$ litera `X` nie występuje w cyklu długości 2. Druga możliwość wygląda następująco:

$$UV = (\mathtt{R},\mathtt{Q})$$
$$VW = (\mathtt{E},\mathtt{O})(\mathtt{F},\mathtt{N})(\mathtt{A},\mathtt{R},\mathtt{T},\mathtt{V},\mathtt{U},\mathtt{Z},\mathtt{L},\mathtt{C},\mathtt{B},\mathtt{H},\mathtt{W})(\mathtt{D},\mathtt{M},\mathtt{G},\mathtt{Q},\mathtt{Y},\mathtt{P},\mathtt{J},\mathtt{X},\mathtt{I},\mathtt{S},\mathtt{K})$$
$$WX = (\ ,\ )(\ ,\ )(\mathtt{P},\mathtt{E},\mathtt{H},\mathtt{R},\mathtt{A},\mathtt{F},\mathtt{U},\mathtt{K},\mathtt{Z},\mathtt{G},\mathtt{V})(\mathtt{T},\mathtt{I},\mathtt{O},\mathtt{M},\mathtt{D},\mathtt{Q},\mathtt{N},\mathtt{C},\mathtt{S},\mathtt{W},\mathtt{X})$$

Otrzymujemy podobną sprzeczność: litera `Z` nie może bowiem przejść na literę `F`. Popatrzmy na trzecią możliwość:

$$UV = (\mathtt{B},\mathtt{K})$$
$$VW = (\mathtt{E},\mathtt{O})(\mathtt{F},\mathtt{N})(\mathtt{A},\mathtt{R},\mathtt{T},\mathtt{V},\mathtt{U},\mathtt{Z},\mathtt{L},\mathtt{C},\mathtt{B},\mathtt{H},\mathtt{W})(\mathtt{D},\mathtt{M},\mathtt{G},\mathtt{Q},\mathtt{Y},\mathtt{P},\mathtt{J},\mathtt{X},\mathtt{I},\mathtt{S},\mathtt{K})$$
$$WX = (\ ,\ )(\ ,\ )(\mathtt{A},\mathtt{F},\mathtt{U},\mathtt{K},\mathtt{Z},\mathtt{G},\mathtt{V},\mathtt{P},\mathtt{E},\mathtt{H},\mathtt{R})(\mathtt{M},\mathtt{D},\mathtt{Q},\mathtt{N},\mathtt{C},\mathtt{S},\mathtt{W},\mathtt{X},\mathtt{T},\mathtt{I},\mathtt{O})$$

Tym razem sprzeczność polega na tym, że litera `A` musiałaby przejść na siebie. Wreszcie czwarta możliwość:

$$UV = (\mathtt{K},\mathtt{B})$$
$$VW = (\mathtt{E},\mathtt{O})(\mathtt{F},\mathtt{N})(\mathtt{A},\mathtt{R},\mathtt{T},\mathtt{V},\mathtt{U},\mathtt{Z},\mathtt{L},\mathtt{C},\mathtt{B},\mathtt{H},\mathtt{W})(\mathtt{D},\mathtt{M},\mathtt{G},\mathtt{Q},\mathtt{Y},\mathtt{P},\mathtt{J},\mathtt{X},\mathtt{I},\mathtt{S},\mathtt{K})$$
$$WX = (\ ,\ )(\ ,\ )(\mathtt{Q},\mathtt{N},\mathtt{C},\mathtt{S},\mathtt{W},\mathtt{X},\mathtt{T},\mathtt{I},\mathtt{O},\mathtt{M},\mathtt{D})(\mathtt{H},\mathtt{R},\mathtt{A},\mathtt{F},\mathtt{U},\mathtt{K},\mathtt{Z},\mathtt{G},\mathtt{V},\mathtt{P},\mathtt{E})$$

daje poszukiwane rozwiązanie:

$$R' = R_z Q R_z^{-1} = (\mathtt{A},\mathtt{Q},\mathtt{F},\mathtt{B},\mathtt{O},\mathtt{L},\mathtt{T},\mathtt{C},\mathtt{I},\mathtt{V},\mathtt{S},\mathtt{P},\mathtt{K},\mathtt{E},\mathtt{Y},\mathtt{U},\mathtt{W},\mathtt{D},\mathtt{H},\mathtt{M},\mathtt{R},\mathtt{N},\mathtt{J},\mathtt{Z},\mathtt{X},\mathtt{G}).$$

Nietrudno sprawdzić, że permutacja $XY$ powstaje z permutacji $WX$ za pomocą tej samej permutacji $R'$ oraz permutacja $YZ$ powstaje w taki sam sposób z permutacji $XY$.

Rozwiązanie układu permutacji zostało znalezione. Zacytujmy jeszcze raz Rejewskiego:

„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 $R$. Tak więc połączenia jednego bębenka, bębenka prawego, były wreszcie znane.

Jak znaleziono połączenia pozostałych bębenków? Przypomnę, że dostarczono mi fotokopię 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 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."

Ponieważ $R' = R_z Q R_z^{-1}$, więc $Q = R_z^{-1} R' R_z$. Permutację $R_z$ otrzymamy podpisując w odpowiedni sposób permutację $Q$ pod permutacją $R'$. Oto ten właściwy sposób podpisania pod sobą permutacji $R'$ i $Q$:

$$R' = (\mathtt{A},\mathtt{Q},\mathtt{F},\mathtt{B},\mathtt{O},\mathtt{L},\mathtt{T},\mathtt{C},\mathtt{I},\mathtt{V},\mathtt{S},\mathtt{P},\mathtt{K},\mathtt{E},\mathtt{Y},\mathtt{U},\mathtt{W},\mathtt{D},\mathtt{H},\mathtt{M},\mathtt{R},\mathtt{N},\mathtt{J},\mathtt{Z},\mathtt{X},\mathtt{G}),$$

$$Q = (\mathtt{N},\mathtt{O},\mathtt{P},\mathtt{Q},\mathtt{R},\mathtt{S},\mathtt{T},\mathtt{U},\mathtt{V},\mathtt{W},\mathtt{X},\mathtt{Y},\mathtt{Z},\mathtt{A},\mathtt{B},\mathtt{C},\mathtt{D},\mathtt{E},\mathtt{F},\mathtt{G},\mathtt{H},\mathtt{I},\mathtt{J},\mathtt{K},\mathtt{L},\mathtt{M}).$$

Otrzymujemy w ten sposób

$$R_z = (\mathtt{A},\mathtt{N},\mathtt{I},\mathtt{V},\mathtt{W},\mathtt{D},\mathtt{E})(\mathtt{B},\mathtt{Q},\mathtt{O},\mathtt{R},\mathtt{H},\mathtt{F},\mathtt{P},\mathtt{Y})(\mathtt{C},\mathtt{U})(\mathtt{G},\mathtt{M})(\mathtt{J})(\mathtt{K},\mathtt{Z})(\mathtt{L},\mathtt{S},\mathtt{X})(\mathtt{T}).$$

Wreszcie $R = (Q^z)^{-1} R_z Q^z$. Dla $z = 7$ otrzymujemy ostatecznie

$$R = (\mathtt{A})(\mathtt{B},\mathtt{J})(\mathtt{C},\mathtt{D},\mathtt{K},\mathtt{L},\mathtt{H},\mathtt{U},\mathtt{P})(\mathtt{E},\mathtt{S},\mathtt{Z})(\mathtt{F},\mathtt{I},\mathtt{X},\mathtt{V},\mathtt{Y},\mathtt{O},\mathtt{M},\mathtt{W})(\mathtt{G},\mathtt{R})(\mathtt{N},\mathtt{T})(\mathtt{Q}).$$

Na zakończenie podamy połączenia wewnętrzne pięciu bębenków ruchomych i dwóch bębenków odwracających używanych przez Wehrmacht niemal do końca II Wojny Światowej:

$$I = (\mathtt{A},\mathtt{E},\mathtt{L},\mathtt{T},\mathtt{P},\mathtt{H},\mathtt{Q},\mathtt{X},\mathtt{R},\mathtt{U})(\mathtt{B},\mathtt{K},\mathtt{N},\mathtt{W})(\mathtt{C},\mathtt{M},\mathtt{O},\mathtt{Y})(\mathtt{D},\mathtt{F},\mathtt{G})(\mathtt{I},\mathtt{V})(\mathtt{J},\mathtt{Z})(\mathtt{S}),$$

$$II = (\mathtt{A})(\mathtt{B},\mathtt{J})(\mathtt{C},\mathtt{D},\mathtt{K},\mathtt{L},\mathtt{H},\mathtt{U},\mathtt{P})(\mathtt{E},\mathtt{S},\mathtt{Z})(\mathtt{F},\mathtt{I},\mathtt{X},\mathtt{V},\mathtt{Y},\mathtt{O},\mathtt{M},\mathtt{W})(\mathtt{G},\mathtt{R})(\mathtt{N},\mathtt{T})(\mathtt{Q}),$$

$$III = (\mathtt{A},\mathtt{B},\mathtt{D},\mathtt{H},\mathtt{P},\mathtt{E},\mathtt{J},\mathtt{T})(\mathtt{C},\mathtt{F},\mathtt{L},\mathtt{V},\mathtt{M},\mathtt{Z},\mathtt{O},\mathtt{Y},\mathtt{Q},\mathtt{I},\mathtt{R},\mathtt{W},\mathtt{U},\mathtt{K},\mathtt{X},\mathtt{S},\mathtt{G})(\mathtt{N}),$$

$$IV = (\mathtt{A},\mathtt{E},\mathtt{P},\mathtt{L},\mathtt{I},\mathtt{Y},\mathtt{W},\mathtt{C},\mathtt{O},\mathtt{X},\mathtt{M},\mathtt{R},\mathtt{F},\mathtt{Z},\mathtt{B},\mathtt{S},\mathtt{T},\mathtt{G},\mathtt{J},\mathtt{Q},\mathtt{N},\mathtt{H})(\mathtt{D},\mathtt{V})(\mathtt{K},\mathtt{U}),$$

$$V = (\mathtt{A},\mathtt{V},\mathtt{O},\mathtt{L},\mathtt{D},\mathtt{R},\mathtt{W},\mathtt{F},\mathtt{I},\mathtt{U},\mathtt{Q})(\mathtt{B},\mathtt{Z},\mathtt{K},\mathtt{S},\mathtt{M},\mathtt{N},\mathtt{H},\mathtt{Y},\mathtt{C})(\mathtt{E},\mathtt{G},\mathtt{T},\mathtt{J},\mathtt{P},\mathtt{X}),$$

$$T_A = (\mathtt{A},\mathtt{I})(\mathtt{B},\mathtt{M})(\mathtt{C},\mathtt{E})(\mathtt{D},\mathtt{T})(\mathtt{F},\mathtt{G})(\mathtt{H},\mathtt{R})(\mathtt{J},\mathtt{Y})(\mathtt{K},\mathtt{S})(\mathtt{L},\mathtt{Q})(\mathtt{N},\mathtt{Z})(\mathtt{O},\mathtt{X})(\mathtt{P},\mathtt{W})(\mathtt{U},\mathtt{V}),$$

$$T_B = (\mathtt{A},\mathtt{Y})(\mathtt{B},\mathtt{R})(\mathtt{C},\mathtt{U})(\mathtt{D},\mathtt{H})(\mathtt{E},\mathtt{Q})(\mathtt{F},\mathtt{S})(\mathtt{G},\mathtt{L})(\mathtt{I},\mathtt{P})(\mathtt{J},\mathtt{X})(\mathtt{K},\mathtt{N})(\mathtt{M},\mathtt{O})(\mathtt{T},\mathtt{Z})(\mathtt{V},\mathtt{W}).$$

**Bibliografia**


[1] Carlson, Andy; Symulator Enigmy zamieszczony na stronie internetowej `http://homepages.tesco.net/~andycarlson/enigma/enigma_j.html`

[2] *Enigma machine*; Wikipedia, strona internetowa `http://en.wikipedia.org/wiki/Enigma_machine` tam też odsyłacz do:

[3] Ulbricht, Heinz; *Die Chiffriermaschine Enigma – Trügerische Sicherheit: Ein Beitrag zur Geschichte der Nachrichtendienste*, praca doktorska, 2005 (po niemiecku).

[4] Gaj, Krzysztof; *Szyfr Enigmy. Metody złamania*, Wydawnictwa Komunikacji i Łączności, Warszawa 1989.

[5] Grajek, Marek; *Enigma. Bliżej prawdy.* Dom Wydawniczy Rebis, Poznań 2007.

[6] Kahn, David, *Enigma. Złamanie kodu U-bootów*, 1939 – 1943. Wydawnictwo Magnum, Warszawa 2005.

[7] Kozaczuk, Władysław; *W kręgu Enigmy, wyd. drugie poszerzone*, Książka i Wiedza, Warszawa 1986.

[8] Rejewski, Marian; *Jak matematycy polscy rozszyfrowali Enigmę*, Wiadomości Matematyczne XXIII (1980), 1 – 28.

[9] Rejewski, Marian; *Wspomnienia z mej pracy w Biurze Szyfrów Oddziału II Sztabu Głównego 1930 – 1945*, Przegląd Historyczno-Wojskowy, rok VI (LVII), nr specjalny 5 (210), Warszawa 2005, str. 71 – 160.