Uniwersytet Jagielloński

Matematyczne aspekty rozszyfrowania Enigmy

Zbigniew Błocki

Wydział Matematyki i Informatyki
Instytut Matematyki
Kraków, 2003

Marian Rejewski
(1905-1980)

15 VII 1928 - armia niemiecka wprowadza Enigmy do użytku

1928/29 - kurs kryptologii w Instytucie Matematyki Uniwersytetu Poznańskiego zorganizowany przez Biuro Szyfrów Oddziału II Sztabu Głównego

1 IX 1932 - Biuro Szyfrów w Warszawie zatrudnia Mariana Rejewskiego, Jerzego Różyckiego i Henryka Zygalskiego; początek prac nad złamaniem kodu Enigmy

Grupa permutacji

$I_n = \{1, 2, \ldots, n\}$ $\quad (n = 26, \quad I_n \cong \{a, b, \ldots, x, y, z\})$
$S_n = \{A : I_n \to I_n$ - bijekcja$\}$ - grupa nieprzemienna (z działaniem $AB = A \circ B$). Każdy element $A \in S_n$ posiada element odwrotny A^{-1}

$$AA^{-1} = A^{-1}A = id, \quad (AB)^{-1} = B^{-1}A^{-1}.$$

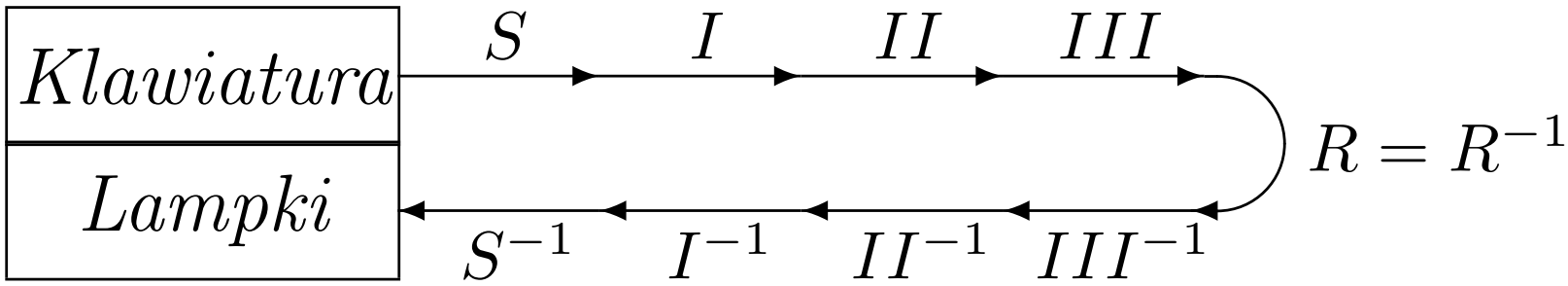
Jeżeli $a_1, \ldots, a_k \in I_n$, $a_i \neq a_j$ dla $i \neq j$, to przez $(a_1 a_2 \ldots a_k)$ oznaczamy cykl długości k

$$a_1 \mapsto a_2 \mapsto \ldots \mapsto a_k \mapsto a_1.$$

Każdą permutację można przedstawić jako złożenie cykli rozłącznych

$$A = (a_1 \ldots a_k)(b_1 \ldots b_l) \ldots$$

Konstrukcja i działanie Enigmy



$S = (a_1 b_1) \dots (a_6 b_6) = S^{-1}$ - połączenia wtyczkowe

Zakładając, że obraca się tylko pierwszy wirnik (25 na 26 razy), mamy

$$I = P^{\alpha+1} N P^{-\alpha-1}, \quad II = P^{\beta} M P^{-\beta}, \quad III = P^{\gamma} L P^{-\gamma},$$

gdzie $\alpha, \beta, \gamma \in \{1, 2, \dots, 26\}$ - ustawienie wirników,

$P = (1, 2 \dots 26)$ - obrót o $1/26$ pełnego kąta,

N, M, L, R - połączenia wewnętrzne wirników (identyczne we wszystkich Enigmach danej sieci).

N, M, L	$26!^3 \simeq 10^{80}$
R	$\dfrac{26!}{13!2^{13}} \simeq 10^{13}$
α, β, γ	$3!26^3 \simeq 10^5$
S	$\dfrac{26!}{6!14!2^6} \simeq 10^{11}$

Sposób szyfrowania depesz (1932 r.)

S, α, β, γ - klucz dzienny (wg. księgi szyfrów)
$\overline{\alpha}, \overline{\beta}, \overline{\gamma}$ - klucz depeszy (wybierany przez szyfranta)

Początek każdej depeszy miał postać

$$A_1(\overline{\alpha}), A_2(\overline{\beta}), A_3(\overline{\gamma}), A_4(\overline{\alpha}), A_5(\overline{\beta}), A_6(\overline{\gamma}),$$

przy czym permutacje $A_1, \ldots, A_6$ były stałe danego dnia ($A_i^{-1} = A_i$, tzn. A_i składają się z transpozycji rozłącznych).

Posiadając odp. ilość zaszyfrowanych depesz z danego dnia (ok. 80) można odtworzyć permutacje $A_{i+3}A_i^{-1} = A_{i+3}A_i$, $i = 1, 2, 3$.

Odtworzenie kluczy depesz (jesień 1932)

Permutacje $A_{i+3}A_i$ miały zawsze następującą własność

$(*)$ cykle danej długości występują w liczbie parzystej

Twierdzenie. $X \in S_{2m}$ spełnia $(*)$ wtedy i tylko wtedy, gdy istnieją $A, B \in S_{2m}$ takie, że $A = A^{-1}$, $B = B^{-1}$ oraz $X = AB$.

Algorytm znajdowania A, B (zakładając, że znamy iloczyn AB spełniający $(*)$):

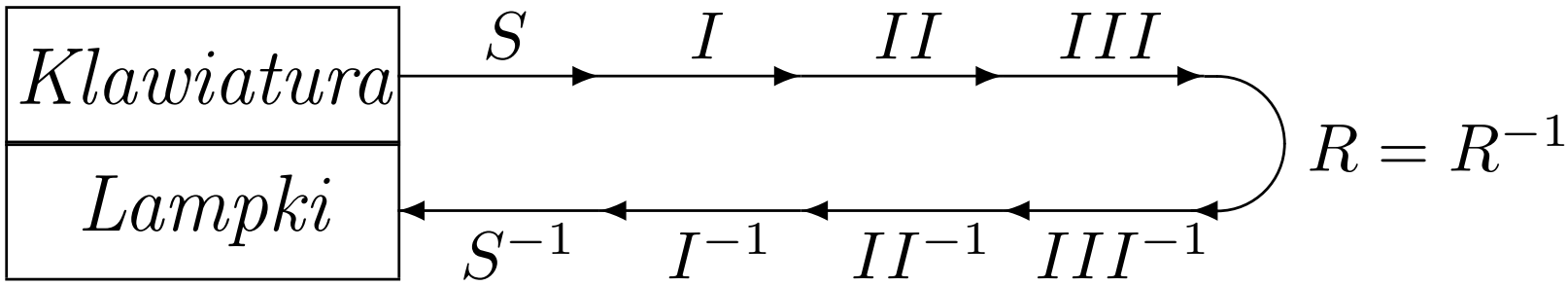
- Cykle danej długości grupujemy w pary;

- Dla danej pary cykli długości k mamy dokł. k możliwości:

$$\begin{aligned}(a_1 \dots a_k)(b_1 \dots b_k) =& (a_k b_l)(a_{k-1} b_{l-1}) \dots (a_1 b_{l+1}) \\ & (a_k b_{l-1})(a_{k-1} b_{l-2}) \dots (a_1 b_l)\end{aligned}$$

- Do wyboru właściwych permutacji A_i z ok. kilku tysięcy możliwych rozwiązań wykorzystywano nawyki szyfrantów (np. wybieranie trzech takich samych liter jako kluczy depesz).

Konstrukcja i działanie Enigmy



$S = (a_1 b_1) \dots (a_6 b_6) = S^{-1}$ - połączenia wtyczkowe

Zakładając, że obraca się tylko pierwszy wirnik (25 na 26 razy), mamy

$$I = P^{\alpha+1} N P^{-\alpha-1}, \quad II = P^{\beta} M P^{-\beta}, \quad III = P^{\gamma} L P^{-\gamma},$$

gdzie $\alpha, \beta, \gamma \in \{1, 2, \dots, 26\}$ - ustawienie wirników,

$P = (1, 2 \dots 26)$ - obrót o $1/26$ pełnego kąta,

N, M, L, R - połączenia wewnętrzne wirników (identyczne we wszystkich Enigmach danej sieci).

Odtworzenie połączeń wewnętrznych

Zakładając, że obraca się tylko pierwszy wirnik (20 na 26 razy), mamy

$$A_i = S^{-1} P^{\alpha+i} N^{-1} P^{-\alpha-i} Q P^{\alpha+i} N P^{-\alpha-i} S,$$
$$i = 1, \ldots, 6,$$

gdzie

$$Q = P^{\beta} M^{-1} P^{-\beta+\gamma} L^{-1} P^{-\gamma} R P^{\gamma} L P^{-\gamma+\beta} M P^{-\beta}.$$

Mamy zatem układ 6 równań z 4 niewiadomymi S, N, Q, α.

Przełom: 9 XII 1932 Rejewski otrzymuje przekazane przez wywiad francuski (Gustave Bertrand) klucze dzienne za wrzesień i październik 1932 r.

$$U_i = N^{-1}P^{-\alpha-i}QP^{\alpha+i}N, \quad i = 1, \ldots, 6$$

$$U_{i+1}U_{i+2} = (N^{-1}PN)U_iU_{i+1}(N^{-1}PN)^{-1}, \quad i = 1, \ldots, 4.$$

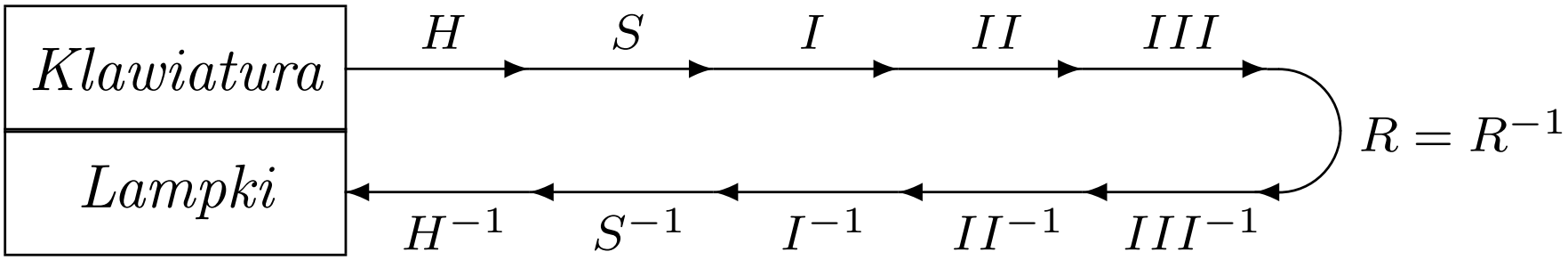
Obserwacja. Jeżeli

$$A = \begin{pmatrix} 1 & \ldots & 26 \\ A(1) & \ldots & A(26) \end{pmatrix} = (a_1 \ldots a_k)(b_1 \ldots b_l) \ldots,$$

to

$$XAX^{-1} = \begin{pmatrix} X(1) & \ldots & X(26) \\ X(A(1)) & \ldots & X(A(26)) \end{pmatrix}$$
$$= (X(a_1) \ldots X(a_k))(X(b_1) \ldots X(b_l)) \ldots$$

Wniosek. Równanie $XAX^{-1} = B$ ma rozwiązanie X wtedy i tylko wtedy, gdy permutacje A i B są podobne (tzn. zbiór długości cykli rozłącznych jest taki sam).



$$H = \begin{pmatrix} q & v & e & r & t & z & \dots \\ a & b & c & d & e & f & \dots \end{pmatrix}$$ (w Enigmie handl.)

$$H = \begin{pmatrix} a & b & c & d & e & f & \dots \\ a & b & c & d & e & f & \dots \end{pmatrix}$$ (w Enigmie wojsk.)!

Odczytywanie depesz (1933-1938)

- wykonanie replik Enigmy przez warszawską firmę AVA;

- metoda $rusztu$ (wykorzystująca fakt, że permutacja S nie zmienia 14 z 26 znaków);

- skatalogowanie długości cykli permutacji $A_{i+3}A_i$ w zależności od α, β, γ przy pomocy specjalnie skonstruowanego urządzenia zwanego $cyklometrem$ (permutacje te są postaci $S^{-1} \ldots S$, zatem długości ich cykli nie zależą od S).

styczeń 1933 - kod Enigmy złamany!

1936-38 - liczne zmiany w Enigmach: zwiększenie liczby wirników oraz liczby połączeń wtyczkowych, częstsze zmiany kodów, itd.

początek 1938 - Polacy odczytują 75% depesz niemieckich

15 IX 1938 - zasadnicza zmiana sposobu szyfrowania

1938-39 - konstrukcja *bomby kryptologicznej* (ang. *bombe*) oraz *płacht Zygalskiego*

25-26 VII 1939 - spotkanie z Brytyjczykami i Francuzami w Warszawie

1940 - Amerykanie łamią japoński kod *Purple*

1943 - Brytyjczycy konstruują maszynę *Colossus*

1974 - książka F.Winterbothama *The Ultra Secret*

??? - Anglicy przyznają, że to nie oni złamali Enigmę

versity (1906), and Vance Air Force Base is nearby. Inc. 1894. Pop. (1990) city, 45,309; Enid MSA, 56,735.

Enigma, device used by the German military command to encode strategic messages before and during World War II. The Enigma code was broken by a British intelligence system known as Ultra (*q.v.*).

Eniwetok (Marshall Islands): *see* Enewetak.

Enkhuizen, *gemeente* (commune), Nordholland *provincie,* northwestern Netherlands, on the IJsselmeer (Lake IJssel). Chartered in 1355,

Ultra, Allied intelligence system that, in tapping the very highest-level communications among the German armed forces, as well as (after 1941) those of the Japanese armed forces, contributed to the Allied victory in World War II.

In 1938 a Polish mechanic employed in a German factory producing secret signaling machines named Enigma (which worked on the basis of a set of preset revolving drums) took notes of the components before being repatriated and, with the help of the British and French secret services, constructed a wooden mockup of the machine. A British cryptographer later smuggled a complete new Enigma machine to England. There, British mathematicians and cryptographers conquered the problems of Enigma variations and found means of cracking the ciphers. Early in 1939 Britain's secret service set up the Ultra project at Bletchley Park, 50 miles (80 km) north of London, for the purpose of intercepting the