Matematyczne aspekty rozszyfrowania Enigmy

Zbigniew Błocki, Wydział Matematyki, Fizyki i Informatyki UJ

Wykład habilitacyjny, Kraków, 24 maja 2001

Wstęp

Rozszyfrowanie maszyny szyfrującej Enigma miało trudne do przecenienia znaczenie dla przebiegu drugiej wojny światowej. W szczytowym okresie Niemcy używali ponad 100 tys. takich maszyn będąc do końca przekonani, że złamanie ich kodu jest niemożliwe. Informacje dotyczące rozszyfrowania Enigmy i ogromnego wpływu jakie miało to dla działań militarnych sił alianckich ujawniono dopiero w latach 70-tych. Z tego też pewnie powodu sprawa Enigmy nie zajmuje w powszechnej świadomości miejsca na jakie zasługuje, a militarną historię wojny powinno się właściwie napisać od nowa.

Polskie stacje nasłuchowe zaczęły przechwytywać depesze szyfrowane Enigmą w połowie 1928 roku. Kluczową okazała się decyzja Biura Szyfrów o zatrudnieniu matematyków (do tej pory jako kryptolodzy pracowali głównie lingwiści). Na początku 1929 roku zorganizowano w Instytucie Matematyki Uniwersytetu Poznańskiego kurs szyfrowy (w Wielkopolsce było najwięcej osób mówiących płynnie po niemiecku). Spośród uczestników tego kursu trzech zostało 1-ego września 1932 roku zatrudnionych na stałe przez Biuro Szyfrów w Warszawie. Byli to: Marian Rejewski, Jerzy Różycki oraz Henryk Zygalski. Pierwszego z nich odseparowano od pozostałych, oddano do dyspozycji egzemplarz Enigmy typu handlowego i polecono pracę nad wersją wojskową.

Konstrukcja i działanie Enigmy

Enigma typu wojskowego miała wielkość przenośnej maszyny do pisania. Oprócz 26-znakowej klawiatury posiadała również zestaw 26 lampek z literami. Mechanizm kodujący składał się z łącznicy wtyczkowej S, w której 6 par liter można było dowolnie pozamieniać, trzech wirników N, M, L oraz bębenka odwracającego R. Permutacja S w związku z tym w rozkładzie na cykle rozłączne składała się z 6 transpozycji, permutacje N, M, L były takie same w każdej Enigmie danego typu (ale a priori całkowicie dowolne), natomiast permutacja R była taka sama jak R^{-1}, tj.

$$R^2 = I, \tag{1}$$

gdzie I oznacza permutację identycznościową. Jest to równoważne z faktem, że R można zapisać jako iloczyn transpozycji rozłącznych. Wirniki były obracalne i można było je dowolnie ustawić, jak również wymieniać między sobą. Po naciśnięciu klawisza o jedno pole obracał się pierwszy wirnik, po pełnym obrocie pierwszego obracał się również drugi, po pełnym obrocie drugiego także trzeci. Oznacza to, że wirniki drugi i trzeci obracały się tylko co 26-te uderzenie klawisza i dla prostoty w większości przypadków można założyć, że obracał się tylko pierwszy wirnik. Jeżeli zatem przez $\alpha, \beta, \gamma \in \{1, 2, \ldots, 26\}$ (litery będziemy utożsamiać z liczbami) oznaczymy ustawienia początkowe trzech wirników, to otrzymamy, że i-tą literę danej depeszy przekształca permutacja

$$A_i = S^{-1}P^{\alpha+i}N^{-1}P^{-\alpha-i}QP^{\alpha+i}NP^{-\alpha-i}S, \quad i = 1, 2, \ldots, \tag{2}$$

gdzie

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

oraz $P = (1, 2, \ldots, 26)$ oznacza obrót o jedno pole. Permutacje A_i miały własność (1) i dzięki temu Enigma służyła zarówno do szyfrowania jak i odszyfrowywania depesz.

Było ok. 10^5 wszystkich możliwości ustawienia wirników oraz ok. 10^{11} różnych połączeń łącznicy S. Niemcy rozumowali, że nawet jeżeli ktoś pozna połączenia wewnętrzne N, M, L oraz R (takie same w każdym egzemplarzu Enigmy wojskowej), to nie będzie w stanie sprawdzić ok. 10^{16} wszystkich możliwych ustawień.

Sposób szyfrowania depesz

Aż do 1938 roku w armii niemieckiej procedura szyfrowania depesz była następująca. Szyfrant miał do dyspozycji klucz dzienny, który określał ustawienie początkowe łącznicy wtyczkowej S oraz wirników α, β, γ. Następnie dla każdej depeszy szyfrant dowolnie ustalał jej szyfr indywidualny $\overline{\alpha}, \overline{\beta}, \overline{\gamma}$, po czym szyfrował go dwukrotnie. Później zmieniał nastawienie wirników na $\overline{\alpha}, \overline{\beta}, \overline{\gamma}$ i nadawał właściwą depeszę. Zatem pierwszych 6 liter każdej depeszy miało 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.

Odtworzenie kluczy depesz

To że pierwszych 6 liter każdej depeszy stanowiło zaszyfrowany dwukrotnie klucz było oczywiste, gdyż jeżeli w dwóch depeszach z danego dnia taka sama była pierwsza litera, to identyczna była również czwarta, jeśli powtarzały się drugie litery, to również piąte, itd. Mając dostateczną liczbę depesz z danego dnia Rejewski mógł odtworzyć iloczyny A_1A_4, A_2A_5 i A_3A_6 (dokładnie $A_iA_{i+3}^{-1}$, ale wiemy, że $A_{i+3}^{-1} = A_{i+3}$). Po rozpisaniu ich na cykle rozłączne zauważył, że wszystkie mają zawsze charakterystyczną własność:

(3) cykle danej długości występują w liczbie parzystej.

Można sformułować proste twierdzenie:

Załóżmy, że X jest permutacją stopnia parzystego. Wtedy X spełnia (3) wtedy i tylko wtedy, gdy istnieją permutacje A, B spełniające (1) takie, że $X = AB$.

Od dowodu tego faktu ważniejszy w naszym przypadku jest prosty algorytm znajdowania wszystkich możliwych permutacji A, B przy danym X. Najpierw trzeba wszystkie cykle X tej samej długości pogrupować w pary, a następnie dla danej pary cykli długości k istnieje dokładnie k możliwości zapisania ich iloczynu jako iloczyn dwóch permutacji składających się z k transpozycji rozłącznych każda. W efekcie dawało to zwykle kilkadziesiąt możliwości na A_i i A_{i+3}, znając ich iloczyn. Do znalezienia właściwego rozwiązania wykorzystywano nawyki szyfrantów, którzy na przykład w początkowym okresie najczęściej jako klucze depesz $\overline{\alpha}, \overline{\beta}, \overline{\gamma}$ wybierali te same litery. W takim przypadku ze zbioru możliwych rozwiązań należało wybrać to, które najczęściej dawało takie same $\overline{\alpha}, \overline{\beta}, \overline{\gamma}$.

Znalezienie połączeń wewnętrznych

Po znalezieniu permutacji A_i możemy traktować (2) jako układ 6 równań z niewiadomymi S, N, Q oraz α. Tego układu jednak Rejewski nie potrafił rozwiązać. Kluczową pomocą okazało się dostarczenie na początku grudnia 1932 roku przez wywiad francuski, a dokładnie kapitana (później generała) Gustave'a Bertranda, kopii tablic kluczy dziennych za wrzesień i październik tego roku. Choć sami Francuzi nie potrafili zrobić z nich żadnego użytku, okazały się one przełomowe w pracy Rejewskiego. W układzie (2) pozostały teraz tylko 2 niewiadome N i Q, podczas gdy S i α stały się znane. Bez straty ogólności możemy założyć, że $\alpha = 0$ (modulo 26). Po przekształceniu (2) dostaniemy

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

gdzie permutacje U_i są znane. Stąd łatwo można otrzymać

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

Zauważmy, ze jeżeli mamy permutację

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

to permutację XBX^{-1} można traktować jako B po zmianie zmiennych X, tzn.

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

Oznacza to, że równanie

$$A = XBX^{-1}, \tag{5}$$

gdzie A, B są dane a X jest niewiadomą, ma rozwiązanie wtedy i tylko wtedy, gdy permutacje A i B są do siebie podobne (tzn. zbiór długości cykli rozłącznych jest taki sam). Żeby znaleźć wszystkie rozwiązania (5) trzeba najpierw danemu cyklowi z A przyporządkować cykl tej samej długości k z B, a następnie istnieje dokładnie k możliwości właściwego przyporządkowania elementom cyklu z A elementów cyklu z B.

To pokazuje jak znaleźć możliwe rozwiązania $N^{-1}PN$ dla danego i w (4), trzeba oczywiście wybrać rozwiązanie wspólne dla wszystkich 4 równań. Tak otrzymano 26 możliwych N, wybór właściwego nastąpił później drogą doświadczalną. Ponieważ dostarczone tablice kluczy dziennych pochodziły z dwóch różnych kwartałów, inne wirniki były na pierwszym miejscu, co pozwoliło znaleźć połączenia obu tę samą metodą (wtedy jeszcze kolejność wirników zmieniano co kwartał, później coraz częściej, ostatecznie codziennie). Znalezienie połączeń trzeciego wirnika oraz bębenka odwracającego R nie przedstawiało już większych trudności.

Odczytywanie depesz

Po odtworzeniu połączeń wewnętrznych Enigmy wykonano jej replikę. W celu odczytywania bieżących depesz należało jeszcze znaleźć metodę znajdowania kluczy dziennych S, α, β, γ. Pierwszym sposobem była tak zwana metoda rusztu, która polegała na

porównywaniu permutacji A_i z wyrażeniami $P^{\alpha+i}NP^{-\alpha-i}$, $i = 1, \ldots, 6$, dla wszystkich możliwych α i szukaniu pewnych podobieństw. (Metoda ta opierała się na fakcie, że permutacja S nie zmieniała 14 z 26 liter.) Bardziej zaawansowanym sposobem było wykorzystanie urządzenia nazwanego *cyklometrem*. Z (2) wynika, że iloczyny A_iA_{i+3} mają postać $S^{-1} \ldots S$. Z rozumowania, które przedstawiliśmy powyżej wynika zatem, że długości cykli tych iloczynów nie zależą od S, a tylko od ustawienia początkowego wirników. Możliwych takich ustawień jest $3!\,26^3$, czyli ok. 10^5. Wystarczyło zatem skatalogować długości cykli w iloczynach A_iA_{i+3}, $i = 1, 2, 3$, w zależności od ustawień wirników. W tym właśnie celu skonstruowano cyklometr. Znając α, β, γ łatwo już odtworzyć S.

Zakończenie

Aż do zasadniczej zmiany sposobu szyfrowania, która nastąpiła we wrześniu 1938 roku, Polacy, stale doskonaląc swoje metody, byli w stanie odszyfrowywać zdecydowaną większość depesz niemieckich kodowanych Enigmą. Po wprowadzeniu przez Niemców nowej metody szyfrowania stało się to już trudniejsze. Wynaleziono jednak dwie metody, które to umożliwiały. Były to tzw. *płachty Zygalskiego* oraz *bomba kryptologiczna*, której pomysł przedstawił Rejewski. Wymagały one jednak znacznie większych niż poprzednio nakładów finansowych oraz pracy personelu, zaś środki, którymi dysponowało Biuro Szyfrów były ograniczone.

W lipcu 1939 roku całą posiadaną wiedzę nt. Enigmy oraz egzemplarze wszystkich skonstruowanych urządzeń przekazano przybyłym do Warszawy Brytyjczykom i Francuzom, którzy mimo usilnych starań do tego czasu nie osiągneli absolutnie niczego w swoich próbach złamania kodu Enigmy. Brytyjczycy do 1944 roku, kiedy to skonstruowali urządzenie o nazwie *Colossus*, dzisiaj przez wielu uważane za pierwszy komputer, używali praktycznie wyłącznie metod dostarczonych przez Polaków, przede wszystkim ciągle ulepszanej bomby kryptologicznej. W przeciwieństwie do Polaków wywiad brytyjski dysponował prawie nieograniczonymi środkami, wystarczy wspomnieć, że w głównej siedzibie w Bletchey Park pracowało w szczytowym okresie prawie 10 tys. ludzi.

Tym bardziej powinno dziwić z jakim trudem do dzisiaj przychodzi Brytyjczykom choćby krótka wzmianka o kluczowej roli Polaków w rozszyfrowaniu Enigmy. Hasło *Enigma* w *Encyclopædia Britannica* do dzisiaj (także w wersji internetowej) brzmi następująco:

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.).*

Pod bardziej rozbudowanym hasłem *Ultra* jedyny polski ślad to całkowicie nieprawdziwa historia o Polaku zatrudnionym w niemieckiej fabryce produkującej Enigmy, który jakoby w 1938 roku miał spisać jej połączenia wewnętrzne i przekazać Brytyjczykom.