„Enigma", nauka, kryptologia

prof. dr hab. n. mat. inż.
Jerzy Gawinecki
mgr inż. Kamil Kaczyński

Wojskowa Akademia Techniczna
im. Jarosława Dąbrowskiego

Artykuł przedstawia pracę polskich matematyków z Biura Szyfrów Sztabu Głównego, którzy dzięki nieszablonowemu podejściu do kryptoanalizy złamali kod „Enigmy". Ten jeden z największych sukcesów kryptoanalityków w historii, pozwolił na skrócenie działań wojennych o 2 lata i ocalenie milionów ludzkich istnień.

I wojna światowa przyniosła zmianę w sposobie komunikacji wojskowej – na szeroką skalę zaczęto wykorzystywać transmisję radiową. Jej zalety są niepodważalne – brak konieczności budowania infrastruktury do przesyłania sygnału i duża mobilność radiostacji. Niestety transmisja radiowa ma także jedną znaczącą wadę – każda transmisja posiada jednego nadawcę, jednakże liczba odbiorców nie może być w łatwy sposób ograniczona. Jasne zatem jest, że każda przesyłana w ten sposób treść powinna być zabezpieczona za pomocą kryptografii.

Metody szyfrowania wykorzystywane w tamtym czasie w większości przypadków opierały się na szyfrowaniu ręcznym, co naturalnie skutkowało licznymi błędami w przesyłanych szyfrogramach. Dodatkowo, duża liczba przesyłanych wiadomości prowadziła do wyeksponowania słabości stosowanych szyfrów, przede wszystkim przez analizę lingwistyczną przekazów. Bardziej zaawansowane algorytmy kryptograficzne stwarzały duże trudności dla operatorów radiostacji i szyfrantów polowych, czego skutkiem były często popełniane błędy. Fridrich Bauser, w „Entzifferte Geheimnissee" opisuje przypadek wykorzystania szyfru Cezara przez armię rosyjską w roku 1915 roku. Okazało się, że sztabowcom nie można było powierzyć niczego bardziej skomplikowanego.

Potrzeba wprowadzenia rozwiązań, które zautomatyzowałyby proces szyfrowania i deszyfrowania była bezsprzeczna. Rozpoczęły się prace nad urządzeniami, wykorzystującymi do działania wirniki elektromechaniczne. W roku 1917 swoje urządzenie zaprezentował Edward Hebern (USA), rok później powstała maszyna Arthura Scherbiusa, twórcy „Enigmy". W roku 1919 pojawiły się kolejne dwa rozwiązania opracowane przez Hugo Kocha (Holandia) i Arvida Damma (Szwecja). Arthur Scherbius niedługo później odkupił patent należący do Kocha, usprawniając tym samym swoją konstrukcję. Z początkiem lat 20. XX wieku pojawiły się pierwsze maszyny „Enigma" wykorzystywane w celach komercyjnych. Następnie w 1926 roku „Enigma" została najpierw zaadoptowana przez niemiecką marynarkę wojenną, a w 1928 roku przez siły lądowe. Od tego czasu maszyna została poddana gruntownej

modernizacji, co zaskutkowało zaprezentowaniem w 1930 roku wojskowej wersji „Enigmy" z wprowadzoną łącznicą kablową.

Technologia „Enigmy"

„Enigma" zarówno wyglądem, jak i sposobem używania przypominała maszynę do pisania. Jej wymiary to 28x34x15 cm, waga około 12 kg. Tak kompaktowa budowa pozwalała na łatwe przenoszenie maszyny, a do jej obsługi nie byli potrzebni wyspecjalizowani operatorzy. Główną innowacją, która wyróżniała „Enigmę" na tle dotychczasowych rozwiązań były elektromechaniczne rotory, które pozwalały na szyfrowanie i deszyfrowanie wiadomości. Najważniejsze części, które składały się na kompletne urządzenie to klawiatura, łącznica kablowa, wirniki i panel z lampkami.

Klawiatura posiadała układ QWERTZ z tylko 26 literami. Nie posiadała liczb, spacji itp. (spacje w szyfrogramach zastępowane były znakami *x*). Naciśnięcie klawisza powodowało przesłanie sygnału elektrycznego od wybranej litery, a także obrót jednego z 3 wirników. Klawisze należało naciskać ze sporą siłą, ze względu na mechaniczne rozwiązanie obrotu rotora.

Fot. 1. Klawiatura maszyny szyfrującej „Enigma"
Źródło: *The History and Technology of the Enigma Cipher Machine*, [on-line] [dostęp 12.05.2015]. Dostępny w World Wide Web: http://ciphermachines.com/enigma.

Łącznica kablowa to element dodany do komercyjnej wersji „Enigmy" przez niemieckie wojsko w roku 1930. Łącznica miała taki sam układ jak klawiatura, tak aby do minimum ograniczyć liczbę błędów ludzkich popełnianych przy ustawianiu wstępnym maszyny. Używane do łączenia liter przewody były zakończone standardowymi wtykami bananowymi. Zgodnie z procedurami używania „Enigmy", wykorzystywano zawsze 10 kabli łączących, co przekładało się na zamianę 20 liter. Użytkowanie zmiennej liczby kabli zdecydowanie zwiększało liczbę możliwych

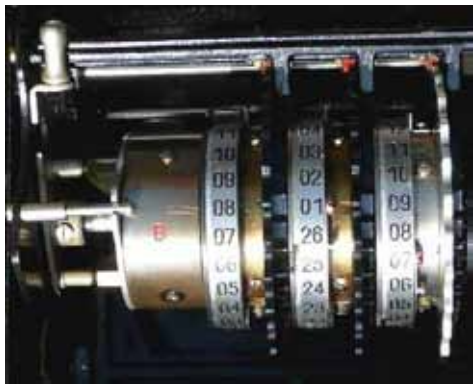
ustawień, jednakże nie było to wykorzystywane, aby zminimalizować liczbę błędów popełnianych przez operatorów.

Wirniki (rotory) były najważniejszym elementem składowym „Enigmy". Miały kształt zbliżony do koła o średnicy około 10 cm. Rotory byli wykonywane z twardej gumy lub bakielitu, z jednej strony posiadały ułożone w okręgu mosiężne nóżki na sprężynkach, zaś z drugiej płaskie styki elektryczne. Gdy wirniki są zamontowane w maszynie, nóżki jednego z wirników łączą się ze stykami kolejnego wirnika, co powoduje zamknięcie obwodu elektrycznego. W wojskowej wersji „Enigmy" wykorzystywany był zestaw 5 wirników o odmiennych połączeniach wewnętrznych, jednakże podczas pracy zainstalowane było tylko 3 z 5 dostępnych wirników. Kolejność ich montażu miała znaczenie, ze względu na różnice w połączeniach wewnętrznych. Na każdym z wirników były umieszczone liczby od 1 do 26, które symbolizowały kolejne litery alfabetu. Zestaw wirników poruszał się w sposób podobny do klasycznego drogomierza znanego m.in. z liczników samochodowych – kolejny wirnik wewnętrzy obracał się o jedną pozycję (1/26 obrotu), po dokonaniu pełnego obrotu przez rotor zewnętrzny. Opisana regularność ruchu wirników stanowi znaczną słabość szyfru, bo oznacza, że przy szyfrowaniu kolejnych 26 liter zmianie będzie ulegało ustawienie tylko jednego wirnika. Rotory wykorzystywane przez siły lądowe i powietrzne miały zainstalowane dodatkowe koło z wcięciem. W pewnych pozycjach wirniki były ustawione w taki sposób, że zapadka sąsiedniego wirnika umożliwiała przestawienie dwóch bębenków jednocześnie. Takie ustawienie nosi nazwę tzw. podwójnego kroku. Trójwirnikowa „Enigma" powtarzała kombinacje kodu na rotorach co 26x25x26=16 900 cykli.

W praktyce oznaczało to, że jeżeli przesyłana wiadomość byłaby dłuższa niż ta wartość, to kolejna część wiadomości byłaby ponownie szyfrowana tym samym kluczem. Standardowe wiadomości miały jednak długość kilkuset znaków, więc problem ten w praktyce nie występował.

Fot. 2. Łącznica kablowa
Źródło: *The History and Technology of the Enigma Cipher Machine*, [on-line] [dostęp 12.05.2015]. Dostępny w World Wide Web: http://ciphermachines.com/enigma.

Walec odwracający (reflektor) służył do zamiany liter parami. Przykładowo, jeżeli A jest zaszyfrowane na G, to G jest szyfrowane na A. Sygnał elektryczny przechodzi najpierw przez 3 rotory, potem przez reflektor, następnie wraca ponownie przez 3 rotory. Reflektor pozwala „Enigmie" na szyfrowanie i deszyfrowanie przy wykorzystaniu tych samych ustawień klucza, co znacząco ułatwia proces komunikacji. Taka konstrukcja reflektora oznacza jednak, że nie ma możliwości, aby litera tekstu jawnego została przekształcona na siebie samą. Jest to poważna słabość kryptograficzna, która została wykorzystana do złamania „Enigmy".

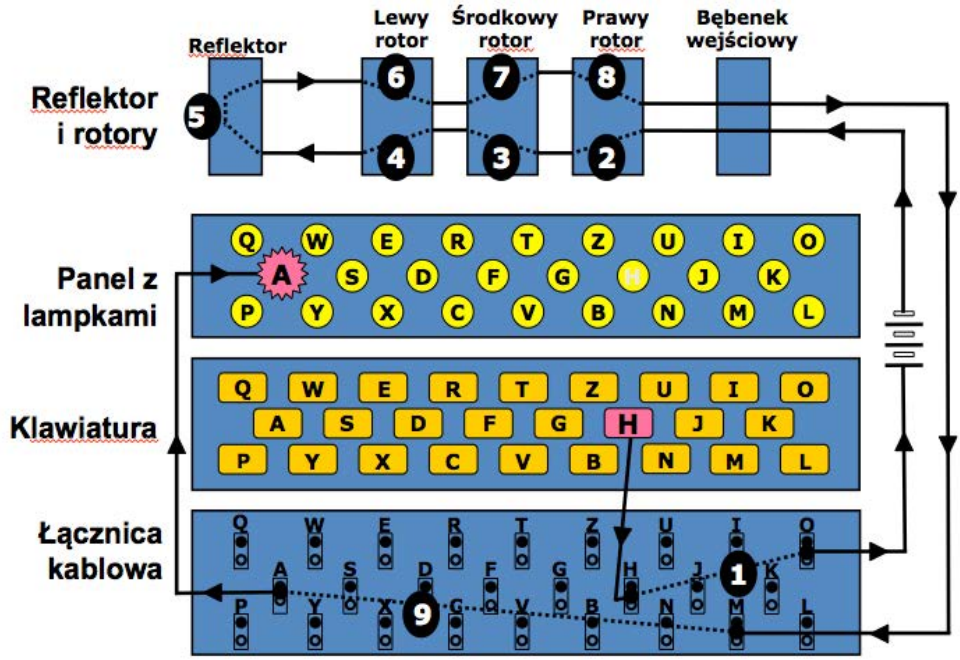


Fot. 3-4. Walec odwracający i wirnik z widocznymi stykami
Źródło: *The History and Technology of the Enigma Cipher Machine*, [on-line] [dostęp 12.05.2015]. Dostępny w World Wide Web: http://ciphermachines.com/enigma.

Panel z lampkami posiadał identyczny układ znaków jak klawiatura i łącznica kablowa. Lampki były zbudowane z żarówek latarkowych, podświetlały literę, która ze względu na brak możliwości wydruku musiała być zapisana przez drugiego operatora. Źródłem zasilania dla „Enigmy" była bateria 4,5 V lub transformator podłączony pod napięcie 220 V.

Fot. 5. Panel z lampkami
Źródło: *The History and Technology of the Enigma Cipher Machine*, [on-line] [dostęp 12.05.2015]. Dostępny w World Wide Web: http://ciphermachines.com/enigma.

Rysunek nr 1 przedstawia schemat połączeń. Liczby w owalach oznaczają numer kolejnego przekształcenia. W zależności, od tego czy dana litera byłą zamieniana przez łącznicę kablową, każda litera była przekształcana 7 lub 9 razy.



Rys. 1. Schemat połączeń maszyny szyfrującej „Enigma"
Źródło: *The History and Technology of the Enigma Cipher Machine*, [on-line] [dostęp 12.05.2015]. Dostępny w World Wide Web: http://ciphermachines.com/enigma.

Liczba ustawień

Łącznica kablowa była elementem „Enigmy", który cechował się największą złożonością kryptograficzną. Przy założeniu, że liczba połączeń jest zmienna można wykorzystać od 0 do 13 kabli. Liczbę kabli oznaczymy jako p. Liczba liter, która może zostać wybrana to liczba podzbiorów 2p elementowych zbioru 26-elementowego. Dodatkowo dla każdego wybranego podzbioru można wykonać (2p-1)·(2p-3)·(2p-5)·…·1 połączeń. W poniższej tabeli przedstawiono obliczenia dla wszystkich możliwych ustawień łącznicy kablowej.

Tabela 1. Liczba ustawień łącznicy kablowej

Liczba kabli w łącznicy (p)	Liczba kombinacji wybranych liter $\binom{26}{2p}$	Liczba możliwych połączeń w ramach wybranej grupy liter $\prod_{n=1}^{p} 2n-1$	Całkowita liczba ustawień $\binom{26}{2p}\prod_{n=1}^{p} 2n$
0	1	1	1
1	325	1	325
2	14 950	3	44 850
3	230 230	15	3 453 450
4	1 562 275	105	164 038 875
5	5 311 735	945	5 019 589 575
6	9 657 700	10 395	100 391 791 500
7	9 657 700	135 135	1 305 093 289 500
8	5 311 735	2 027 025	10 767 019 638 375
9	1 562 275	34 459 425	53 835 098 191 875
10	**230 230**	**654 729 075**	**150 738 274 937 250**
11	14 950	13 749 310 575	205 552 193 096 250
12	325	316 234 143 225	102 776 096 548 125
13	1	7 905 853 580 625	7 905 853 580 625
		Razem:	**532 985 208 200 576**

Źródło: *The History and Technology of the Enigma Cipher Machine*, [on-line] [dostęp 12.05.2015]. Dostępny w World Wide Web: http://ciphermachines.com/enigma.

Wewnętrzne połączenia wirników mogą być skonstruowane na 26! różnych sposobów. Ponieważ wykorzystywano 3 różne rotory, to liczba kombinacji jest równa $26!\cdot(26!-1)\cdot(26!-2)$, co daje około $65\cdot10^{78}$ różnych rotorów. Każdy z 3 rotorów mógł być początkowo ustawiony na dowolną literę alfabetu, stąd liczba możliwych ustawień jest równa $26^3=17.576$. Skrajny prawy wirnik przesuwa się o jedną literę po każdym naciśnięciu klawisza. Wirniki drugi i trzeci obracają się dopiero wtedy, gdy pierwszy wirnik wykona pełen obrót. Ustawienie wcięcia, które spowoduje obrót także mogło być zmieniane. Stąd liczba ustawień to 26·26=676 (wcięcie na skrajnym lewym wirniku nie miało znaczenia).

Walec odwracający zamienia litery parami, tak aby możliwe było zarówno szyfrowanie, jak i deszyfrowanie. Litera A może zatem być zamieniona na dowolną z pozostałych 25 liter, kolejna litera na dowolną z pozostałych 23 itd. Całkowita liczba ustawień jest więc równa: $25\cdot23\cdot21\cdot\ldots\cdot1=7.905.853.580.625$.

Całkowita teoretyczna liczba ustawień „Enigmy" jest równa iloczynowi liczby ustawień łącznicy kablowej, liczby możliwych rotorów, liczby ich początkowych ustawień, liczby możliwych ustawień wcięć na wirnikach oraz liczby możliwych walców odwracających. Iloczyn ten jest w przybliżeniu równy $3{,}28 \cdot 10^{114} \approx 2^{380}$. Liczba ta jest znacznie większa niż liczba wszystkich atomów w obserwowalnym wszechświecie (10^{80}).

Teoretyczna liczba ustawień nie była jednak nigdy w praktyce wykorzystywana przez nazistów. Niemieckie procedury przewidywały wykorzystanie zawsze 10 kabli w łącznicy kablowej, co dawało 150.738.274.937.250 możliwych jej ustawień. Twórcy „Enigmy" przyjęli, że maszyna ma pozostać bezpieczną, nawet wtedy, gdy okablowania wirników będą znane. W praktyce pozostawały utajnione, jednakże wykorzystywano zestaw tylko 5 z 26! wszystkich możliwych rotorów. Wirniki mogły być zakładane w dowolnej kolejności, zatem liczba wszystkich ustawień to 5x4x3=60. Liczba początkowych ustawień wirników oraz liczba wcięć pozostawały takie same jak w przypadku teoretycznym i wynosiły odpowiednio 17.576 i 676. Ustawienia walca odwracającego były znane i operatorzy nie dokonywali w nich zmian, stąd liczba wykorzystywanych ustawień to 1. Iloczyn powyższych wartości jest w przybliżeniu równy $1{,}07 \cdot 10^{23} \approx 2^{77}$.

Tak wielka liczba możliwości oznacza, że gdyby zadania łamania szyfru podjęło się jednocześnie 100 000 operatorów, sprawdzając przy tym każdy możliwy klucz w czasie 1 sekundy, to potrzebowaliby dwa razy więcej czasu do znalezienia właściwych ustawień niż wynosi wiek wszechświata. Liczba ta była tak ogromna, że twórcy „Enigmy" byli pewni, iż jest to maszyna nie do złamania. Naturalnie odporność ta jest wyliczona tylko dla ataku brutalnego, polegającego na przeszukaniu wszystkich możliwych kluczy. Warto w tym miejscu zaznaczyć, że algorytm DES, który pozostawał standardem szyfrowania do roku 2002 cechował się siłą kryptograficzną na poziomie 2^{56}.

Procedury używania „Enigmy"

Ogromna przestrzeń klucza sprawiała, że złamanie „Enigmy" metodami brutalnymi nie miało szans powodzenia. Atak powinien korzystać ze słabości konstrukcji, pracy wywiadu oraz wykorzystywać błędne procedury eksploatacji maszyny. Przyjrzyjmy się zatem procedurom stosowanym przez niemieckich operatorów.

Rozpoczęcie korzystania z „Enigmy" wymagało od użytkownika zmiany klucza dziennego. Na tę czynność składała się instalacja 3 z 5 dostępnych wirników w odpowiedniej kolejności. Następnie należało połączyć 10 par liter z wykorzystaniem łącznicy kablowej, tak jak zostało to wyszczególnione w ustawieniu dziennym. Ostatecznie należało ustawić rotory we wskazanym położeniu. Wszystkie te ustawienia były przekazywane w książce kodowej, która była dostarczana operatorom raz w miesiącu. W celu wysłania wiadomości, operator wybierał 3 literowy kod i szyfrował go dwukrotnie, następnie ustawiał 3 rotory w położenie zgodne z wybranym

kodem i wtedy dokonywał szyfrowania przekazu. Niektórzy operatorzy wybierali takie same kody 3 literowe dla większości przesyłanych przez siebie wiadomości. Często były to np. inicjały ich partnerek, kolejne litery alfabetu lub wyrazy w języku niemieckim. W późniejszym czasie wprowadzanie takich kluczy zostało zakazane.

Odszyfrowywanie wiadomości wymagało zresetowania ustawień wirników do tych podanych w książce kodowej i odszyfrowania pierwszych 6 znaków szyfrogramu. Tekst jawny powinien był składać się z 3 znaków, które były dwukrotnie powtórzone. Następnie operator ustawiał wirniki na odczytane ustawienie, dekodując tym samym pozostałą część wiadomości. W warunkach pola walki zazwyczaj jeden operator wprowadzał szyfrogram/tekst jawny, natomiast drugi zapisywał podświetlające się znaki. Często też pomagała im trzecia osoba, która przenosiła odszyfrowane rozkazy do dedykowanego odbiorcy. Podwójne wysyłanie klucza dziennego przestało być wykorzystywane krótko po rozpoczęciu II wojny światowej, tym samym utrudniając Aliantom deszyfrowanie przesyłanych wiadomości.

Naziści byli całkowicie przekonani o bezpieczeństwie „Enigmy". Pomimo licznych sytuacji, w których jasne było, że wiadomości przesyłane za jej pomocą zostały odczytane, Niemcy byli przekonani, że musiały one zostać wykradzione przez szpiegów, bądź sprzedane przez operatorów. Naturalnie, siła kryptograficzna samego urządzenia była bardzo wysoka, jednakże wybrane procedury jej użytkowania spowodowała znaczne jej osłabienie. Za główne mankamenty uznaje się brak możliwości zaszyfrowania litery tekstu jawnego w samą siebie, używanie zawsze 10 kabli w łącznicy kablowej, czy też dwukrotne przesyłanie klucza wiadomości.

Złamanie „Enigmy"

Polska była pierwszym krajem, który odnotował wykorzystanie przez Niemców nowego typu szyfru – szyfru maszynowego. Wtedy też podjęto decyzję o zakupie komercyjnej wersji „Enigmy". Niestety znaczne różnice w konstrukcji wersji komercyjnej i wojskowej nie pozwoliły na złamanie szyfru. W 1929 roku Biuro Szyfrów Oddziału II Sztabu Głównego Wojska Polskiego zorganizowało kurs kryptologii dla 20 najbardziej zdolnych studentów Uniwersytetu w Poznaniu. Trzech najbardziej utalentowanych – Marian Rejewski, Henryk Zygalski i Jerzy Różycki zostało w późniejszym czasie zatrudnionych do łamania szyfru „Enigmy".

Pierwszym, który rozpoczął analizę niemieckich szyfrogramów był Marian Rejewski. Posiadając jedynie grupy 6 liter, które powstawały w wyniku szyfrowania kluczem dziennym nowego klucza wiadomości, Rejewski zdołał odtworzyć zestaw permutacji określający sposób działania „Enigmy". Zestaw ten składa się z następujących równań:

$$A=SHR'T'R'^{-1}H^{-1}S^{-1}$$
$$B=SHQR'Q^{-1}T'QR'^{-1}Q^{-1}H^{-1}S^{-1}$$
$$C=SHQ^{2}R'Q^{-2}T'Q^{2}R'^{-1}Q^{-2}H^{-1}S^{-1}$$
$$D=SHQ^{3}R'Q^{-3}T'Q^{3}R'^{-1}Q^{-3}H^{-1}S^{-1}$$
$$E=SHQ^{4}R'Q^{-4}T'Q^{4}R'^{-1}Q^{-4}H^{-1}S^{-1}$$
$$F=SHQ^{5}R'Q^{-5}T'Q^{5}R'^{-1}Q^{-5}H^{-1}S^{-1}$$

Powyższy układ składa się z sześciu równań z czterema nieznanymi permutacjami: *S, H, R', T '*, gdzie:

- *S* – permutacja określona przez łącznicę kablową.
- *H* – stała permutacja określająca połączenia pomiędzy łącznicą kablową a bębenkiem wejściowym.
- *R'* – permutacja określana przez wewnętrzne połączenia prawego rotoru.
- *T'* – permutacja określona przez wewnętrzne połączenia wirnika środkowego, lewego i walca odwracającego.

Pozostałe permutacje to:

- *Q* – prosta permutacja, która zmienia każdą literę na literę następną, np. a na b, b na c, z na a.
- *A-E* – to znane permutacje, określone przez Rejewskiego na podstawie analizy zaszyfrowanych kluczy wiadomości.

Do dnia dzisiejszego nie jest wiadome, czy powyższy układ równań może być rozwiązany. Rejewski próbując rozwiązać ten zestaw, otrzymał materiały, które w znaczący sposób to ułatwiały. Kapitan Gustave Bertrand, szef francuskiego wywiadu radiowego dostarczył polskiemu Biuru Szyfrów dokumenty przekazane przez agenta o nazwisku Hans-Thilo Schmidt, który pracował w departamencie kryptografii niemieckiej armii. W dokumentach znajdowały się m.in. tablice kluczy dziennych dla dwóch kolejnych miesięcy (wrzesień i październik 1932 roku). Brakowało natomiast informacji dotyczących wewnętrznych połączeń wirników. Tablice kluczy dziennych pozwoliły na określenie permutacji S, określającej połączenia łącznicy kablowej. Rejewskiemu udało się także odgadnąć permutację H – okazało się, że permutacja ta w odróżnieniu od komercyjnej wersji „Enigmy" miała postać permutacji identycznościowej. Pozostałe dwie permutacje zostały określone m.in. z wykorzystaniem kolejnych materiałów dostarczanych przez francuski wywiad – niemieckich instrukcji używania „Enigmy" oraz par szyfrogram-tekst jawny dla przykładowych kluczy dziennych i wiadomości.

Ustalenie wewnętrznych połączeń wirników przez Mariana Rejewskiego nie było wystarczające do systematycznego łamania niemieckich szyfrogramów. Konieczne było opracowanie efektywnych metod, które pozwolą na wykonywanie tych czynności w jak najkrótszym czasie. W latach 1932-39 Marian Rejewski, Jerzy Różycki i Henryk Zygalski opracowali kilka metod, które były stale rozwijane ze względu na zmiany wprowadzane do procedury dystrybucji kluczy dziennych przez niemiecką armię. Do tych metod należały:

- metoda rusztu, która była wykorzystywana wraz z zegarem Różyckiego i tzw. metodą ANX,
- katalogi charakterystyk, opracowane z wykorzystaniem specjalnego urządzenia – cyklometru,
- płachty Zygalskiego,
- Bomba Rejewskiego.

Za najważniejszą z przedstawionych metod należy uznać Bombę Rejewskiego i płachty Zygalskiego. Bomba została opracowana w odpowiedzi na zmianę niemieckich procedur dokonaną 15 września 1938 roku, która spowodowała że wszystkie obecne metody nie były dłużej użyteczne. W listopadzie 1938 roku zakłady AVA wyprodukowały pierwszą Bombę zgodnie z projektem przedstawionym przez Rejewskiego. Składała się z sześciu połączonych ze sobą „Enigm", pracujących wspólnie w celu określenia prawidłowej pozycji początkowej wirników. Pełen proces określenia położeń zajmował około 2 godzin.

Metoda Zygalskiego, opracowana pod koniec 1938 roku wymagała wykorzystania specjalnych perforowanych arkuszy papieru. Sposób ten wykorzystywał fakt, że tylko około 40% ze wszystkich 263 ustawień rotorów prowadziło do permutacji AD, która zawierała co najmniej jedną parę jednoliterowych cykli (a1) (a2). Dla każdego z ustawień lewego rotora tworzona była oddzielna płachta, zawierająca macierz wszystkich ustawień prawego i środkowego wirnika. Pola macierzy odpowiadające pozycjom wirnika z jednoliterowymi cyklami były perforowane. W przypadku wykorzystania zestawu 3 rotorów istniało 6 kombinacji ich ustawienia. Dla każdego z ustawień należało wytworzyć zestaw 26 płacht. Ze względu na ograniczone zasoby Biura Szyfrów do wybuchu wojny wytworzono tylko dwa zestawy płacht, dodatkowo 15 grudnia 1938 roku Niemcy wprowadzili dwa dodatkowe rotory, co spowodowało zwiększenie liczby możliwych kombinacji ich ustawienia z 6 do 60. Sytuacja ta spowodowała, że możliwości dekodowania niemieckich szyfrogramów znacząco się zmniejszyły na zaledwie kilka miesięcy przed wybuchem II wojny światowej.

W dniach 24-26 lipca 1939 roku w Pyrach, w lesie Kabackim, odbyło się historyczne spotkanie wywiadów polskiego, francuskiego i brytyjskiego. Ze strony polskiej było tam trzech kryptologów – Rejewski, Różycki i Zygalski oraz dwóch oficerów Biura Szyfrów – ppłk dypl. Gwido Langer i mjr Maksymilian Ciężki, ze strony francuskiej byli to Gustave Bertrand i Henri Braquenie, ze strony brytyjskiej Alastair Denniston, Alfred D. Knoc oraz Humprey Sandwich. Podczas spotkania Polacy przekazali dwie kopie zrekonstruowanej „Enigmy" dla każdego z wywiadów, kompletną dokumentację płacht Zygalskiego oraz Bomby Rejewskiego oraz innych metod wykorzystywanych do tej pory przez polskich kryptoanalityków. Przedstawiciele francuskiego i brytyjskiego wywiadu byli kompletnie zaskoczeni, gdyż aż do tej chwili nie mieli jakiejkolwiek wiedzy na temat złamania „Enigmy" przez Polaków, sami też nie poczynili znaczących postępów w łamaniu jej szyfru.

W lecie 1939 roku rząd brytyjski przeniósł swoją komórkę odpowiedzialną za łamanie szyfrów do Bletchley Park. Brytyjczycy, wzorem Polaków, także zatrudnili matematyków do kryptoanalizy, a dwóch z nich Alan Turing oraz Gordon Welchmann w największym stopniu przyczynili się do sukcesu w łamaniu „Enigmy". Początkowo, Brytyjczycy stosowali polskie metody. Wytworzyli komplet wszystkich 60 zestawów płacht Zygalskiego. Za największy sukces brytyjskich kryptologów należy uznać wytworzenie Bomby, która podobnie jak Bomba Rejewskiego służyła do maszynowego przyspieszania obliczeń niezbędnych do łamania szyfrogramów. W odróżnieniu od polskiej Bomby, wersja brytyjska nie bazowała już na wadliwej procedurze dystrybucji kluczy, lecz na ataku ze znanym tekstem jawnym (konw-plaintext attack). Wykorzystywano tu przede wszystkim typową zawartość niemieckich wiadomości, taką jak zapisywanie pełnych danych odbiorców i nadawców, wliczając w to pełne tytuły i afiliacje, a także typowe zwroty grzecznościowe. Pierwsze brytyjskie Bomby zaczęły być wykorzystywane w październiku 1941 roku. Do końca wojny zbudowano 210 takich urządzeń.

Podsumowanie

Informacje dotyczące złamania kodu „Enigmy" pozostawały utajnione aż do roku 1974, pomimo że nad jego łamaniem pracowało blisko 11 tysięcy ludzi w Bletchley Park i blisko tysiąc kolejnych w Stanach Zjednoczonych. Krótko po wojnie Wielka Brytania i USA przekazały przejęte maszyny „Enigma" innym krajom, w tym swoim sojusznikom. Były one użytkowane przez kolejne 30 lat, a tym samym wszystkie wiadomości przesyłane z ich wykorzystaniem były odczytywane przez wywiad brytyjski i amerykański. Łącznie wyprodukowano blisko 30 tysięcy egzemplarzy „Enigmy", większość z nich została zniszczona podczas wojny i tuż po niej. Obecnie pozostało mniej niż 350 egzemplarzy tej maszyny szyfrującej, z czego połowa znajduje się w prywatnych kolekcjach.

Wprowadzenie do powszechnego użycia szyfrów maszynowych ujawniło słabości dotychczas stosowanych metod kryptoanalitycznych. Ogromna przestrzeń klucza powodowała, że ręczna analiza szyfrogramów w poszukiwaniu zastosowanego klucza była zbyt czasochłonna. Analiza przechwytywanych szyfrogramów wymagała zastosowania maszyn przyśpieszających najbardziej żmudne obliczenia. Szyfrogramy „Enigmy" były łamane z wykorzystaniem maszyn elektromechanicznych – Polacy stosowali Bombę złożoną z 6 maszyn „Enigma", brytyjski odpowiednik był zbudowany z 36 takich maszyn. „Enigma" nie była jedyną maszyną szyfrującą stosowaną przez nazistów. Komunikacja dowództwa wysokiego szczebla odbywała się z wykorzystaniem maszyny Lorenza.

Komunikacja ta wykorzystywała dalekopis, co wymuszało stosowanie pięciobitowego kodu Baudot, reprezentującego każdą literę w formie zapisu binarnego. Z punktu widzenia kryptografii, implementowany szyfr był szyfrem strumieniowym.

Proces kryptoanalizy przesyłanych szyfrogramów wymagał wykonywania wielu specyficznych czasochłonnych operacji. Rozwiązaniem było zbudowanie komputera, który będzie w stanie wykonać je znacznie szybciej i bezbłędnie.

W grudniu 1943 roku przedstawiono prototyp urządzenia o nazwie Colossus – pierwszego programowalnego komputera cyfrowego. Jego twórcami byli Tommy Flowers i Alan Turing. Urządzenie to stało się podstawą do dalszego rozwoju techniki cyfrowej, a także do rozwoju stosowanych technik kryptograficznych. Wraz z dalszym rozwojem komputerów, szyfry operujące na znakach i ich przekształceniach przestały mieć praktyczne znaczenie. Wytworzone zostały nowe szyfry, o znacznie większej złożoności, które nie operowały już na znakach, lecz na bitach, co dało początek nowej ery dla światowej kryptografii i kryptoanalizy.

Bibliografia

Druki zwarte:

Gaj K., *German Cipher Machine Enigma – Methods of Breaking*, Wydawnictwa Komunikacji i Łączności, Warszawa, 1989;

Gaj K., Orłowski A., *Facts and myths of Enigma: breaking stereotypes. In Eurocrypt 2003*, Warszawa, 2003;

Gaj K., *Szyfr Enigmy: metody złamania*, Wydawnictwa Komunikacji i Łączności, Warszawa 1989;

Grajek M., *Enigma: bliżej prawdy*, Wydawnictwo Rebis, 2007;

Kahn D., *Seizing the Enigma*, Houghton Mifflin, Boston, MA, 1991;

Kahn D., *The Codebreakers: The Story of Secret Writing*, 2 edition, Scribner, New York, 1996;

Kozaczuk W., *Enigma: how the German Machine Cipher Was Broken, and How It Was Read by the Allies in World War Two*, University Publications of America, (1984).

Strony internetowe:

http://ciphermachines.com/enigma, [on-line] [dostęp 12.05.2015].

Abstract

Breaking of the "Enigma" code is definitely the biggest cryptanalyst success in the history of the mankind. The work done by the employees of the Polish Cipher Bureau

shortened the war by ca 2 years and saved millions of lives. The high technological level and innovativeness of "Enigma" required unorthodox approach in the process of revealing its secrets. Previously used linguistic analysis was useless, so the authorities of the Second Polish Republic decided to employ mathematics for breaking the "Enigma" code. The first success came after 3 years, when Marian Rejewski revealed the internal connections of the rotors. From then on "Enigma" was no longer a mystery.

w: Polska myśl techniczna w II wojnie światowej w 70 rocznicę zakończenia działań wojennych w Europie. Materiały pokonferencyjne. Centralna Biblioteka Wojskowa, ISBN 978-83-63050-28-3, Warszawa 2015, s. 53-65