informatyka+

Algorytmika i programowanie

Bazy danych

Multimedia, grafika i technologie internetowe

Sieci komputerowe

Tendencje w rozwoju informatyki i jej zastosowań

Człowiek – najlepsza inwestycja

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Warszawska Wyższa Szkoła Informatyki

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.

informatyka+

Wszechnica Popołudniowa: Tendencje w rozwoju informatyki i jej zastosowań

Od złamania Enigmy do współczesnej kryptologii

Jerzy Gawinecki

Człowiek – najlepsza inwestycja

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Warszawska Wyższa Szkoła Informatyki

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.

Od złamania Enigmy do współczesnej kryptologii

Rodzaj zajęć: Wszechnica Popołudniowa
Tytuł: Od złamania Enigmy do współczesnej kryptologii
Autor: prof. dr hab. n. mat. Jerzy Gawinecki

Redaktor merytoryczny: prof. dr hab. Maciej M Sysło

Zeszyt dydaktyczny opracowany w ramach projektu edukacyjnego **Informatyka+** — ponadregionalny program rozwijania kompetencji uczniów szkół ponadgimnazjalnych w zakresie technologii informacyjno-komunikacyjnych (ICT).
www.informatykaplus.edu.pl
kontakt@informatykaplus.edu.pl

Wydawca: Warszawska Wyższa Szkoła Informatyki
ul. Lewartowskiego 17, 00-169 Warszawa
www.wwsi.edu.pl
rektorat@wwsi.edu.pl

Projekt graficzny: FRYCZ I WICHA

Warszawa 2010

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

Warszawska Wyższa Szkoła Informatyki

UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ SPOŁECZNY

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.

Od złamania Enigmy do współczesnej kryptologii

Jerzy Gawinecki
Instytut Matematyki i Kryptologii
Wydział Cybernetyki
Wojskowa Akademia Techniczna
jgawinecki@wat.edu.pl

Streszczenie

Wykład składa się z trzech części.

Pierwsza część jest poświecona ukazaniu roli kryptologii w wielu historycznych wydarzeniach począwszy od czasów starożytnych po złamanie Enigmy.

Druga część jest poświęcona dokonaniom polskich kryptologów Mariana Rejewskiego, Jerzego Różyckiego i Henryka Zygalskiego w złamaniu Enigmy. Wykazanie, że polscy kryptolodzy dokonali przełomu w kryptoanalizie stosując metody matematyczne oparte na teorii permutacji. Od tej pory datuje się przełom w kryptoanalizie. Zostanie podkreślone również znaczenie złamania Enigmy dla skrócenia czasu trwania II Wojny Światowej.

Część trzecia wykładu jest poświęcona współczesnej kryptologii począwszy od złamania Enigmy a skończywszy na współczesnych dokonaniach. Podkreślone zostaną zagrożenia, jakie niesie ze sobą wykorzystanie komputerów w przesyłaniu informacji, w szczególności zostanie omówiony cyberterroryzm.

Spis treści

1. Zanim złamano Enigmę 5

2. Tło historyczne 6

3. Złamanie Enigmy 7

4. Od Enigmy do współczesnej kryptologii 12

Literatura 13

Tam sięgaj, gdzie wzrok nie sięga.
Łam, czego rozum nie złamie.
[A. Mickiewicz]

1. ZANIM ZŁAMANO ENIGMĘ

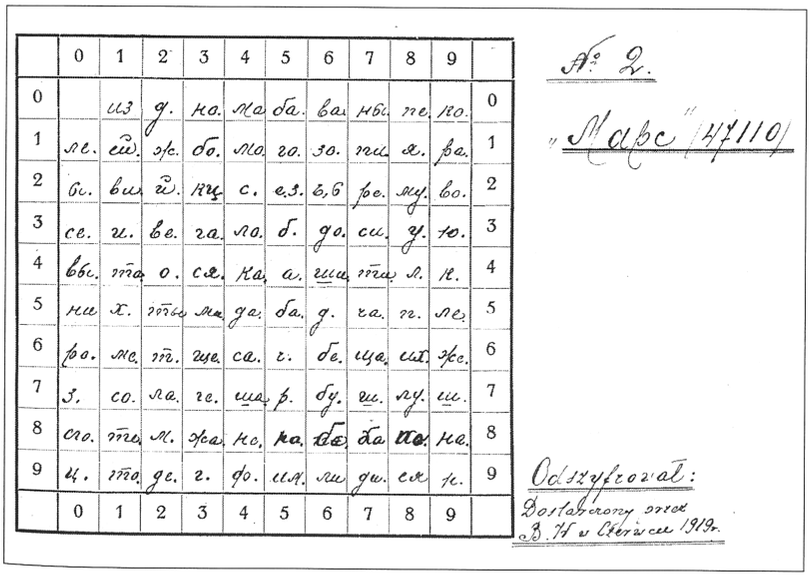
Ogromnym przełomem w kryptologii było zastosowanie w kryptoanalizie, a później także w kryptografii metod matematycznych. Uczynili to po raz pierwszy przed II Wojną Światową, polscy matematycy. Zastosowanie przez nich ***teorii permutacji*** umożliwiło kryptoanalitykom złamanie niemieckiego szyfru maszyny Enigma, co z kolei miało wpływ, według słów premiera Wielkiej Brytanii Winstona Churchilla, na skrócenie wojny o dwa, trzy lata.

Ale sukcesy polskiej kryptoanalizy w walce z Enigmą nie były pierwszymi. Najnowsze prace historyczne odtajniły niedawno fakt łamania przez Polskę radzieckich szyfrów podczas wojny w 1920 roku. Oznacza to, że polska szkoła kryptoanalizy nie zaczęła się od zatrudnienia matematyków do łamania Enigmy, ale była wynikiem prac rozpoczętych wraz z odzyskaniem niepodległości.

Najbardziej znany specjalista od historii kryptologii, profesor uniwersytetu w Oksfordzie David Kahn, autor książki *Łamacze kodów* [3] twierdzi, że dobrzy specjaliści z kryptologii pochodzą z krajów wielojęzycznych i wielokulturowych. I jak mówi „muszą być tam uniwersytety z matematyką na wysokim poziomie i coś jeszcze – improwizacja: musi być tam komponowana muzyka." Bo matematyka to logiczne myślenie, a muzyka to kwestia wyobraźni.

Jeszcze przed sukcesem złamania szyfrów Enigmy, w latach dwudziestych brali udział zatrudnieni po raz pierwszy w historii kryptologii wybitni polscy profesorowie matematyki: Stefan Mazurkiewicz, Wacław Sierpiński i Stanisław Leśniewski.

Wybitny polski matematyk, profesor Wacław Sierpiński – twórca polskiej szkoły matematycznej, autor prac z dziedziny teorii funkcji rzeczywistych, teorii liczb i teorii mnogości wraz z profesorem Stefanem Mazurkiewiczem, jednym z założycieli słynnej na cały świat warszawskiej szkoły logicznej, i profesorem Stanisławem Leśniewskim – specjalistą od logiki matematycznej z Wydziału Matematyki i Nauk Przyrodniczych Uniwersytetu Warszawskiego, wspólnymi siłami złamali około setki rosyjskich szyfrów podstawieniowych, którymi posługiwali się dowódcy wojsk rosyjskich. Pozwoliło to w oparciu o systematycznie prowadzone nasłuchy radiowe stacji bolszewickich na przechwycenie i rozszyfrowanie kilku tysięcy rosyjskich radiodepesz, a tylko w samym sierpniu 1920 roku, czyli w okresie przesilenia wojny, blisko 500.



Rysunek 1.
Odszyfrowany szyfr sowiecki MARS

Złamanie rosyjskich szyfrów dostarczyło Sztabowi Generalnemu szerokiej i pełnej wiedzy o przeciwniku i dawało polskiej stronie znaczną przewagę w trzech wymiarach: taktycznym, operacyjnym i strategicznym. Można powiedzieć, że marszałek Józef Piłsudski miał tak dokładne informacje, jakich do jego czasów nie miał żaden dowódca w żadnej wojnie. W konsekwencji doprowadziło to do „cudu nad Wisłą" i zatrzymania nawałnicy bolszewickiej, co jak wiemy zmieniło historię Polski i Europy.

Do rangi symbolu urasta bolszewicki szyfr Rewolucja. Złamali go wspólnie w sierpniu 1920 roku dwaj polscy kryptoanalitycy – bardzo zasłużony, pochodzący z Łodzi chemik, talent matematyczny i lingwistyczny, porucznik Jan Kowalewski, odznaczony za zasługi w roku 1921 przez szefa Sztabu Generalnego gen. Władysława Sikorskiego najwyższym odznaczeniem państwowym Krzyżem Virtuti Militarii, oraz profesor Stefan Mazurkiewicz, o którym już wcześniej wspomniano.

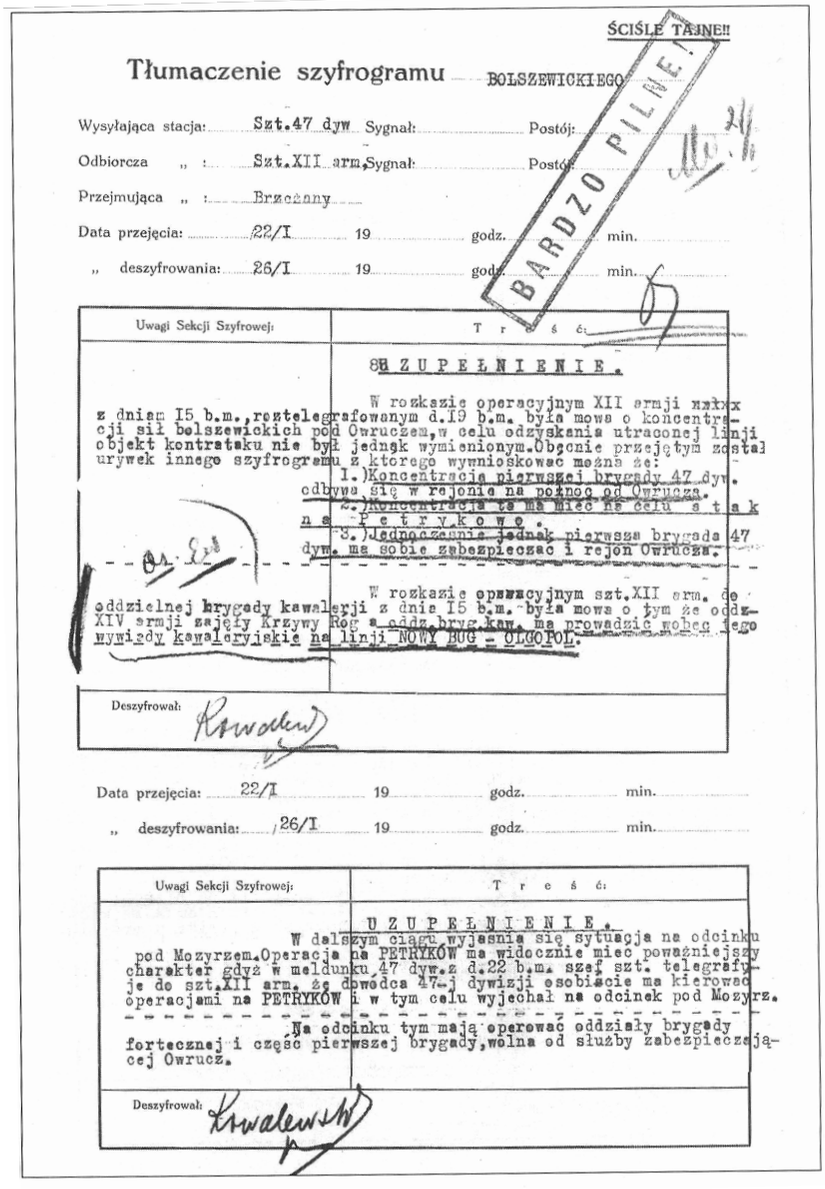
Rysunek 2.
mjr Jan Kowalewski

Złamanie szyfru Rewolucja i dziesiątków innych szyfrów rosyjskich przez Polaków, profesorów matematyki, profesorów logiki, studentów i oficerów, zaowocowało później złamaniem niemieckiego szyfru maszynowego Enigma.

W czasach współczesnych ujawniono skrywane przez dziesięciolecia tajemnice funkcjonowania polskiego Biura Szyfrów i jego niezwykłe sukcesy odniesione podczas wojny z bolszewicką Rosją w latach 1918-1920. Systematyczne łamanie kluczy szyfrowych nieprzyjaciela umożliwiło odczytanie kilku tysięcy bolszewickich szyfrogramów i miało wielki wpływ na zwycięstwo odniesione w tej wojnie. Dzięki pracy między innymi por. Jana Kowalewskiego i odczytaniu wielu rozkazów i meldunków radzieckich marszałek Piłsudski posiadał taką wiedzę na temat wojsk przeciwnika, jakiej być może nie posiadał żaden inny dowódca wcześniej. Te sukcesy sprawiły, że polski kontrwywiad przygotowywał się przed II Wojną Światową także do walki kryptologicznej z Niemcami.

2 TŁO HISTORYCZNE

Można powiedzieć, że walka między kryptografami a kryptoanalitykami przed II Wojną Światową weszła w nową fazę. Po raz pierwszy zaczęto stosować do szyfrowania urządzenia mechaniczno-elektryczne. Przykładem takiej maszyny była Enigma. Zastosowanie tej maszyny przez Niemców zmusiło początkowo do „kapitulacji" angielskich kryptoanalityków, którzy stwierdzili, że tego szyfru nie można złamać, natomiast Francuzom udało się uzyskać cenne informacje o Enigmie opłacając niemieckiego szpiega Hansa Szmidta o pseudonimie Asche. Sami Niemcy do końca wojny byli przekonani o nienaruszalnej sile Enigmy. Jedynie Polacy, nauczeni sukcesem wojny bolszewickiej, nie powiedzieli „nie" i przystąpili do działań w kierunku złamania tego szyfru. Wykorzystano potencjał polskich matematyków tym razem z Poznania. O sukcesie Polaków zadecydowały trzy czynniki: strach, matematyka i szpiegostwo. Gdyby nie strach przed inwazją Polacy zapewne uważaliby, że złamanie szyfru jest niemożliwe (bo wszystkich konfiguracji ustawień w maszynie Enigma jest czterysta sekstylionów czyli 4×10^{26} – więcej niż liczba sekund, jakie upłynęły od początku świata zakładając, że świat istnieje od pięciu miliardów lat – liczba kluczy, według których można kodować tekst za pomocą Enigmy, to 10 bilionów czyli 1×10^{10}.



ŚCIŚLE TAJNE!!

BARDZO PILNE!

Tłumaczenie szyfrogramu BOLSZEWICKIEGO

Wysyłająca stacja: Szt.47 dyw Sygnał: Postój:

Odbiorcza „ : Szt.XII arm. Sygnał: Postój:

Przejmująca „ : Brzeżany

Data przejęcia: 22/I 19 godz. min.

„ deszyfrowania: 26/I 19 godz. min.

Uwagi Sekcji Szyfrowej:	T r e ś ć:
	8B U Z U P E Ł N I E N I E . W rozkazie operacyjnym XII armji z dniem I5 b.m., rozt elegrafowanym d.I9 b.m. była mowa o koncentracji sił bolszewickich pod Owruczem, w celu odzyskania utraconej linji objekt kontrataku nie był jednak wymienionym. Obecnie przejętym został urywek innego szyfrogramu z ktorego wywnioskowac można że: 1.) Koncentracja pierwszej brygady 47 dyw. odbywa się w rejonie na północ od Owrucza. 2.) Koncentracja ta ma miec na celu s t a k n s P e t r y k o w e . 3.) Jednoczenie jednak pierwsza brygada 47 dyw. ma sobie zabezpieczac i rejon Owrucza. W rozkazie operacyjnym szt.XII arm. do oddzielnej brygady kawalerji z dnia I5 b.m. była mowa o tym że oddz. XIV armji zajęły Krzywy Róg a oddz.brygkaw. ma prowadzic wobec tego wywiedy kawaleryjskie na linji NOWY HUC - OLGOPOL.
Deszyfrował: Kowalewski	

Data przejęcia: 22/I 19 godz. min.

„ deszyfrowania: 26/I 19 godz. min.

Uwagi Sekcji Szyfrowej:	T r e ś ć:
	U Z U P E Ł N I E N I E . W dalszym ciągu wyjaśnia się sytuacja na odcinku pod Mozyrzem. Operacja na PETRYKÓW ma widocznie miec poważniejszy charakter gdyż w meldunku 47 dyw. z d.22 b.m. szef szt. telegrafuje do szt. XII arm. że dowodca 47-j dywizji osobiście ma kierowac operacjami na PETRYKÓW i w tym celu wyjechał na odcinek pod Mozyrz. Na odcinku tym mają operowac oddziały brygady fortecznej i część pierwszej brygady, wolna od służby zabezpieczającej Owrucz.
Deszyfrował: Kowalewski	

Rysunek 3.
Tłumaczenie odszyfrowanego meldunku

Bez matematyki Marian Rejewski nie byłby w stanie zanalizować łańcuchów. A bez dokumentów, dostarczonych przez Schmidta o pseudonimie Asche, Polacy nie znaliby wewnętrznych połączeń w bębenkach i nie mogliby rozpocząć kryptoanalizy. Szybko zorientowano się, że Niemcy wykorzystują zmodyfikowaną wersję handlowej maszyny Enigma. Tu dopomógł przypadek. Na przełomie 1932 i 1933 roku w Biurze Szyfrów w Pyrach odtworzono wewnętrzne połączenia Enigmy i w konsekwencji zbudowano jej działającą replikę. Atak Mariana Rejewskiego na Enigmę (razem z Jerzym Różyckim i Henrykiem Zygalskim) był jednym z największych osiągnięć w historii kryptoanalizy i miał znaczący wpływ na dalsze losy wojny.

3 ZŁAMANIE ENIGMY

Opiszemy teraz zdarzenie, które dokonało przełomu w kryptologii na miarę Przełomu Kopernikańskiego. Było to złamanie szyfru maszyny Enigma. Przy okazji można przytoczyć opinie wybitnych polityków: premiera Wielkiej Brytanii Winstona Churchilla oraz prezydenta USA Billa Clintona o wpływie złamania Enigmy na losy II Wojny Światowej.

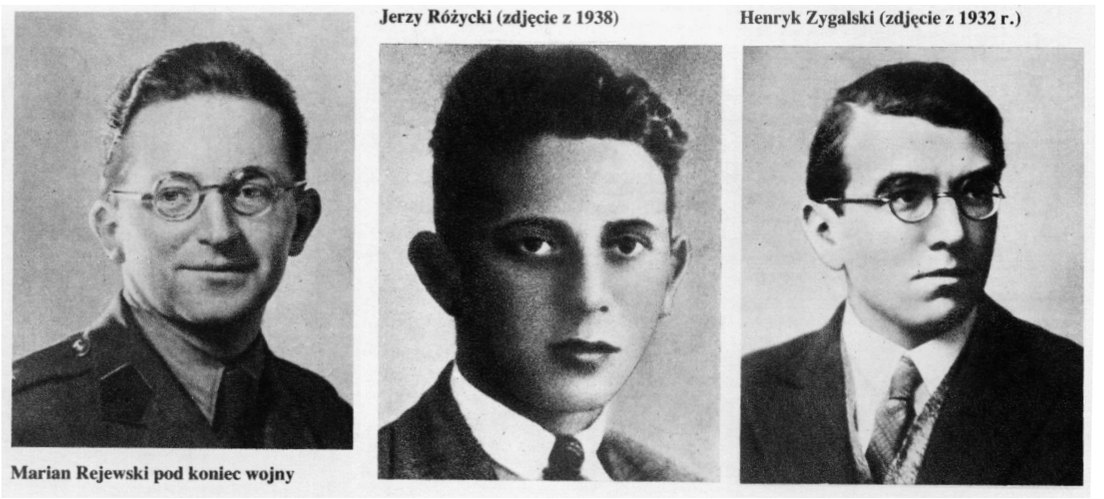
Według słów premiera Wielkiej Brytanii Winstona Churchila – gdyby nie złamanie Enigmy, dzięki której między innymi zniszczono dużą liczbę niemieckich łodzi podwodnych na Atlantyku, wojna skończyłaby się znacznie później bo w 1948 r. zrzuceniem bomby atomowej na Niemcy.

Natomiast Bill Clinton, jako prezydent USA w 1994 roku powiedział w Polskim Sejmie: *For it was the Polish mathematicians from the laboratories of Posen who brake the secrets of the Enigma Code – what Winston Churchill called the most important weapon against Hitler and his armes. It was these code-breakers who made possible the great Allied landings at Normandy, when American, English, French, Canadian, and yes free Polish forces joined together to liberate this continent – to destroy one terrible tyranny that darkened our century.*

A teraz trochę historii. Enigma z łaciny to zagadka. Ta maszyna powstała w Niemczech w 1918 roku, a jej wynalazcą był Hugo Koch, który sprzedał jej patent inżynierowi Arturowi Scherbiusowi. Planowanymi użytkownikami tej maszyny miały być korporacje, wielkie firmy chcące chronić swoją korespondencję, poczty a także inne instytucje państwowe. Początkowo armia niemiecka nie była zainteresowana wprowadzeniem maszyn szyfrujących na miejsce powszechnego w tym czasie kodu ręcznego, jednakże plany remilitaryzacji Republiki Weimarskiej a także odkrycie, iż służby Królestwa Brytyjskiego czytały depesze niemieckie w czasie I wojny światowej spowodowały, że dowództwo niemieckie zdecydowało się na wprowadzenie kodu maszynowego, stanowiącego gwarancje zachowania bezpieczeństwa przekazywania informacji. Ulepszona wersja Enigmy pojawiła się po raz pierwszy na wyposażeniu niemieckiej armii już w 1926 roku, najpierw w marynarce wojennej, a dwa lata później w siłach lądowych

W 1929 roku w Instytucie Matematyki Uniwersytetu Poznańskiego na zlecenie Sztabu Głównego Wojska Polskiego zorganizowano kurs kryptologii dla studentów matematyki. Wyłonieni w trakcie tego kursu Marian Rejewski, Jerzy Różycki, Henryk Zygalski podjęli pracę nad niemieckimi szyframi w Biurze Szyfrów Sztabu Głównego Wojska Polskiego w Warszawie. W tym czasie mocarstwa zachodnie były przekonane, że złamanie algorytmu szyfrującego Enigmy jest niemożliwe i nie podejmowały jakichkolwiek prób.

Rejewski zaczął pracować nad deszyfracją maszyny Enigmą w 1932 roku. W tym czasie do szyfrowania zaczęto po raz pierwszy używać maszyn kryptograficznych. Po doświadczeniach z wielu wieków walki między kryptografami i kryptoanalitykami zauważono, że szyfrowanie ręczne nie daje wystarczającego bezpieczeństwa. Bo to co człowiek zaszyfruje, człowiek potrafi złamać.

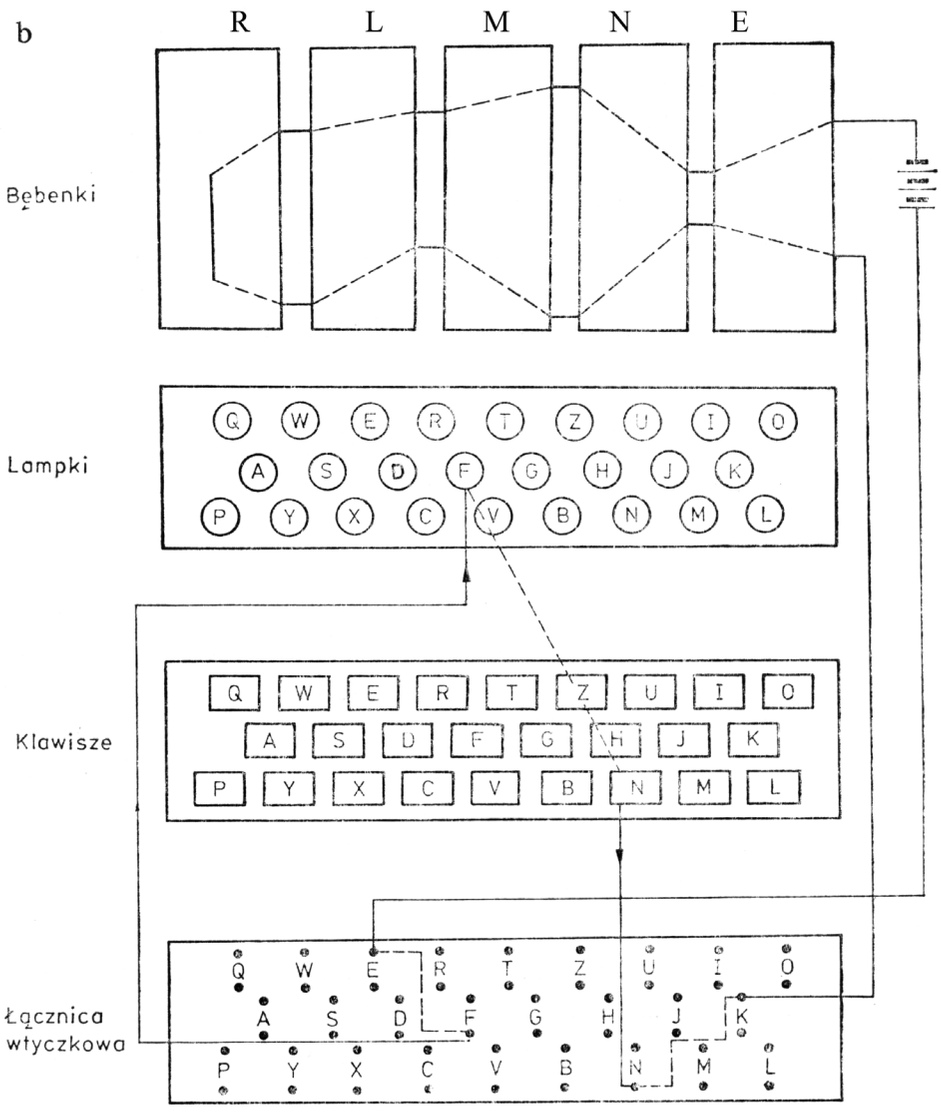


Rysunek 4.
Polscy pogromcy Enigmy

Enigma jest maszyną mechaniczno-elektryczną, ma wymiary i wygląd przenośnej maszyny do pisania. Głównymi częściami składowymi maszyny są:

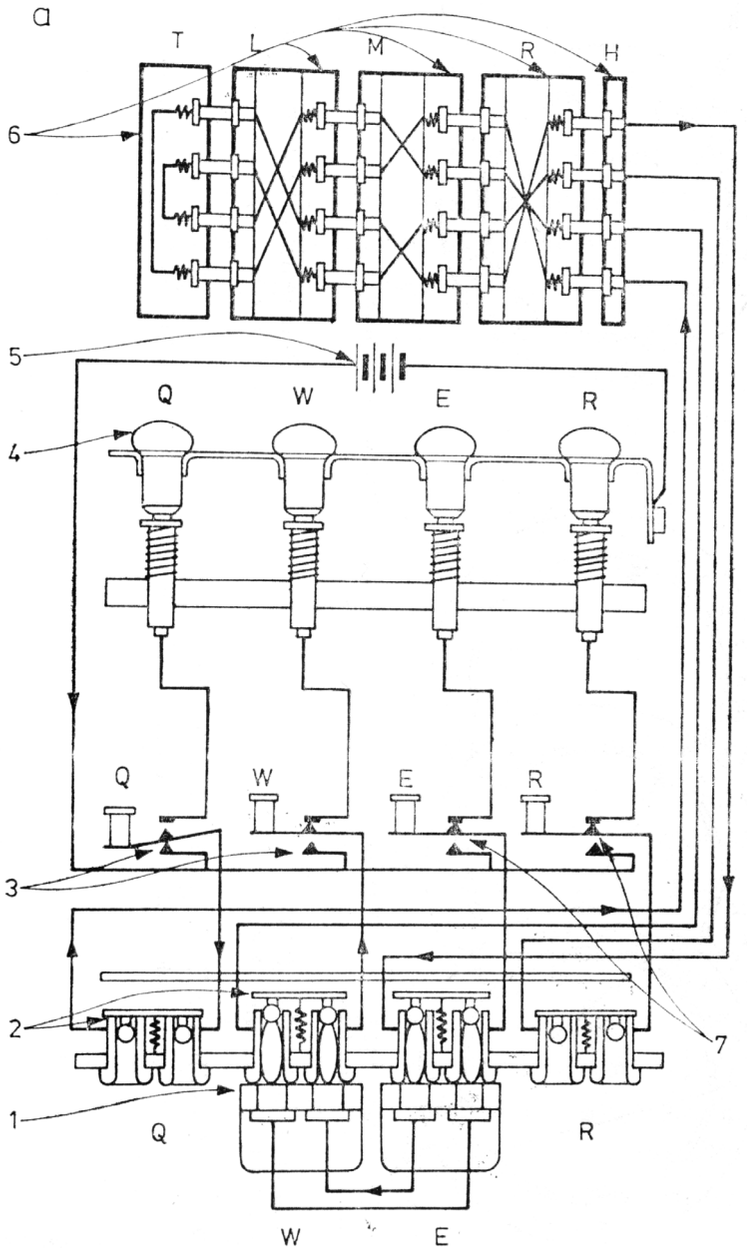
- klawiatura,
- zestaw lampek oświetlających,
- bębenki tworzące zasadniczą cześć maszyny tzw. mieszacz (ang. *scramble-unit*),
- łącznica wtyczkowa,

Rysunek 5.
Pomnik Mariana Rajewskiego w Bydgoszczy



Rysunek 6.
Schemat działania maszyny Enigma

- bateria zasilająca,
- mechanizm obrotowy,
- bęben odwracający (R),
- trzy bębenki szyfrujące (L, M, N),
- bębenek wstępny (E).



Rys. 4. Enigma wojskowa
a) schemat, b) przykładowy obwód prądu
1 — wtyczki, *2* — gniazdka, *3* — wyłączniki *Q* i *W*, *4* — lampki, *5* — bateria, *6* — bębenek odwracający *T*, trzy bębenki szyfrujące *L, M, R, i* bębenek wstępny *H*, *7* — wyłączniki *E* i *R*

Rysunek 7.
Schemat działania Enigmy wojskowej

Naciśnięcie dowolnego klawisza na klawiaturze powoduje zamknięcie obwodu z prądem, który płynie przez:

- łącznicę wtyczkową,
- bębenek wstępny (E),
- bębenki szyfrujące (N, M, L) ,
- bębenek odwracający (R),
- ponownie przez trzy bębenki szyfrujące (L, M, N),

- bębenek wstępny (E) i łącznicę,
- do określonej lampki, która zapala się.

Mechanizm obrotowy Enigmy jest oparty na zasadzie licznika. Po naciśnięciu klawisza prawy bębenek zawsze obraca się o 1/26 kąta pełnego, bębenki środkowy i lewy zwykle pozostają nieruchome, każdy następny bębenek obraca się po pełnym obrocie bębenka poprzedniego. W ten sposób każda następna litera jest szyfrowana przy innych położeniach bębenka co sprawia, że naciskając kilka razy ten sam klawisz pod rząd uzyskuje się zapalenie coraz to innych lampek. Fakt ten implikuje m.in. charakterystyczną dla szyfru maszynowego cechę polegającą na tym, że zaszyfrowane teksty dowolnej długości cechuje prawie idealnie równe częstości występowania poszczególnych liter. Równie ważną cechą wynikającą wprost ze schematu połączeń elektrycznych Enigmy jest fakt, że proces szyfrowania i deszyfrowania są identyczne.

Rozszyfrowywanie tekstu polega na wystukaniu utajnionego tekstu na Enigmę przy takich samych połączeniach łącznicy oraz kolejnych ustawieniach wirników.

Kluczem maszyny Enigma było ustawienie kolejności i pozycji początkowych trzech wymiennych bębenków, a także połączenia w łącznicy. W sumie liczba możliwych kluczy była ogromna nawet na dzisiejsze warunki, wynosiła bowiem około 10^{22}, co oznacza, że Enigma była porównywalna ze współczesnymi szyframi o długości kluczy na poziomie 75 bitów. Oprócz zmienianych codziennie kluczy Polacy nie znali budowy samej Enigmy, a zwłaszcza połączeń wewnętrznych w poszczególnych bębenkach.

Genialnym pomysłem Mariana Rejewskiego było zastosowanie do opisu budowy i działania Enigmy aparatu matematycznego, a konkretnie teorii permutacji. Proces przebiegu prądu przez łącznicę i bębenki szyfrujące zapisał on za pomocą równań permutacyjnych o nieznanych permutacjach *N*, *M*, *L*, *R*.

$$A = SPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}S^{-1}$$
$$B = SP^{2}NP^{-2}MLRL^{-1}M^{-1}P^{2}N^{-1}P^{-2}S^{-1}$$
$$\ldots$$
$$E = SP^{5}NP^{-5}MLRL^{-1}M^{-1}P^{5}N^{-1}P^{-5}S^{-1}$$
$$F = SP^{6}NP^{-6}MLRL^{-1}M^{-1}P^{6}N^{-1}P^{-6}S^{-1}$$

Korzystając między innymi z błędów popełnianych przez niemieckich szyfrantów wyznaczył znane iloczyny permutacji:

$$AD = SPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{3}NP^{-4}MLRL^{-1}M^{-1}P^{4}N^{-1}P^{-4}S^{-1}$$
$$BE = SP^{2}NP^{-2}MLRL^{-1}M^{-1}P^{2}N^{-1}P^{3}NP^{-5}MLRL^{-1}M^{-1}P^{5}N^{-1}P^{-5}S^{-1}$$
$$CF = SP^{3}NP^{-3}MLRL^{-1}M^{-1}P^{3}N^{-1}P^{3}NP^{-6}MLRL^{-1}M^{-1}P^{6}N^{-1}P^{-6}S^{-1}$$

W ten sposób skonstruował układ równań permutacyjnych z ogromną liczbą niewiadomych. W celu rozwiązania tego układu udowodnił następujące twierdzenie:

Twierdzenie. Jeżeli znane są permutacje *A* oraz *T*, to permutacja

$$B = T^{-1}AT$$

i permutacja *A* mają rozkład na iloczyn cykli rozłącznych o odpowiadających sobie cyklach o tej samej długości.

Z uwagi na wkład tego twierdzenia w złamanie Enigmy i z kolei wpływ złamania Enigmy na przebieg II Wojny Światowej, twierdzenie to nazwano: *Twierdzeniem, które wygrało II wojnę światową*. Na bazie tego twierdzenia Rejewski rozwiązał układ równań permutacyjnych. Odtworzył wszystkie nieznane permutacje, czyli zrekonstruował wewnętrzne połączenia bębenków Enigmy.

Odtworzona permutacja *N*:

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

Na tej podstawie zbudowano kopię Enigmy i można było codziennie znajdywać jej klucze, a w konsekwencji odszyfrowywać niemieckie meldunki.

Rejewski jest uważany za twórcę nowoczesnej kryptologii ze względu na głębokie i skuteczne zastosowanie matematyki do kryptoanalizy.

Dopuszczeni tuż przed wybuchem wojny, a dokładnie 25 lipca 1939 roku, do tej tajemnicy przekazanej przez Polaków, najpierw Francuzi, a później Anglicy umiejętnie wykorzystali i rozwinęli polskie koncepcje tworząc w Blechley Park pod Londynem sprawnie działający ośrodek dekryptażu. To właśnie w Blechley Park zbudowano pierwszy komputer lampowy Colossus, który służył do łamania szyfrów maszyn Enigma i Lorentza, używanej przez niemiecki Sztab Generalny do komunikacji między Hitlerem i jego generałami.

Z okazji 100. rocznicy urodzin Mariana Rejewskiego, jednego z matematyków, którzy złamali szyfr maszyny Enigma, w Wojskowej Akademii Technicznej odbyła się międzynarodowa konferencja naukowa. Obecny na niej Prezes Międzynarodowego Stowarzyszenia Badań Kryptologicznych (IACR) Andy Clark podkreślił, że polscy kryptolodzy złamali szyfry niemieckie i sowieckie. W konferencji uczestniczyli współcześni najwybitniejsi kryptolodzy świata m.in. Eli Bihama, Andrew J. Clarka, P. Landrocka, N. Courtoisa. Konferencja zakończyła się złożeniem wieńców na grobie Mariana Rejewskiego.

4 OD ENIGMY DO WSPÓŁCZESNEJ KRYPTOLOGII

W czasie II Wojny Światowej, słynny szpieg radziecki pochodzenia niemieckiego Richard Sorge, wnuk sekretarza Karola Marksa, jako attache prasowy ambasady niemieckiej w Tokio od 1933 do 1941 roku kierował siatką agentów o nazwie Czerwona Orkiestra. To on przekazywał zdobyte bezcenne informacje radzieckiemu wywiadowi wojskowemu, między innymi o pakcie berlińskim, ataku na Pearl Harbor i o tym, że Japonia nie zaatakuje Związku Radzieckiego, podał również dokładną datę rozpoczęcia planu Barbarossa. Moskwa podziękowała za te informację, ale nie podjęła żadnych działań. Co ciekawe, Sorge w swoich przekazach wykorzystywał stary szyfr podstawieniowy, gdzie właściwe szyfrowanie oparte było na ciągach liczb losowych, którymi były dane z niemieckich roczników statystycznych. Szyfr ten nie został złamany przez żadne służby specjalne.

Jednym z ważniejszych osiągnięć kryptologicznych, które zmieniło bieg wydarzeń II Wojny Światowej na Pacyfiku, było rozszyfrowanie japońskiego szyfru maszynowego Purple, czyli Purpurowego, przez wojskowego kryptologa Williama Friedmana. Amerykański wywiad mógł gromadzić informacje na temat ruchu japońskich okrętów i samolotów. Amerykanie dzięki temu wygrali bitwę o Midway. Także, dzięki tym informacjom, udało się zestrzelić samolot admirała Yamamoto, znakomitego dowódcy japońskiego, który jako jeden z niewielu wśród najwyższych rangą dowódców cesarskiej floty, posiadał ogromną wiedzę na temat planowania strategicznego. Mówiono o nim, że był „mózgiem" armii japońskiej i postrachem armii amerykańskiej. Podobno prezydent USA Franklin D. Roosvelt wiedział o wcześniejszym ataku na Pearl Harbor ale nie poinformował o tym społeczeństwa, gdyż chciał, aby Senat USA wyraził zgodę na przystąpienie Stanów Zjednoczonych do wojny.

„Nasi łamacze kodów kryptografowie i kryptoanalitycy, uczynili dla wcześniejszego i zwycięskiego zakończenia wojny tyle samo co wszystkie inne oddziały wojsk" – tak powiedział Franklin D. Roosvelt z ogromną dumą po zakończeniu wojny na posiedzeniu Senatu USA.

W latach 1948-1955 w ramach projektu Venona, przeprowadzonego przez Amerykanów, udało się im rozszyfrować część depesz radzieckich. Rosjanie zrobili błąd używając czasami jako klucza do różnych depesz tego samego ciągu losowego.

20 czerwca 1953 roku w nowojorskim więzieniu Sing-Sing miała miejsce egzekucja małżeństwa Ethel i Juliusa Rosenbergów. Dwa lata wcześniej skazano ich za zdradę tajemnic związanych z budową bomby atomowej. Szpiegowali na rzecz ZSRR, zdemaskowano ich dzięki „wypadkowi przy pracy". Rosjanie wykorzystywali kilkakrotnie ten sam klucz. Również oficer odpowiedzialny za całą akcję przypłacił tę pomyłkę życiem. Służby specjalne byłego ZSRR posługiwały się przypadkowo skonstruowanymi kluczami, a mówiąc dokładniej – ciągami tzw. liczb losowych.

Kiedy w czerwcu 1957 roku w jednym z nowojorskich hoteli został ujęty radziecki szpieg Rudolf Abel, agenci FBI znaleźli blok, którego strony wielkości znaczków pocztowych były pokryte długimi ciągami liczb. Były to klucze numeryczne.

W latach siedemdziesiątych również innym szpiegom sowieckim nie udało się zniszczyć posiadanych kluczy przed ich schwytaniem. Amerykanie szybko odkryli, że nie są to w żadnym wypadku prawdziwie liczby losowe. Można sądzić, że właściwości rosyjskich kluczy z liczb przypadkowych wpłynęły na historię świata w sierpniu 1991 roku. Wówczas to podczas puczu przeciwko Michaiłowi Gorbaczowowi dwaj spiskowcy – szef KGB Władimir Kriuczkow i minister obrony narodowej Dymitrij Jazow wymieniali zaszyfrowane informacje. Dzięki regularnościom w kluczu, Amerykanie zdołali odczytać te wiadomości. Prezydent George Bush przekazał je następnie Borysowi Jelcynowi.

Można powiedzieć, że I Wojna Światowa była wojną chemików – ponieważ wówczas po raz pierwszy zastosowano chlor i gaz musztardowy jako gazy bojowe. Natomiast II Wojna Światowa była wojną fizyków, którzy skonstruowali bombę atomową. Zapewne III Wojna Światowa będzie wojną matematyków, bo to właśnie oni będą kontrolować następną ważną broń – informację. To matematycy stworzyli szyfry stosowane obecnie do zabezpieczania informacji wojskowych i oczywiście również oni przewodzą w próbach złamania tych szyfrów.

LITERATURA

1. Bertrand G., *Enigma ou la plus grande énigme de la guerre 1939–1945* (*Enigma: the Greatest Enigma of the War of 1939-1945*), Paris 1973
2. Gannon J., *Stealing Secrets, Telling Lies: How Spies and Codebreakers Helped Shape the Twentieth Century*, Washington D.C. 2001
3. Kahn D., *Łamacze kodów*, WNT, Warszawa 2004
4. Kippenhahn R. *Tajemne przekazy, szyfry, Enigma i karty chipowe*, Prószyński i Spółka, Warszawa 2000
5. Kozaczuk W., *Enigma: How the German Machine Cipher Was Broken, and How It Was Read by the Allies in World War II*, edited and translated by Christopher Kasparek, Frederick MD, 1984
6. Levy S., *Rewolucja w kryptografii*, WNT, Warszawa 2002
7. Nowik G., *Zanim Złamano Enigmę. Polski Radiowy wywiad podczas wojny z bolszewicką Rosją 1918-1920*, Rytm 2005
8. Singh S., *Księga szyfrów. Od starożytnego Egiptu do kryptografii kwantowej*, Albatros, Warszawa 2001

W projekcie **Informatyka +**, poza wykładami i warsztatami, przewidziano następujące działania:

- 24-godzinne kursy dla uczniów w ramach modułów tematycznych
- 24-godzinne kursy metodyczne dla nauczycieli, przygotowujące do pracy z uczniem zdolnym
- nagrania 60 wykładów informatycznych, prowadzonych przez wybitnych specjalistów i nauczycieli akademickich
- konkursy dla uczniów, trzy w ciągu roku
- udział uczniów w pracach kół naukowych
- udział uczniów w konferencjach naukowych
- obozy wypoczynkowo-naukowe.

Szczegółowe informacje znajdują się na stronie projektu

www.informatykaplus.edu.pl