Muzeum II Wojny Światowej

Egzemplarz Enigmy ze zbiorów Muzeum II Wojny Światowej w Gdańsku otrzymany w darze od Muzeum Wojskowego w Oslo. Fot. Dominik Jagodziński

SEKRETY ENIGMY

warsztaty edukacyjne

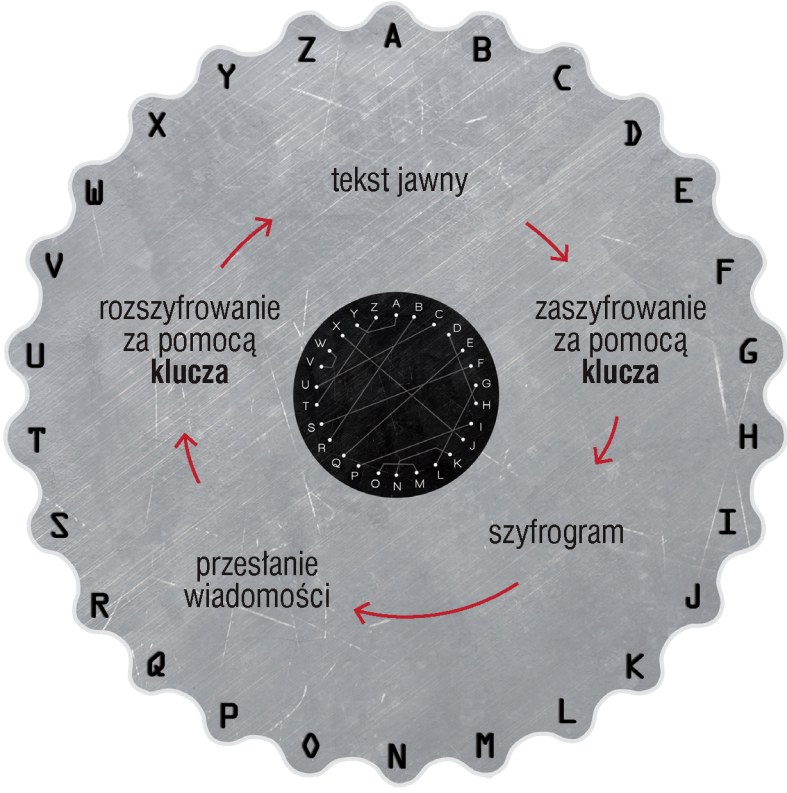
Mateusz Jasik, Monika Liedke

#M2WSwirtualnie

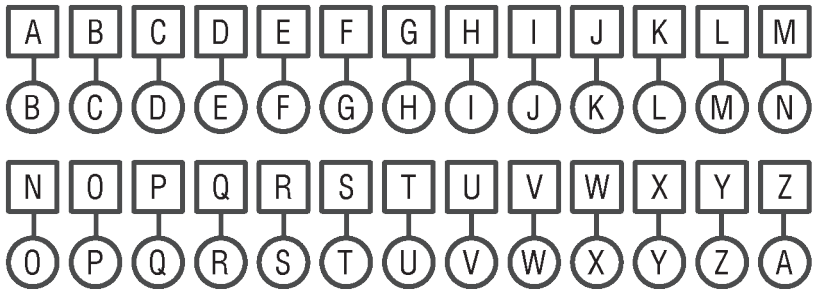
Trudno dokładnie wskazać, kiedy powstał pierwszy szyfr, czyli funkcja matematyczna polegająca na przekształceniu tekstu jawnego [zrozumiałego dla wszystkich w szyfrogram, a więc wiadomość, która jest czytelna tylko dla posiadającego odpowiedni klucz [algorytm szyfrowania, rozszyfrowania]. Być może pierwszym szyfrem był hebrajski AtBasz datowany na około 500 r. p.n.e. Więcej sławy zyskał nieco bardziej skomplikowany, późniejszy o pięć wieków szyfr przypisywany Gajuszowi Juliuszowi Cezarowi. Zanim go jednak poznamy, przyjrzyjmy się najważniejszym zasadom szyfrowania.

Mamy zatem pewną wiadomość, którą chcemy przekazać np. naszym stronnikom czy dowodzonym przez nas oddziałom, ale w taki sposób, by dostawszy się w niepowołane ręce nie była ona możliwa do odczytania, bez znajomości klucza. Im bardziej skomplikowany szyfr wykonywany przez człowieka, tym większe bezpieczeństwo informacji, ale też większa czasochłonność procesu, jak i prawdopodobieństwo zaistnienia błędów.

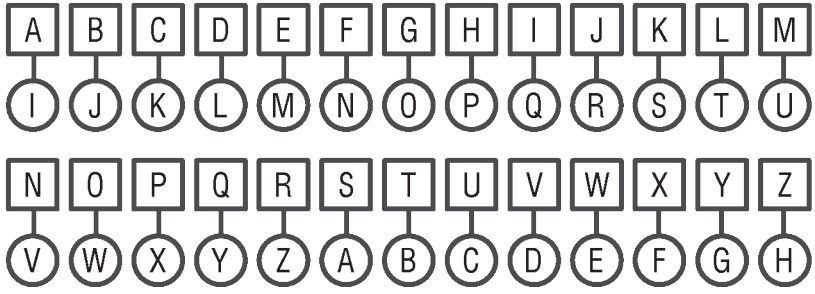
Możemy powiedzieć, że wspomniany proces zachodzi według poniższego schematu:



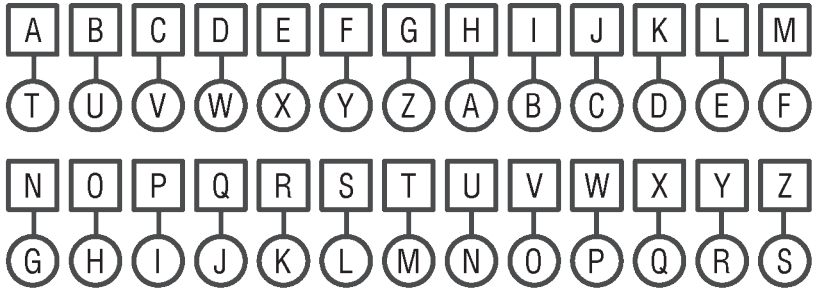
SZYFR CEZARA – ĆWICZENIE



KOSCI ZOSTALY RZUCONE ⟷ LPTDJ APTUBMZ SAVDPOF



ZDRADE KOCHAM ⟷ _____ _____



_____ _____ ⟷ SWKTCVHP GBXGTPBWSX

SZYFR POLIBIUSZA – ĆWICZENIE

Klucz: **brak klucza**

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

KRYPTOGRAFIA ⟷
25 42 54 35 44 34 22 42 11 21 24 11

Klucz: **KLUCZ**

	1	2	3	4	5
1	K	L	U	C	Z
2	A	B	D	E	F
3	G	H	I/J	M	N
4	O	P	Q	R	S
5	T	V	W	X	Y

KRYPTOGRAFIA ⟷
11 44 55 42 51 41 31 44 21 25 33 21

SZYFR POLIBIUSZA – ĆWICZENIE

Klucz: **MASZYNA***

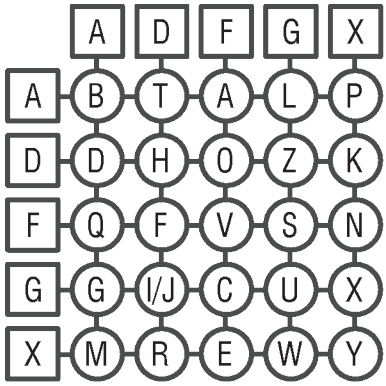
	1	2	3	4	5
1					
2					
3					
4					
5					

KRYPTOGRAF ⟷
— — — — — — — — — —

— — — — — — — — — —
13 14 15 31 45 12 21 51 ⟷

*** Klucz posiada dwie litery A, jednak do tworzenia tabeli należy użyć tylko pierwszej z nich, drugą pominąć**

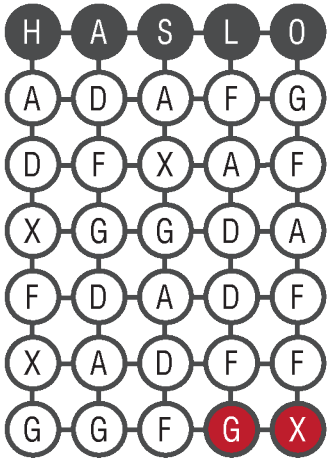
SZYFR ADFGVX – ĆWICZENIE

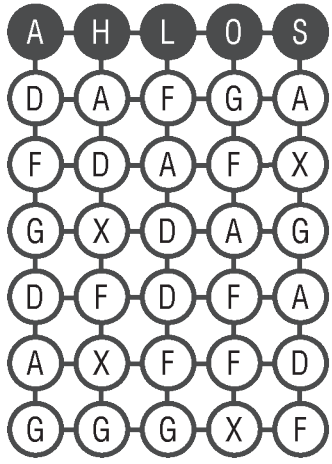


Text jawny:
TAJNA WIADOMOŚĆ

Klucz:
HASŁO

T	A	J	N	A	W	I	A	D	O	M	O	S	C
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
AD	AF	GD	FX	AF	XG	GD	AF	DA	DF	XA	DF	FG	GF



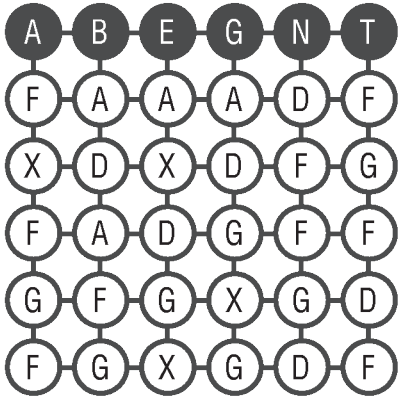


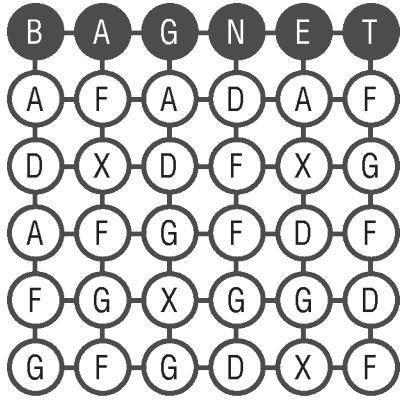
Tekst zaszyfrowany: **DFGDAG ADXFXG FADDFG GFAFFX AXGADF**

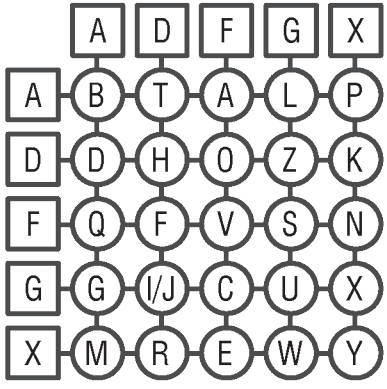
SZYFR ADFGVX – ĆWICZENIE

Text zaszyfrowany:
FXFGF ADAFG AXDGX ADGXG DFFGD FGFDF

Klucz:
BAGNET







AF	AD	AF	DX	DF	XG	AF	GF	DF	FG	XG	GD	GF	GD	XF
A	T	A	K	O	W	A	C	O	S	W	I	C	I	E

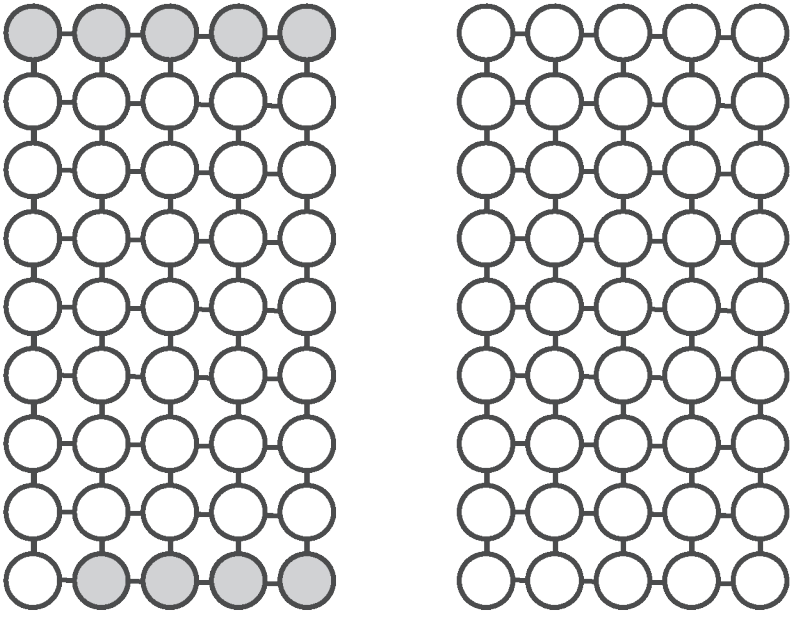
Tekst jawny: **ATAKOWAĆ O ŚWICIE**

SZYFR ADFGVX – ĆWICZENIE

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

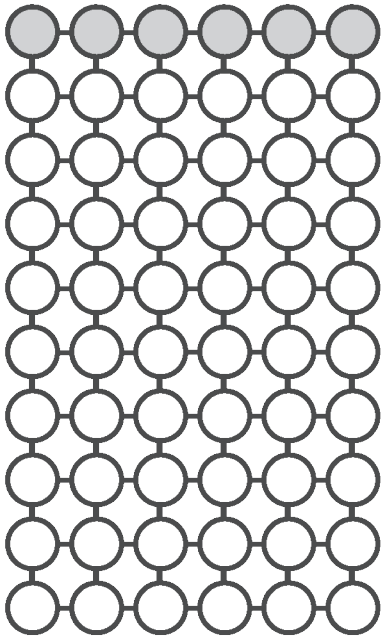
Text jawny:
NA ZACHODZIE BEZ ZMIAN

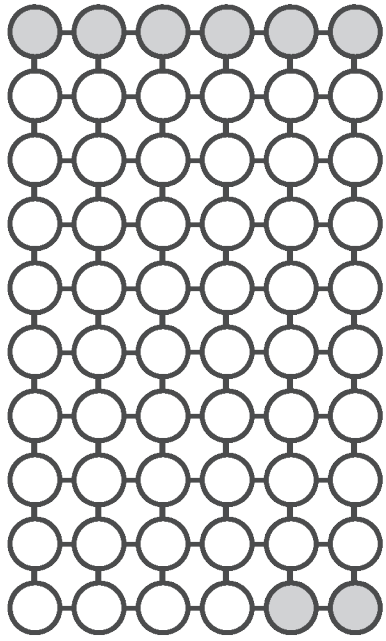
Klucz:
WOJNA



Tekst zaszyfrowany: _____ _____ _____ _____ _____

Text zaszyfrowany:
DXGADDGXX AAFXAAAAG GFGDFDXFX FXFAAFXDX ADXDGDAXX AFDDFADFD





Klucz:
CZOLGI

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

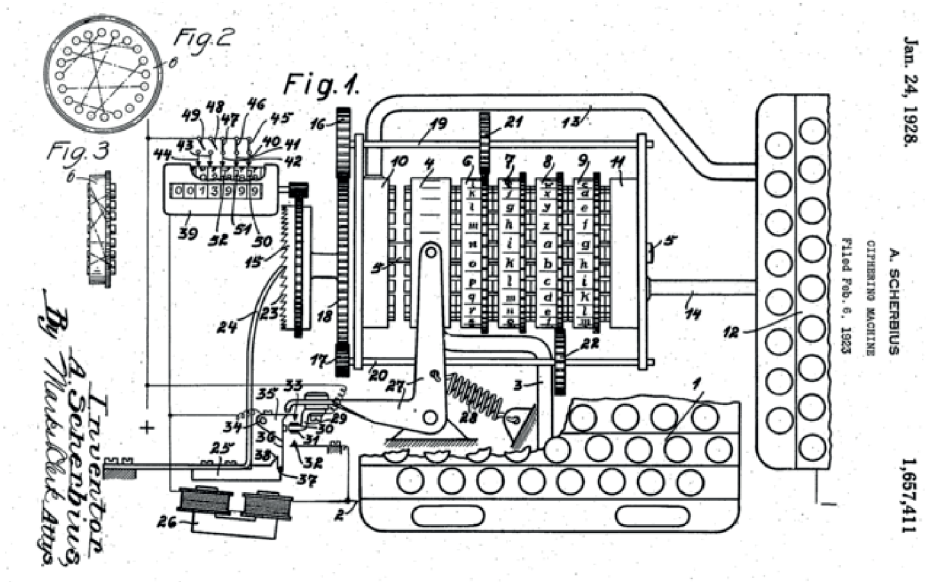
Tekst jawny: : _____ ____ _____ __ _____

SZYFR OTTENDORFA – ĆWICZENIE

↔ 2 – 1 – 4 – 3
↔ 11 – 3 – 1 – 11
↔ 12 – 4 – 2 – 2
↔ 10 – 16 – 3 – 4
↔ 13 – 7 – 1 – 1
↔ 11 – 21 – 2 – 6

♠ – numer strony
♣ – numer linijki na stronie
♥ – numer wyrazu w linijce
♦ – numer litery w wyrazie

Szczególnego znaczenia bezpieczeństwo przesyłanych informacji zyskało w trakcie I wojny światowej. Stało się tak za sprawą rozwoju łączności radiowej, a więc możliwości przesyłania wiadomości bez udziału kurierów czy przewodów, jednak z dużym prawdopodobieństwem podsłuchania przez przeciwnika. Jak się wkrótce okazało, obawy o bezpieczeństwo komunikacji były całkowicie uzasadnione. Sukcesy na polu łamania rosyjskich radiodepeszy odnotowali Austriacy i Niemcy, a co szczególnie ważne, miało to istotny wpływ na przebieg działań na froncie wschodnim. Z drugiej strony niektórzy historycy łączą fakt złamania niemieckiego szyfru ADFGVX zawartego w ćw. nr XX ze zwycięstwem aliantów na froncie zachodnim. Z pewnością łamanie przez polskich kryptologów rosyjskich depeszy miało kluczowe znaczenie w trakcie wojny polsko – bolszewickiej 1920 roku, kiedy to informacje uzyskiwane przez radiowywiad walnie przyczyniły się do polskiego zwycięstwa w bitwie warszawskiej. Doświadczenia I wojny światowej pokazały, że proces szyfrowania przeprowadzany przez człowieka jest nie dość doskonały, dlatego jeszcze w trakcie jej trwania w wielu krajach starano się zastąpić czynności szyfranta przez maszynę. Tak narodziła się najsłynniejsza maszyna szyfrująca w dziejach - niemiecka Enigma.



Jeden z rysunków patentowych handlowej wersji Enigmy

Od lewej: Henryk Zygalski, Jerzy Różycki i Marian Rejewski.
Źródło: Polska Agencja Prasowa

Wprowadzenie szyfru maszynowego w 1926 roku w korespondencji radiowej Kriegsmarine [niemieckiej marynarki wojennej], a od 1928 roku także niemieckich wojsk lądowych otworzyło nowy rozdział walki wywiadów o informacje. Co ciekawe Enigma była maszyną początkowo przeznaczoną do przekazywania informacji handlowych, zaś różne jej wersje stosowały także służby dyplomatyczne, a nawet przemysł. Dotychczasowe metody lingwistyczne stosowane przez Brytyjczyków i Francuzów stały się bezużyteczne wobec liczby kombinacji generowanej przez Enigmę. Inaczej, powiedzielibyśmy: innowacyjnie, do ataku na niemiecki szyfr podeszło polskie Biuro Szyfrów. Postanowiono o zatrudnieniu zawodowych matematyków. W tym celu utworzono kurs kryptologiczny w Poznaniu dla wybijających się studentów matematyki tamtejszego uniwersytetu.

Przyszłość udowodniła słuszność polskiego podejścia. Trzej uczestnicy kursu – **Marian Rejewski**, **Jerzy Różycki**, **Henryk Zygalski** – doprowadzili do złamania pierwszej radiodepeszy zaszyfrowanej za pomocą Enigmy już w 1932 roku. Ogromny sukces Polaków był efektem zastosowania oryginalnych teorii matematycznych, współpracy z francuskim wywiadem, a także... błędów i złych nawyków niemieckich szyfrantów. Był to jednak tak na prawdę początek, a nie koniec wyścigu polegającego na kolejnych udoskonaleniach niemieckiej konstrukcji i procedur, a z drugiej strony coraz wydajniejszych metod stosowanych przez kryptologów.

W przeddzień II wojny światowej polskie Biuro Szyfrów, będące częścią struktury Oddziału II Sztabu Głównego Wojska Polskiego [m.in. wywiad, kontrwywiad] dysponowało bezcenną wiedzą i umiejętnościami, ale ograniczonymi możliwościami finansowymi i organizacyjnymi, nie pozwalającymi na wypadek konfliktu zbrojnego na łamanie tysięcy depesz dziennie. Wobec narastającego niemieckiego zagrożenia postanowiono przekazać komplet wiedzy zarówno Francuzom jak i Brytyjczykom. Przekazanie kopii Enigmy i pełnej dokumentacji nastąpiło 25 lipca 1939r. w Pyrach pod Warszawą. Polska umiejętność łamania niemieckich szyfrów była dla zachodnich aliantów niemałym zaskoczeniem, dotychczas sceptycznie podchodzących do podatności Enigmy na kryptologiczne ataki.

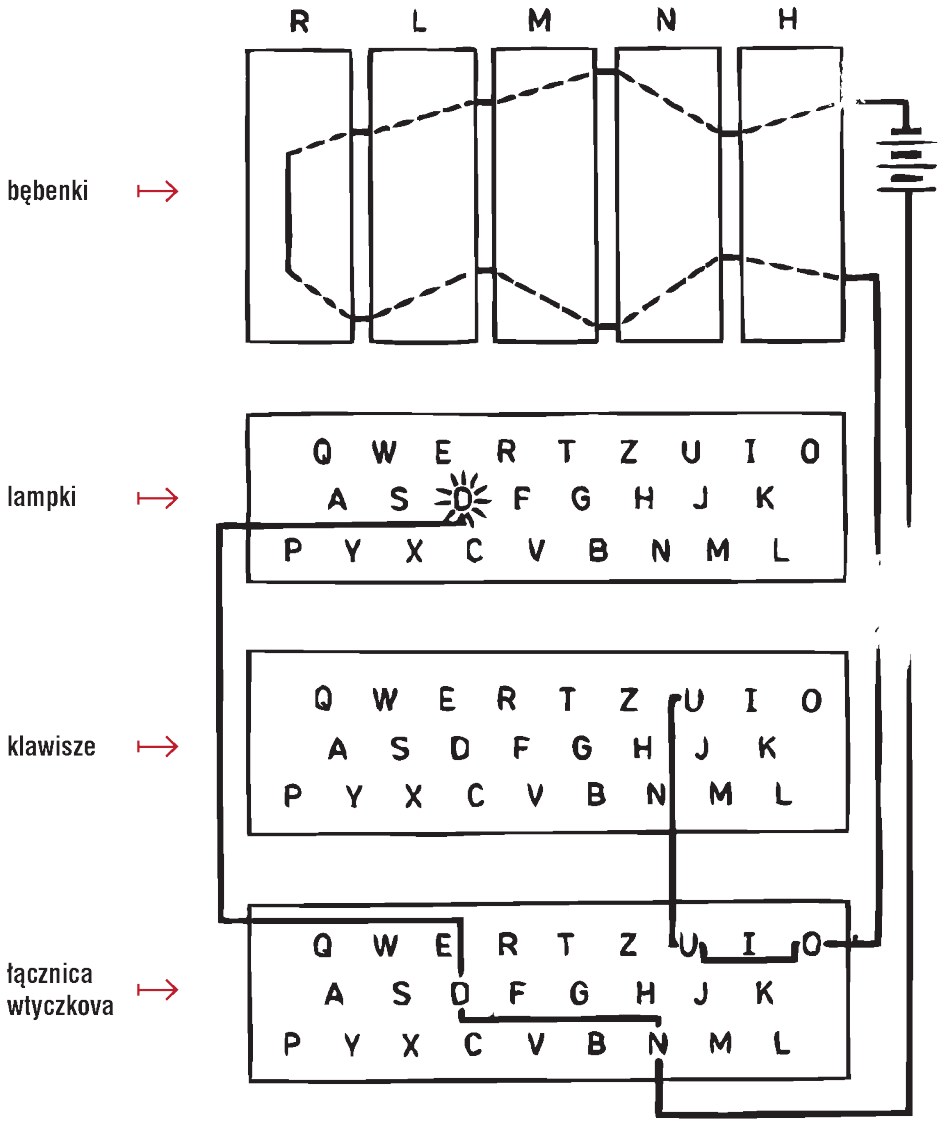
Alan Turning. Źródło: wikipedia.org

Po wybuchu wojny ewakuowano polskich kryptologów do Francji, gdzie zmierzali się z kolejnymi wyzwaniami wynikającymi z modyfikacji i udoskonaleń stosowanych przez Niemców. Brytyjczycy zaś kontynuowali dzieło w ośrodku w Bletchley Park. Zespół pod kierunkiem **Alana Turinga** stworzył bombę kryptologiczną. Bomba była urządzeniem, dzięki któremu możliwe stało się niemal „przemysłowe" odczytywanie niemieckich radiodepesz. Za sprawą od powiednich funduszy, a także osobistej interwencji Winstona Churchilla, ośrodek w Bletchley Park dysponował potencjałem organizacyjnym pozwalającym na dostarczanie własnym siłom zbrojnym strumienia bezcennych informacji o militarnych zamierzeniach III Rzeszy. Co istotne, dzięki szczególnym środkom ostrożności, np.celowemu niewykorzystywaniu całości posiadanej wiedzy, Brytyjczykom udało się utrzymać Niemców w zgubnym dla nich przekonaniu, że szyfr generowany przez Enigmę jest nie do pokonania.

Nie jest możliwe dokładne oszacowanie jaki konkretnie wpływ miała umiejętność łamania niemieckich szyfrów na losy II wojny światowej w całościowym ujęciu. Wszystkie kalkulacje będą podlegały różnego rodzaju zmiennym i niewiadomym. Z dużą dozą pewności można jednak wskazać, że w najtrudniejszym dla Wielkiej Brytanii okresie Bitwy o Atlantyk łamanie szyfrów Kriegsmarine pozwoliło na utrzymanie funkcjonowania konwojów płynących z USA i Kanady. Warto podkreślić, że mimo wielu zagrożeń udało się zachować w tajemnicy fakt łamania niemieckich szyfrów – był to warunek konieczny do operacyjnego wykorzystania wiedzy pochodzącej z dekryptażu. Nie umniejszając pomocy francuskiej i późniejszego usprawnienia czy właściwie umasowienia procesu deszyfracji zawdzięczanego Brytyjczykom, złamanie szyfru Enigmy pozostaje jednym z najważniejszych polskich wkładów w zwycięstwo aliantów nad III Rzeszą, zaś upowszechnianie wiedzy o tym fakcie jest istotnym elementem misji Muzeum.

Fragment wystawy głównej Muzeum II Wojny Światowej w Gdańsku poświęcony złamaniu szyfru Enigmy. Wizualizacja Tempora S.A.

SCHEMAT PRZEBIEGU PRĄDU W ENIGMIE WOJSKOWEJ



Szyfr Cezara

ZDRADE KOCHAM ⟷ HLZILM SWKPIU

ZDRAJCOW NIENAWIDZE ⟷ SWKTCVHP GBXGTPBWSX

Szyfr Polibiusza

	1	2	3	4	5
1	M	A	S	Z	Y
2	N	B	C	D	E
3	F	G	H	I/J	K
4	L	O	P	Q	R
5	T	U	V	W	X

KRYPTOGRAF ⟷
35 45 15 43 51 42 32 45 12 31

SZYFRANT ⟷
13 14 15 31 45 12 21 51

Szyfr ADFGVX

NA ZACHODZIE BEZ ZMIAN ⟷ DFDDXAFX AFDGAGAX FGFGAXFG XADDFDDG FGDAXFGX

DXGADDGXX AAFXAAAAG GFGDFDXFX FXFAAFXDX ADXDGDAXX AFDDFADFD ⟷
DALEKA JEST DROGA DO TIPPERARY

Szyfr Ottendorfa

E ⟷ 2 – 1 – 4 – 3
N ⟷ 11 – 3 – 1 – 11
I ⟷ 12 – 4 – 2 – 2
G ⟷ 10 – 16 – 3 – 4
M ⟷ 13 – 7 – 1 – 1
A ⟷ 11 – 21 – 2 – 6