Piotr Dormus

Mateusz Wanatowicz

Klasa VIA
SP 4 Kraków

Szyfry na przestrzeni wieków

Luty 2005

Spis treści

Wstęp

Szyfr (kryptogram) to procedura takiego przekształcania wiadomości, żeby była ona niemożliwa (lub bardzo trudna) do odczytania przez każdego, kto nie posiada odpowiedniego klucza. Wiadomość przed zaszyfrowaniem nazywa się tekstem jawnym, a wiadomość zaszyfrowaną – tekstem tajnym lub szyfrogramem. Szyfrowanie jest zajęciem bardzo starym.

Ta definicja może niektórym pomóc w zrozumieniu tego czym jest naprawdę szyfr. Wg nas, autorów, szyfry to bardzo ciekawy materiał na pracę matematyczno – naukową. Temat ten z pewnością zainteresuje wiele osób, np. przeciętnego ucznia, chcącego zaszyfrować ściągę na sprawdzian (czego bynajmniej nie popieramy – do testów trzeba się przecież uczyć).

W naszej pracy można znaleźć informacje o szyfrach używanych zarówno w starożytności, jak i podczas II wojny światowej. Jest tu mowa o wielu metodach szyfrowania. Zamieszczamy również wiele tabelek, pomagających zrozumieć istotę danego szyfru.

Nasza praca nie zawiera opisów technologii komputerowych, których zadaniem jest szyfrowanie wiadomości, gdyż uważamy, iż są one zbyt zaawansowane, by mogły być zrozumiane przez przeciętnego człowieka.

Mamy nadzieję, iż lektura naszej pracy zachęci niektórych, do skierowania swych zainteresowań w stronę kryptografii.

Autorzy.

Szyfry przesuwające

Szyfry przesuwające (z angielskiego: *shifts ciphers)* to grupa kryptogramów charakteryzująca się tym, że każdemu znakowi tekstu jawnego odpowiada dokładnie jeden znak tekstu tajnego, przesunięty o określoną liczbę miejsc w alfabecie.Litery z końca alfabetu stają się literami z jego początku. Najbardziej popularnym szyfrem przesuwającym jest *Szyfr Cezara*. W szyfrach przesuwających zazwyczaj przestrzegane są pewne założenia, np.:

- używamy alfabetu z 26 znakami, numerowanymi od 0 do 25

- x to znak tekstu jawnego

- y to znak tekstu tajnego (szyfrogramu)

- k to klucz (liczba o jaką przesuwamy)

Wzór na szyfrowanie to:

$Y = (x + k) \bmod 26$

Mod – obliczanie reszty z dzielenia

Wzór na deszyfrowanie:

$X = (y – k) \bmod 26$

Szyfry przesuwające były używane zarówno w starożytnym Rzymie, jak i w XIX-wiecznej Rosji, natomiast teraz, w dobie komputerów, nie gwarantują żadnego bezpieczeństwa. Aby złamać szyfr przesuwający należy przeszukać przestrzeń klucza, czyli sprawdzić wszystkie jego wartości, aż do otrzymania sensownego tekstu jawnego.

Szyfry monoalfabetyczne

Szyfry monoalfabetyczne to najprostsze szyfry przesuwający. Ich nazwa pochodzi od słowa „mono”, co oznacza „jeden”. Istota tych szyfrów polega na przypisaniu jednej literze alfabetu jawnego dokładnie jednej litery alfabetu tajnego, zgodnie z obowiązującym kluczem. Klucz to liczba o jaką przesuwamy literę jawną, zamieniając ją na tajną. Przyjmijmy, że klucz wynosi 2, a my chcemy zaszyfrować wiadomość:

Proszę o pomoc.

Nie używamy litery „ę”, więc wiadomość brzmi:

Prosze o pomoc.

W tym przypadku za każdą literę podstawiamy inną oddaloną od niej o 2 miejsca w prawo w alfabecie łacińskim. W efekcie otrzymujemy tekst tajny:

Survch r srprf.

Algorytm stosowany przy szyfrach monoalfabetycznych wygląda tak:

y = (x+k)

y oznacza znak tekstu tajnego
x oznacza znak tekstu jawnego
k oznacza klucz

Algorytm, którego użyliśmy do zaszyfrowania słów „PROSZĘ O POMOC” to:

y = (x+2)

Obecnie szyfr ten nie jest w ogóle stosowany, gdyż wiadomość zaszyfrowaną nim może, przy odrobinie sprytu, odczytać każdy. Wystarczy wiedzieć, że tekst jawny napisany po polsku (bez użycia polskich znaków diakrytycznych) można zaszyfrować na dwadzieścia pięć różnych sposobów, gdyż za dwudziestym piątym razem ponownie otrzymamy tekst jawny, używając kluczy od 1 do 25. By rozszyfrować tekst należy przeprowadzić próby z kolejnymi kluczami poczynając od klucza 1, aż nie uzyskamy sensownego tekstu. Maksymalna ilość prób wynosi dwadzieścia pięć, dlatego też szyfr monoalfabetyczny absolutnie nie gwarantuje żadnego bezpieczeństwa.

Szyfr Cezara

Jedną z pierwszych ważnych postaci historycznych, która szyfrowała swoje listy był Juliusz Cezar, rzymski wódz i polityk. Stosował on w listach do swego przyjaciela Cycerona szyfr monoalfabetyczny z kluczem równym 3. Taki sposób szyfrowania nazywamy od jego imienia szyfrem Cezara.

W owych czasach dawał on praktycznie stuprocentową gwarancję, iż nikt niepożądany nie odczyta zaszyfrowanej wiadomości. Teraz szyfr Cezara nie jest używany, gdyż jak wiadomo jest on powszechnie znany. Jeśli ktoś wie, że ma z nim do czynienia, może posłużyć się taką oto tabelką:

A	B	C	D	E	F	G	H	I	J	K	L	M
d	e	f	g	h	i	j	k	l	m	n	o	p

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
q	r	s	t	u	v	w	x	y	z	a	b	c

W żółtych miejscach wpisane są litery alfabetu jawnego, pod nimi zaś odpowiadające im litery alfabetu tajnego. Oczywiście znajdują się tu znaki powszechnie używanego alfabetu łacińskiego, jeśli jednak używamy jakiegokolwiek innego alfabetu, to układamy tabelkę na takiej samej zasadzie.

Można również użyć dwóch tarcz (jedna jest w środku drugiej), które obraca się wzajemnie wobec siebie. W zewnętrzną tarczę wpisane są litery alfabetu jawnego, z kolei w wewnętrznej litery alfabetu tajnego. Przekręcanie tarcz pozwala na uzyskanie wszystkich możliwych kombinacji szyfrów wg metody Cezara. Dzięki nim osiąga się dokładnie taki sam efekt, jak przy użyciu wyżej narysowanej tabelki.

Tarcza taka widniała kiedyś w herbie Narodowej Agencji Bezpieczeństwa USA (z angielskiego: National Security Agency – NSA).

Szyfr Cezara z użyciem cyfr

Inną metodą na zaszyfrowanie wiadomości jest szyfr Cezara z wykorzystaniem cyfr. Za jego pomocą można szyfrować informację na różne sposoby, np. każdej literze alfabetu można przyporządkować liczbę, którą zapiszemy przy pomocy dwóch cyfr. Ilość różnych liczb musi zgadzać się z ilością liter występującą w stosowanym alfabecie. Dla alfabetu łacińskiego użyjemy liczb od 01(którą zapiszemy jako „01”) do 26 (zapisujemy po prostu „26”).
W zrozumieniu tego z pewnością pomoże tabelka:

Znak alfabetu jawnego	**Znak alfabetu tajnego**
A	01
B	02
C	03
D	04
E	05
F	06
G	07
H	08
I	09
J	10
K	11
L	12
M	13
N	14
O	15
P	16
Q	17
R	18
S	19
T	20
U	21
V	22
W	23
X	24
Y	25
Z	26

Przypuśćmy, iż chcemy przesłać tajną wiadomość:

Nie ufaj nikomu

W tym celu każdej literze przyporządkowujemy cyfrę, tak jak jest to ukazane w tabelce. Zaszyfrowana wiadomość to:

140905 21060110 140911151321

Cezar z użyciem cyfr to kolejny szyfr używany w przeszłości, którego złamanie dla deszyfrantów to kwestia kilku minut. Niemniej jednak dawniej stanowił nie lada przeszkodę do pokonania.

Tablica Thritemiusa

Tablica Trithemiusa (nazwa pochodzi od godności francuskiego opata) jest jedną z najprostszych tablic szyfrowych. Ma ona 26 kolumn po 26 liter w rzędzie. Pierwszy rząd odpowiada normalnemu alfabetowi. Następny rząd jest przesunięty o jedną literą w lewo, czyli zaczyna się od B a kończy na A, trzeci rozpoczyna się od C a jest zakończony na B itd. Gdy nie po lewej stronie brakuje miejsca, przesuwamy ostatnią literą na początek rzędu. Przy użyciu tej tabeli szyfrujemy w następujący sposób: pierwszą literę szyfrujemy według pierwszego rzędu, czyli pozostaje bez zmian. Drugą literę szyfrujemy według drugiego rzędu, czyli jest ona przesunięta o jedną literę w lewo itd. Jeśli np. chcemy zaszyfrować wiadomość:

Prosimy o pomoc

to będzie to wyglądało w ten sposób: litera P pozostanie bez zmian. Litera R zostanie przesunięta o jedno miejsce w lewo, czyli stanie się S. Dalej, z O otrzymamy Q, z S – V, I – M, M – R, a Y – E. Słowo prosimy zmieni się w PSQVMRE. Cała wiadomość będzie brzmiała PSQVMRE V XXWZO. Jeśli tekst ma więcej niż 26 liter to zaczynamy od początku, to znaczy że dwudziestą siódmą literę zaszyfrujemy znów według pierwszej linijki.

ABCDEFGHIJKLMNOPQRSTUVWXYZ

ABCDEFGHIJKLMNOPQRSTUVWXYZ
BCDEFGHIJKLMNOPQRSTUVWXYZA
CDEFGHIJKLMNOPQRSTUVWXYZAB
DEFGHIJKLMNOPQRSTUVWXYZABC
EFGHIJKLMNOPQRSTUVWXYZABCD
FGHIJKLMNOPQRSTUVWXYZABCDE
GHIJKLMNOPQRSTUVWXYZABCDEF
HIJKLMNOPQRSTUVWXYZABCDEFG
IJKLMNOPQRSTUVWXYZABCDEFGH
JKLMNOPQRSTUVWXYZABCDEFGHI
KLMNOPQRSTUVWXYZABCDEFGHIJ
LMNOPQRSTUVWXYZABCDEFGHIJK
MNOPQRSTUVWXYZABCDEFGHIJKL
NOPQRSTUVWXYZABCDEFGHIJKLM
OPQRSTUVWXYZABCDEFGHIJKLMN
PQRSTUVWXYZABCDEFGHIJKLMNO
QRSTUVWXYZABCDEFGHIJKLMNOP
RSTUVWXYZABCDEFGHIJKLMNOPQ
STUVWXYZABCDEFGHIJKLMNOPQR
TUVWXYZABCDEFGHIJKLMNOPQRS
UVWXYZABCDEFGHIJKLMNOPQRST
VWXYZABCDEFGHIJKLMNOPQRSTU
WXYZABCDEFGHIJKLMNOPQRSTUV
XYZABCDEFGHIJKLMNOPQRSTUVW
YZABCDEFGHIJKLMNOPQRSTUVWX
ZABCDEFGHIJKLMNOPQRSTUVWXY

Tablica Blaisa de Vignère'a

Jest to szyfr opierający się na tablicy Trithemiusa. Jest on o wiele trudniejszy do dekryptacji (rozszyfrowania), gdyż używamy do niego klucza np. 7,1,2,6,10,25. Cyfry oznaczają rzędy, przy których użyciu będziemy szyfrować. Możemy też, jako klucz obrać słowo np.

kogut

Wtedy pierwszą literę zaszyfrujemy przy użyciu rzędu, który zaczyna się od litery K, następną korzystając z rzędu rozpoczynającego się od O itp. Tak samo jak w szyfrze Trithemiusa, jeśli wiadomość jest dłuższa niż sześć liter, zaczynamy od początku według ustalonego klucza. Aby ułatwić sobie szyfrowanie piszemy u góry raz za razem słowo-klucz, a poniżej wiadomość.

k o g u t k o g u t k o g
p r o s i m y o p o m o c

Tablica de Vignère'a

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

Szyfr kombinowany

Szyfr kombinowany należy do grupy szyfrów przesuwających. Szyfrowanie nim wymaga znajomości kilku zasad:

- zawsze posługujemy się alfabetem łacińskim i nie używamy znaków występujących w innych językach
- usuwamy wszystkie spacje i znaki interpunkcyjne
- posługujemy się wyłącznie małymi literami
- litera pierwsza, trzecia, piąta, siódma itd. tekstu, który chcemy zaszyfrować jest zastępowana literą występującą bezpośrednio po niej w alfabecie (literę *z* zastępujemy literą *a*)
- litera druga, czwarta, szósta, ósma itd. jest zastępowana przez literę występującą bezpośrednio przed nią w alfabecie (literę *a* zastępujemy literą *z*)

Przykładowo chcemy zaszyfrować wiadomość o treści:

Czerwony alarm!

Najpierw przekształcamy ją zgodnie z zasadami. Powinna ona wówczas wyglądać następująco:

czerwonyalarm

Później szyfrujemy ją wg zasad wymienionych powyżej. Zaszyfrowany tekst brzmi:

dyfqxnoxbkbqn

Szyfr ten również jest jednym z ciekawszych prostych szyfrów. Nie potrzeba dużych umiejętności, aby biegle go opanować.

Szyfr Parkan

Dosyć znanym szyfrem, w szczególności w kręgach młodzieży szkolnej, jest szyfr zwany *parkanem*. Sposób szyfrowania parkanem jest prosty. Przypuśćmy, że chcemy zaszyfrować tekst:

Uwaga wróg się zbliża.

Na początek z tekstu eliminujemy wszystkie spacje. Później należy zdecydować się, w ilu rzędach będziemy chcieli ją zapisać. Na początek mogą być to dwa rzędy. Szyfrując parkanem umieszczamy w górnym rzędzie literę pierwszą, trzecią, piątą itd. W dolnym rzędzie piszemy zaś literę drugą, czwartą, szóstą itd. W efekcie tych zabiegów otrzymujemy następującą zbitkę liter:

Uaargizlż
wgwósębia

Następnie litery te zapisujemy w jednym rzędzie jako dwa słowa:

Uaargizlż wgwósębia.

Osoba chcąca odszyfrować tekst musi odczytać najpierw pierwszą literę pierwszego słowa, potem pierwszą literę drugiego słowa, drugą literę pierwszego słowa, drugą literę drugiego słowa itd.

Oczywiście szyfrując parkanem możemy zdecydować się na dowolną ilość rzędów. Przykładowo wiadomość:

Uwaga wróg się zbliża

możemy zapisać w pięciu rzędach. Będzie ona wtedy wyglądać tak:

Uwii
wręż
aóza
ggb
asl

Po przepisaniu ją do jednego rzędu otrzymujemy tekst:

Uwii wręż aóza ggb asl.

Chcąc go odczytać czytamy najpierw pierwsze litery tych słów, następnie ich drugie liter itd.

Szyfrowanie parkanem jest bardzo proste, a osoba nie mająca z nim wcześniej do czynienia musi sporo pomyśleć, zanim odczyta zaszyfrowaną parkanem wiadomość.

Jedną z zalet parkanu jest to, iż można wykorzystać go w każdym alfabecie. Podsumowując, jest to jeden z ciekawszych prostych szyfrów.

Tablica Polibiusza

Tablica Polibiusza zwana również Szachownicą Polibiusza jest jedną z metod szyfrowania, nazwaną tak na cześć greckiego historyka o imieniu Polibiusz. Z założenia w szyfrze tym posługujemy się alfabetem łacińskim i nie rozróżniamy liter *i* oraz *j*. Szyfrowanie przy pomocy Tablicy Polibiusza polega na zastępowaniu każdej litery przez dwie cyfry: najpierw tą, która jest na początku wierszu, w którym znajduje się dana litera, a później tą, która jest na górze kolumny z daną literą. Osoba, do której wysyłamy zaszyfrowaną wiadomość również musi znać Tablicę Polibiusza, by móc odczytać wiadomość.

	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

Załóżmy, że musimy zaszyfrować wiadomość:

Spotkajmy się dzisiaj

Najpierw należy wyeliminować z niej wszystkie polskie znaki diakrytyczne (w tym przypadku ę) oraz wszystkie tzw. spacje (przerwy pomiędzy słowami). Wtedy wiadomość będzie wyglądała tak:

Spotkajmysiedzisiaj

Następnie zamieniamy litery na cyfry zgodnie z instrukcją. Ostateczny kształt wiadomości po zaszyfrowaniu to:

43 35 34 44 25 11 24 32 54 43 24 15 14 55 24 43 24 11 24

Tą metodą szyfrowania posługiwali się np. więźniowie w carskiej Rosji. Zmodyfikowali oni tablicę do wymiarów 6 x 6, tak by mogła pomieścić trzydzieści pięć liter cyrylicy. Metodę tą nazwali nihilistyczną na cześć nihilistów - przeciwników reżimu cesarskiego.

Tablicę Polibiusza można zmodyfikować tak, aby kolejność liter w niej nie była zgodna z alfabetem. W tym celu należy umieścić w tablicy ciąg liter, dzięki któremu kolejność innych liter zmieni się. Przypuśćmy, że na początku tablicy umieścimy słowo *trapez*. Tablica Polibiusza ze zmienionym układem liter, poprzez umieszczenie słowa *trapez* znajduje się poniżej:

	1	**2**	**3**	**4**	**5**
1	t	r	a	p	e
2	z	b	c	d	f
3	g	h	i/j	k	l
4	m	n	o	q	s
5	u	v	w	x	y

Szyfrowanie za pomocą zmodyfikowanej Tablicy Polibiusza wygląda tak samo jak szyfrowanie podstawową wersją. O zmienionym układzie liter musi wiedzieć osoba, do której wysyłamy zaszyfrowaną wiadomość. Zmiana taka ma na celu utrudnienie odczytania zaszyfrowanej wiadomość osobom postronnym, mającym wcześniej kontakt z Tablicą Polibiusza.

Szyfr Playfair'a

Szyfr Playfair'a, nazwany od nazwiska angielskiego lorda, który go opublikował, działa w następujący sposób:

Najpierw tworzymy tabelę-klucz. Postępowanie jest podobne jak w Cezarze: z hasła usuwa się powtarzające się litery. Następnie dodaje się pozostałe litery alfabetu. Litery *i* oraz *j* traktuje się jako ten sam znak. Mamy więc alfabet składający się z 25 liter i możemy go zapisać w kwadracie 5 na 5. Hasło *margerytka* daje słowo klucz *margeytk.* Weźmy tekst jawny:

Wracam we wtorek.

I podzielmy go na pary:

Wr ac am we wt or ek.

Kiedy odszukujemy litery danej pary w tabeli szyfrowej, możliwe są trzy przypadki:

1) Obie litery leżą w tym samym rzędzie
2) Obie litery leżą w tej samej kolumnie
3) Obie litery nie leżą ani w tym samym rzędzie ani w tej samej kolumnie.

<u>Przypadek 1)</u> Szyfrujemy litery zastępując je literami bezpośrednio po nich następującymi w tym samym rzędzie: AM zamienia się w RA

<u>Przypadek 2)</u> Szyfrujemy litery zastępując je literami znajdującymi się bezpośrednio pod nimi. Jeśli litera jest w ostatnim rzędzie, bierzemy pierwszą literą z tej kolumny. Z WR otrzymujemy zatem RK.

<u>Przypadek 3)</u> Od pierwszej litery pary posuwamy się w lewo lub w prawo do kolumny zawierającej drugą literę. Znajdująca się tam litera staje się pierwszą literą zaszyfrowanej pary. Drugą znajdujemy, przesuwając się poziomo od drugiej litery pary (w tekście jawnym) do kolumny, w której widnieje pierwsza litera. Oznacza to, iż AC oznacza ET, WE - ZR, WT - VK, OR - PA, EK – RC.

1

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

2

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

3

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

Zatem tekst jawny *Wracamwewtorek* zmienia się w *Rketrazrukparc*.

Enigma

Legendarna hitlerowska Enigma była najlepszą maszyną szyfrującą swojej epoki. Wynaleziona została przez Scheribiusa, a następnie wielokrotnie udoskonalana. W 1928 roku stworzył on maszynę wyposażoną w 26 wtyczek, przez które przechodziły przewody biegnące od klawiszy do wirników, i z powrotem do żarówek. Nowsze modele, Enigmy Wehrmachtu, miały 3 wirniki, jeden walec wracający i jedną łącznice. Mogły one mieć na przykład taki układ połączeń, że powstawał następujący szyfr:

ABCDEFGHIJKLMNOPQRSTUWXYZ
EYCFADHGOKJMLNIWQSRUTZPXBV

Chodzi tu o permutację tj. przestawianie, przy której np. A przechodzi w E, a E w A. Jeżeli zastosuje się ją do tekstu jawnego, a potem do powstałej wiadomości, to ponownie pojawi się pierwotny tekst. Taka permutacja to inwolucja[1].

Pod koniec wojny Enigma używana była często przez marynarkę. Posiadała ona cztery walce. Każdy z wirników zawierał część wewnętrzną wyposażoną po obu stronach w styki elektryczne. W jej środku znajdowały się druty łączące styki z jednej i drugiej strony. Część środkową obejmował pierścień. Na zewnętrznym obwodzie miał on dwadzieścia sześć liter alfabetu. Poza tym posiadał jedno lub dwa nacięcia zapewniające przenoszenie ruch na następny. Jeżeli wirnik był włożony do urządzenia, to w okienku obudowy ukazywała się litera na pierścieniu, dzięki czemu można było odczytać położenie wirnika.

Znajdująca się na wirniku zębatka pozwalała na obracanie walca z zewnątrz. Przy właściwym położeniu nacięcie pierścienia wyzwalały mechanizm, który przy następnym naciśnięciu klawisza przesuwał również następny wirnik o jedną literę naprzód. Pierścień z nacięciem oraz część środkowa wirnika z układem połączeń i stykami mogły się obracać względem siebie. Dawało to możliwość zmiany położenia pierścienia w stosunku do części środkowej.

Pierwsze sześć liter depeszy Enigmy.

Każda wiadomość szyfrowana za pomocą Enigmy posiadała na początku dwukrotnie występujący trzyliterowy klucz depeszowy, kodowany na podstawie klucza dziennego.

Schemat ten miał trzy wady:

1) Szyfrowanie pierwszych sześciu liter następował według klucza dziennego, co oznaczało, że przez cały dzień obowiązywało identyczne ustawienie wejściowe maszyny.
2) Pierwsze sześć liter każdej depeszy odpowiadało w tekście jawnym dwóm identycznym trójką liter. Jeśli na przykład meldunek zaczynał się od grupy DMQVBN, to pierwszy i czwarty znak odpowiadały identycznej literze alfabetu,

---

[1] <u>Inwolucja</u> to w matematyce przekształcenie mające tę właściwość, że wykonane kolejno dwa razy daje w wyniku przekształcenie tożsamościowe, to jest takie, w którym każdy punkt zostaje na swoim miejscu.

tyle że zaszyfrowanej przy innej permutacji. Ta sama sytuacja występowała w przypadku drugiej i piątej, oraz trzeciej i szóstej.

3) Walec odwracający drastycznie ograniczał liczbę możliwych permutacji, w rezultacie każda z nich była inwolucją.

Dzięki temu maszyna działała w sposób znacznie mniej losowy niż się to Niemcom wydawało. Słabości Enigmy umożliwiły Polakom na odczytywanie hitlerowskich depesz. Gdy pracownicy oddziału BS4 (w skład którego wchodzili między innymi wybitni polscy kryptolodzy: Marian Rejewski, Henryk Zygalski i Jerzy Różycki) dysponowali dużą ilością meldunków pochodzących z jednego dnia, otrzymywali wiele informacji na temat pierwszych sześciu permutacji Enigmy przy danym kluczu dziennym. Tymczasem Polakom dodatkowo ułatwiano pracę. Szyfranci dla wygody obierali jako klucz depeszowy trzy takie same lub sąsiadujące ze sobą na klawiaturze litery.

Zdrada niemieckiego agenta a Enigma.

Na początku 1931 roku, niemiecki pracownik ministerstwa sił zbrojnych, Hans Thilo Schmidt, przekazał francuskiemu wywiadowi informacje dotyczące maszyn szyfrujących, między innymi Enigmy. Podczas spotkań mających miejsce w różnych miastach Europy Asche (Hans Thilo Schmidt) przekazał kopię niemieckiej instrukcji wojskowej dotyczącą Enigmy, a ponadto klucze dzienne na wrzesień i październik 1932 roku, czyli pozycje wyjściowe wirników dla każdego dnia, położenia pierścieni i układ wtyczek w łącznicy. Bertrand (szef francuskiego biura szyfrów) przekazał uzyskane informacje do Warszawy w grudniu 1932 roku. Mając dostęp do depesz z poprzednich miesięcy, Polacy mogli nie tylko rozszyfrować wiadomości, ale dokonując zestawienia tekstu tajnego z jawnym zdobyć więcej materiałów na temat połączenia układów elektrycznych walców Enigmy. W roku 1934 Polacy mieli szyfr Enigmy w ręku.

W tym czasie Niemcy zaczęli się bać o tajemnicę Enigmy i dlatego podjęli kroki mające uniemożliwić złamania szyfru. Polacy starali się sprostać zadaniu, choć było ono wyjątkowo trudne. Nawet jeśli się znało układ połączeń elektrycznych, to na podstawie pierwszych sześciu liter trudno było wywnioskować kolejność wirników, pozycję pierścieni, położenie wyjściowe i układ wtyczek. By to osiągnąć, trzeba było dysponować dużą ilością meldunków szyfrowanych tym samym kluczem dziennym. Dla ułatwienia sobie pracy trzej matematycy skonstruowali maszynę podobną do Enigmy. Zawierała dwa zestawy po trzy wirniki. Miały one takie układy połączeń elektrycznych jak walec Enigmy i dawały się obracać oddzielnie. Ponad to był tam komplet dwudziestu sześciu lampek i takiej samej liczby wyłączników. Urządzenie to, nie miało jednak służyć ani do szyfrowania, ani do dekryptarzu. Jego zadanie polegało na ułatwianiu rozpoznawania pewnych charakterystycznych cech permutacji alfabetu, uzyskiwanych przy różnych położeniach wirników. W tym celu polscy kryptolodzy wypróbowali wszystkie możliwe kombinacje, których było 17576 (26 do sześcianu). Maszynę tę nazwano cyklometrem. Dzięki niej pracownicy BS4 sporządzili katalog, na podstawie którego mogli szybko znaleźć klucz dzienny już po paru depeszach.

Jednakże Niemcy postanowili wprowadzić kilka udoskonaleń do swej Enigmy. Zastosowali nowy walec obrotowy, a z czasem dodali dwa nowe walce. W efekcie szyfranci mieli do dyspozycji pięć wirników, z których wybierano trzy. Polscy kryptolodzy mieli do sprawdzenia dziesięciokrotnie więcej możliwości. Cyklometr już nie wystarczał. Aby móc rozszyfrowywać depesze pochodzące z nowej, ulepszonej Enigmy, Polacy musieli skonstruować jeszcze doskonalsze urządzenie. Ochrzcili je „bomba”. Symulowała ona pracę sześciu Enigm. Zbudowano sześć egzemplarzy tego urządzenia. Niestety do dzisiaj nie zachowała się ani jeden egzemplarz, dlatego nikt nie wie dziś dokładnie, w jaki sposób działał ten fenomen polskiej kryptografii.

W dniu 25 lipca 1938 roku w Pyrach pod Warszawą spotkali się przedstawiciele polskiego, brytyjskiego i francuskiego wywiadu. Polacy przekazali wówczas informacje na temat swych dotychczasowych badań. Postanowiono, że dla dobra sprawy, biura szyfrów podzielą się obowiązkami. Polacy kontynuowali pracę nad dekryptacją, Francuzi wykorzystali swe kontakty z Niemcami w celu przechwycenia wiadomości na temat wirników, a Brytyjczycy zbudowali więcej „bomb”. Wkrótce po tym Hitler wypowiedział Polsce wojnę, co bardzo utrudniło dalsze prace. Biuro szyfrów zostało zamknięte, matematyków wywieziono z kraju, a siedzibę BS4 zniszczono.

Jednak w roku 1940 stacjonujący we Francji Polacy w końcu odkryli tajemnicę ulepszonej Enigmy.

Szyfr liczb pierwszych

Szyfr ten jest wymyślony przez autorów.

Szyfr ten można przydzielić do grupy szyfrów polialfabetycznych. Działa on na następujących zasadach:

Za każdym razem, gdy numer danej litery w tekście jest liczbą pierwszą, to znak szyfrogramu jest znakiem tekstu jawnego przesuniętego o jedną literę w alfabecie do tyłu, natomiast gdy numer ten nie jest liczbą pierwszą, to literę w alfabecie przesuwamy do przodu. Przy szyfrowaniu możemy skorzystać z takiej oto tabelki:

1	**2**	**3**	**4**	**5**	**6**		**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
J	E	S	T	E	M		Z	A	G	R	O	Ż	O	N	Y

Przykładowo możemy chcieć zaszyfrować zdanie:

Jestem zagrożony.

Litera *j* ma w tekście numer pierwszy. Jedynka nie jest liczbą pierwszą, dlatego też literę *j* zastępujemy przez literę znajdującą się po niej w alfabecie polskim. Tą literą jest *k*. Następnie szyfrujemy kolejną (drugą) literę tekstu, czyli *e*. Dwójka jest liczbą pierwszą, to też zostaje zastąpiona przez literę, która jest w alfabecie przed nią– *d*. Z kolei literę numer 3, *s*, zamieniamy na, *r*, ponieważ trójka jest liczbą pierwszą. Szyfrujemy takim sposobem cały tekst. Efektem jest szyfrogram:

Kdrśdł yąhsńźńńz.

Osoba, do której jest zaadresowana zaszyfrowana wiadomość musi znać instrukcję szyfrowania, by ją odczytać.

Zakończenie

W naszej pracy opisaliśmy najważniejsze według nas szyfry historyczne. Można zaryzykować twierdzenie, iż są to „kultowe pozycje” dla każdego miłośnika kryptogramów.

Potrzeba szyfrowania wiadomości zawsze towarzyszyła ludziom, szczególnie od czasu kiedy zaczęli posługiwać się pismem. Szyframi posługiwano się pragnąc chronić zwłaszcza tajemnice państwowe lub wojskowe. Używano ich jednak też w innych okolicznościach np. przekazując sobie poufne wiadomości z życia prywatnego.

Metody szyfrowania, wraz z upływem czasu, udoskonalały się zmieniając się na coraz bardziej skomplikowane i trudniejsze do odczytania. Ciekawe jest to, że szyfry były wymyślane nie tylko przez matematyków i kryptografów, ale także polityków (Juliusz Cezar), historyków (Polibiusz), czy też duchownych (Thritemius). Mamy nadzieję, iż po lekturze naszej pracy czytelnik nie umarł z nudów.

Autorzy.

Bibliografia

Piśmiennictwo:

1. I.N. Bronsztein, K.A. Siemiendiajew, **Matematyka. Poradnik encyklopedyczny**, Warszawa 2003

2. R. Kippenhahn, **Tajemne przekazy. Szyfry, Enigma i karty chipowe**, Warszawa 2000

3. **Wielka Encyklopedia PWN**, tom 8, Warszawa 2002

4. **Wielka Encyklopedia PWN**, tom 15, Warszawa 2003

Strony internetowe:

1. http://pl.wikipedia.org/wiki/Szyfr_przesuwaj%C4%85cy

2. http://pl.wikipedia.org/wiki/Szyfr_monoalfabetyczny

3. http://pl.wikipedia.org/wiki/Szyfry_wieloalfabetowe

4. http://pl.wikipedia.org/wiki/Szachownica_Polibiusza

5. http://pl.wikipedia.org/wiki/Szyfr_kombinowany

6. http://pl.wikipedia.org/wiki/Szyfr