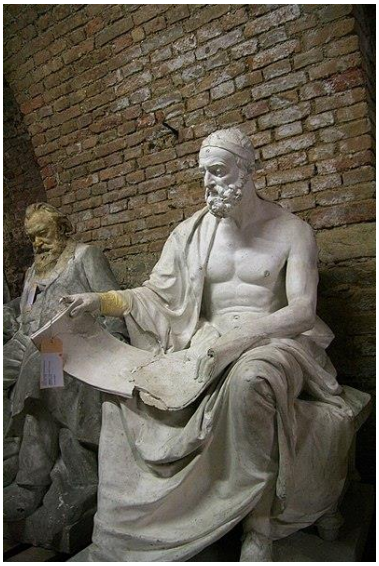
Szachownica Polibiusza



Grecki pisarz Polibiusz wymyślił system sygnalizacyjny, stosowany powszechnie jako jedna z metod kryptograficznych. Jest znany jako Szachownica Polibiusza.

To rodzaj szyfru monoalfabetycznego (ukryta litera odpowiada literze jawnej), który swoją nazwę zawdzięcza słynnemu antycznemu historykowi i pisarzowi – Polibiuszowi. Jak sam Polibiusz przekazuje nam w swoich „Dziejach", autorem szyfru są Grecy – Kleoksenos i Demoklet – jednak on podjął się usprawnienia mechanizmu.

Szachownica Polibiusza składała się z pięciu tabliczek, gdzie na każdej znajdowało się pięć liter greckich (wyjątkiem była ostatnia, gdzie były tylko cztery litery; w wersji łacińskiej każda tabliczka ma pięć liter). Do naszych czasów nie zachowała się żadna oryginalna tabliczka z szyfrem.

Grecka wersja	Rzymska wersja
Α Β Γ Δ Ε Ζ Η Θ Ι Κ Λ Μ Ν Ξ Ο Π Ρ Σ Τ Υ Φ Χ Ψ Ω	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

Jak informuje Polibiusz, usprawnienie szyfrowania wiadomości było istotne do wysyłania pilnych i nieoczywistych informacji. Dotychczasowe metody umożliwiały wysyłanie jedynie wcześniej ustalonych i oczekiwanych formatów wiadomości.

Aby przekazanie wiadomości mogło się odbyć, obie strony musiały posiadać tabliczki z alfabetem. Przekazywanie sygnałów odbywało się za pomocą sygnalizacji świetlnej (pochodni) i jak informuje Polibiusz, sygnalizatorzy po obu stronach musiały wpierw potwierdzić, że przekaz wiadomości jest w danej chwili możliwy. W tym celu człowiek nadający informację podnosił dwie pochodnie i czekał na podobną odpowiedź ze strony przeciwnej. Następnie, kiedy obie strony były pewne, że przekaz szyfru jest możliwy, osoba nadająca wiadomość podnosiła odpowiednią ilość pochodni po lewej stronie, wskazując wiersz-tabliczkę. Następnie nadawca podnosił odpowiednią ilość pochodzi po prawej stronie, wskazując kolumnę. W ten sposób można było przekazać wiadomość na odległość np. między posterunkami wojskowymi.

Szyfrowanie metodą Polibiusza

Metoda ta polega na ułożeniu liter w kwadrat, którego wiersze i kolumny są ponumerowane.

	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

Każda litera może być reprezentowana za pomocą dwóch liczb: numeru wiersza i numeru kolumny. Tak, więc litera **B** to **12**, a litera F to **21**. Przykładowe słowo zakodowane przy pomocy:

D	O	M	E	C	Z	E	K
14	34	32	15	13	55	15	25

Słowo DOMECZEK jest zastąpione przez zbiór liczb *14 34 32 15 13 55 15 25*. Odszyfrowanie wiadomości polega na wyszukaniu w odpowiednich polach właściwych liter wiadomości.

Istnieje wiele odmian tej metody.

Litery mogą być wewnątrz kwadratu różnie rozmieszczone, Liczby zastępujące litery mogą być dodatkowo szyfrowane, dodawany do nich jakiś współczynnik maskujący statystyczne właściwości liter, liczby można grupować po 5 cyfr itp.

Deszyfrowanie

Generalnie zasada deszyfrowania polega na podaniu konkretnych cyfr, które oznaczają położenie danej litery w tabeli – pierwszą cyfrą jest numer wiersza, a drugą – kolumny. W ten sposób, słowo: **CEZAR** w zaszyfrowanej wersji przyjmuje postać: 13 15 55 11 42.

Wymagane jest posiadanie dwóch tych samych kompletów tablic.

Podatność na kryptoanalizę statystyczną

Najprostszą metodą dekryptażu jest ***analiza częstości***. Przy zapisie w postaci par liczb, należy sprawdzić rozkład częstości ich występowania i dopasować go do statystyki danego języka.

W wypadku występowania metod maskujących te cechy, należy wykorzystać ***cechy charakterystyczne informacji*** przysłanych tą metodą lub ***metodę słów prawdopodobnych***.

Wersja rozbudowana

W wersji rozbudowanej można pracować na tablicy kwadratowej o długości boku 10, co daje 100 pól do wyboru (10 x 10).

W takiej tablicy można zwielokrotnić niektóre litery (częściej używane), sylaby a nawet niektóre słowa, frazy czy zdania.

Większa opcja jest przydatna zwłaszcza przy alfabetach mających więcej liter (np. polski).

	0	1	2	3	4	5	6	7	8	9	
0		м	ш	з	ю	о					0
1	и	н	в	г	л	е					1
2	ж	б	р	к	ц	ь					2
3	ф	д	т	щ	я	а					3
4	с	ы	ч	п*	у	х					4
5											5
6											6
7											7
8											8
9											9
	0	1	2	3	4	5	6	7	8	9	

Rysunek 1 - Szyfr Rewolucja

Ćwiczenie

1. Napisz program szyfrujący (rozmiar 5 x 5) korzystający z szyfru Polibiusza:
   a) Szyfrujący wiadomość
   b) Deszyfrujący wiadomość
   c) Zamień w wiadomości literę j na i.

2. Napisz program szyfrujący korzystający z szyfru Polibiusza:
   a) Szyfrujący i deszyfrujący wiadomość
   b) Rozmiar tablicy ma wynosić 8 x 8 (postać taka jak w przykładzie poniżej)
   c) Dodaj małe i duże litery
   d) Dodaj cyfry

Uwagi do programów

Dokładne odwzorowanie tematu ćwiczenia	10 pkt
Komentarze (w języku polskim)	3 pkt
Zmienne umożliwiające dostęp do indeksów tablic, łańcuchów tekstowych powinny być krótkie i literami typu i. j. k l itp.	2 pkt

Postać tablicy w programie:

```
tab = [['a', 'b', 'c', 'd' , 'e'],
       ['f', 'g', 'h', 'i' , 'k'],
       ['l', 'm', 'n', 'o' , 'p'],
       ['q', 'r', 's', 't' , 'u'],
       ['v', 'w', 'x', 'y' , 'z'],]
```