Szyfr Playfaira

Charles Wheatstone i Lyon Playfair w 1854 zademonstrowali pierwszy w świecie szyfr digraficzny (digramowy). Szyfruje się w nim dwie litery tak, by wynik był zależny od nich obu jednocześnie.

Moc szyfru polega na zatarciu charakterystycznej cechy szyfru jednoznakowego. Litery nie są identyfikowane jako samodzielne jednostki. Szyfrowi brak też charakterystycznych punktów zaczepienia jak np. podwojone litery.

Dodatkowym atutem jest zastosowanie wymieszanego alfabetu szyfrowego.

Szyfr działa dla tablicy zarówno prostokątnej jak i kwadratowej.

Ułożenie tablicy szyfrującej

Pierwszym krokiem jest ułożenie tablicy szyfrującej.

Składają się na nią:

1. Klucz szyfrujący

S	Z	A	L	O	N	E	K	U	R	Y

2. Tablica z alfabetem (w którym I oraz J są na tej samej pozycji)

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

Tabela wyjściowa składa się z klucza szyfrującego pod którym wypisywano pozostałe litery alfabetu.

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

Szyfrowanie metodą Playfaira

W szyfrze używa się jednocześnie dwóch liter tak, by wynik był zależny od nich obu jednocześnie.

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

Tablica szyfru Playfaira (ze słowem SZALONEKURY)

Przykładowym hasłem niech będzie słowo: **chlorella**.

Aby zaszyfrować tekst jawny, należy podzielić go na pary liter: **ch lo re ll a**

Litery **i** oraz **j** są traktowane jako identyczne, czyli że słowo *kijki* byłoby szyfrowane jak *kiiki*.

Jednakowe litery występujące razem w parze muszą być rozdzielone literą **x**, co oznacza, że słowo **chlorella** byłoby szyfrowane jak **ch lo re lx a**;

Jeśli słowo ma nieparzystą liczbę liter, na końcu dodajemy jakąś rzadko używaną literę np. **x**. Słowo **chlorella** byłoby szyfrowane jak **ch lo re lx ax**;

Konfiguracje par liter:

Litery każdej pary mogą występować w tym samym wierszu, w tej samej kolumnie, lub nie występować w żadnym z tych położeń.

- Litery stojące w tym samym wierszu są zastępowane literami bezpośrednio znajdującymi się na prawo od nich. Tak, więc *sa* = ZL, *hi* = IM, *yb* = BC. Każdy wiersz jest traktowany jako cykliczny, a zatem literą leżącą na prawo od ostatniej w danym wierszu będzie pierwsza litera po lewej w tym wierszu. Tak, więc ***lo*** - **OS**, ***re*** = **NK**.

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

- Litery występujące w tej samej kolumnie są zastępowane literami znajdującymi się bezpośrednio pod nimi. Tu też obowiązuje zasada cykliczności (literą leżącą w dół od ostatniej w danej kolumnie, będzie pierwsza litera od góry tej kolumny). Tak, więc *ak* - KC, *he* = TB, *ht* = TZ, *uw* = DL.

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

- Jeśli litery tekstu jawnego nie występują ani w tym samym wierszu, ani w tej samej kolumnie, to każda z nich jest zastępowana literą z jej własnego wiersza, stojącą w kolumnie, w której znajduje się druga litera tekstu jawnego.

Aby na przykład zaszyfrować ***ch***, należy najpierw zlokalizować je w kwadracie. Potem trzeba przesuwać się wzdłuż wiersza z pierwszą literą ***c***, aż napotka się kolumnę, w której występuje druga litera tekstu jawnego ***h***:

	Z			
	E			
Y	**B**	C	D	F
	H			
	T			

Litera położona w miejscu przecięcia wiersza i kolumny **B** staje się pierwszą literą szyfru. Teraz należy podążać wzdłuż wiersza z drugą literą tekstu jawnego (***h***), aż dotrze się do przecięcia wiersza z kolumną, w której występuje pierwsza litera tekstu jawnego (***c***):

		A		
		K		
		C		
G	H	**I**	M	P
		V		

Litera położona w miejscu przecięcia I staje się drugą literą szyfru. W ten sposób otrzymuje się *ch* = BI. W celu zachowania porządku liter najpierw bierze się zawsze pierwszą literę tekstu jawnego.

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

Przykładowy klucz: **szalonekury**
Tekst do zaszyfrowania: **chlorella**
Tekst zaszyfrowany: **biosnkowov**

Deszyfrowanie

Deszyfrowanie w tym ostatnim przypadku odbywa się dokładnie tak samo jak szyfrowanie: jeśli *ow* = SY, to *sy* = OW.

W pozostałych dwóch przypadkach jako litery tekstu jawnego należy wziąć litery znajdujące się na lewo lub powyżej liter szyfrogramu.

Podatność na kryptoanalizę statystyczną

Szyfr Playfaira jest dość dobrze odporny na kryptoanalizę statystyczną.

Jako szyfr digraficzny zaciera on charakterystyczną cechę szyfru jednoznakowego - znak ***e***, na przykład, nie jest identyfikowany, jako samodzielna jednostka. Szyfrowi brak też charakterystycznych punktów zaczepienia jak np. podwojone litery.

Należy wykorzystać ***analizę częstości par liter***.

Szyfrowanie digraficzne zmniejsza o połowę liczbę elementów dostępnych przy analizie częstości. Tekst 100-literowy będzie liczyć tylko 50 zaszyfrowanych bigramów.

Liczba bigramów jest o wiele większa niż liczba pojedynczych liter. W języku angielskim jest 26 liter, ale 676 digrafów. Dwie najczęściej występujące w angielskim litery,

e i ***t***, mają średnią częstość 12 i 9 procent; dwa najczęstsze w angielskim digrafy, ***th*** i ***he***, osiągają częstość tylko 3¼ i 2½ procent. To nie tylko więcej jednostek do analizy, ale są one jednocześnie niezbyt zróżnicowane.

Do łamania takich szyfrów należy raczej wykorzystać inne ***cechy charakterystyczne informacji*** przesyłanych tą metodą lub ***metodę słów prawdopodobnych***.

Ćwiczenie:

1. Napisz program kryptograficzny używający metody Playfaira.

2. Program ma mieć następujące właściwości:

Poprawne zaimplementowanie szyfrowania i deszyfrowania metodą Playfaira	10 pkt
Menu wyboru operacji: • Szyfrowanie • Deszyfrowanie • Wyjście	2 pkt
Z tekstu wejściowego usuwać **j** zamieniając je na **i**	1 pkt
Redukować podwójne litery	1 pkt
Uwzględniać nieparzystą ilość znaków tekstu wejściowego	1 pkt
Uzyskanie tekstu odszyfrowanego analogicznego z wejściowym	2 pkt
Komentarze opisujące co robi dany fragment programu	2 pkt
Używać polskich nazw i tekstów	1 pkt

3. Dane kontrolne:

Klucz	**Tekst jawny**	**Tekst zaszyfrowany**
szalonekury	domeknaprerii	flhuueoinkkppv
czarek	hellenistyczny	ncmwgtmpyezate
handel	abrakadabra	bkwbrbenkwnw
Szkola	odleglosci	diemmzlzdh