Eksploatacja i bezpieczeństwo systemów

dr inż. Mirosław Mazurek

Zakład Systemów Złożonych
Bud. F, pok. 305, tel. 17 865 11 04

Kryptografia - podstawowe definicje

Kryptografia – sztuka ochrony danych w taki sposób, aby tylko powołana osoba mogła je odczytać. Jest realizowana za pomocą szyfrowania (encryption). Proces odwrotny do szyfrowania to deszyfracja (decryption).

Kryptoanaliza – sztuka czytania zaszyfrowanych wiadomości bez posiadania odpowiednich uprawnień (klucza, algorytmu) – łamanie szyfrów.

Kryptologia – połączenie kryptografii i kryptoanalizy.

Kryptogram (informacja zaszyfrowana) – to zwykła informacja (tzw. Jawna) przetworzona przez funkcję szyfrującą do postaci nieczytelnej.

Funkcja szyfrująca – przetwarza informację (jawną) na nieczytelną (zaszyfrowaną)

Funkcja deszyfrująca – przetwarza informację zaszyfrowaną (nieczytelną) na jawną (odszyfrowaną).

$$E(M) = C$$
$$D(C) = M$$
$$D(E(M)) = M$$

Kategorie łamania szyfrów

Jeśli koszt złamania szyfru jest większy niż wartość zaszyfrowanej informacji, to prawdopodobnie szyfr jest bezpieczny.
Jeśli czas niezbędny do złamania szyfru jest dłuższy niż czas, w którym dane muszą być utajnione, to prawdopodobnie szyfr jest bezpieczny.
Jeśli ilość danych zaszyfrowanych z zastosowaniem pojedynczego klucza jest mniejsza niż ilość danych niezbędnych do złamania szyfru, to prawdopodobnie jesteś bezpieczny.

Kategorie łamania szyfrów:

1. Całkowite złamanie szyfru.

2. Ogólne wnioskowanie.

3. Lokalne wnioskowanie.

4. Częściowe wnioskowanie.

Kategorie łamania szyfrów

Algorytm jest **bezwarunkowo bezpieczny** (unconditionaly secure), jeśli niezależnie od liczby szyfrogramów, które kryptoanalityk ma, nie jest możliwe odtworzenie tekstu jawnego.

Algorytm jest uznawany za **obliczeniowo bezpieczny** lub **silny**, jeśli nie może być złamany za pomocą dostępnych (teraz i w przyszłości) środków.

Miary złożoności metod łamania szyfrów:

1. **Złożoność danych** – ilość danych wymaganych jako dane wejściowe metody łamania szyfru.

2. **Złożoność przetwarzania** – czas wymagany do złamania szyfru (nakład pracy)

3. **Wymagania pamięci** – wielkość pamięci niezbędnej do złamania szyfru.

Metody łamania szyfrów

1. Łamanie z szyfrogramami (ciphertext-only attack)

Dostępne są kryptogramy wielu wiadomości zaszyfrowanych za pomocą tego samego algorytmu szyfrującego. Jego zadaniem jest odtworzenie tekstu jawnego jak największej ilości wiadomości lub odtworzenie klucza (kluczy), które wykorzystane zostały do zaszyfrowania wiadomości, żeby potem za jego pomocą otrzymać tekst jawny dostępnych wiadomości.

2. Łamanie ze znanym tekstem jawnym (known-plaintext attack)

Dostępne są zarówno kryptogramy wielu wiadomości, jak i ich teksty jawne. Jego zadaniem jest znalezienie klucza (kluczy), które wykorzystane zostały do zaszyfrowania wiadomości lub też opracowanie algorytmu umożliwiającego deszyfrowanie kolejnych wiadomości zaszyfrowanych z tym samym kluczem (kluczami).

3. Łamanie z wybranym tekstem jawnym (chosen-plaintext attack)

Dostępny jest wybrany tekst jawny i jego kryptogram. W takiej sytuacji można wybrać określony tekst jawny do zaszyfrowania i tym samym uzyskać więcej informacji o kluczu. Jego zadaniem jest wywnioskowanie klucza (kluczy), które wykorzystane zostały do szyfrowania lub opracowanie algorytmu do deszyfrowania kolejnych wiadomości zaszyfrowanych tym samym kluczem (kluczami).

Metody łamania szyfrów

4. Łamanie z adaptacyjnie wybranym tekstem jawnym (adaptiv-chosen-plaintext attack)

Dostępny jest wybrany tekst jawny i możliwość wykonania kolejnych prób, w których dobiera się tekst jawny w odpowiedzi na wyniki otrzymane z poprzednich szyfrowań. Łamiący może wybierać spośród bloków tekstu jawnego, biorąc pod uwagę wyniki poprzednich wyborów.

5. Łamanie z wybranym szyfrogramem (chosen-ciphertext attack)

Dostępne są różne kryptogramy do deszyfrowania, a także dostęp do tekstu jawnego. Jego zadaniem jest znalezienie klucza.

6. Łamanie z wybranym kluczem (chosen-key attack)

Dostępna jest wiedza o powiązaniach pomiędzy różnymi kluczami.

Metody łamania szyfrów

7. Łamanie z gumową pałką (rubber-hose cryptoanalysis)

Metoda ta zakłada groźby i przemoc wobec osoby posiadającej klucz. Możliwe jest również przekupstwo. Wbrew pozorom jest to bardzo skuteczna metoda, często również określana jako najlepsza (i najtańsza).

8. **Łamanie brutalne**

Metoda ta polega na sprawdzaniu wszystkich możliwych kluczy dopóki nie otrzyma się tekstu jawnego. Określana jest jako najbardziej prymitywna, jednak w połączeniu z dużą mocą obliczeniową kilku komputerów jest w stanie przynieść oczekiwane rezultaty. Algorytm ten jest tym wydatniejszy, im bardziej ograniczona jest pula potencjalnych kluczy. Klucz powinien być wygenerowany nie tylko za pomocą liter i cyfr, ale także znaków specjalnych. Czas łamania szyfru w dużej mierze zależy od złożoności klucza. Oszacowanie złożoności obliczeniowej w przypadku łamania brutalnego nie jest skomplikowane; jeżeli klucz ma długość 8 bitów, to bada się $2^8=256$ możliwych kluczy. Dla klucza zapisanego na 64 bitach potrzebne jest około 585 000 lat badań.

Rodzaje szyfrów

Szyfry podstawieniowe

- Prosty szyfr podstawieniowy
- Homofoniczny szyfr podstawieniowy
- Poligramowy szyfr podstawieniowy
- Wieloalfabetowe szyfry podstawieniowe

Szyfry przestawieniowe (transpozycyjne)

XOR

Szyfrowanie przestawieniowe

Szyfrowanie przestawieniowe polega na odczytywaniu znaków według określonego schematu. Metoda ta stanowi permutację tekstu jawnego. Oznacza to, że zawiera te same znaki, co w oryginale, jednak ich kolejność jest zmieniona. Proces ten nazywany jest również transpozycją.

Przykład 1

Wiersze macierzy o wymiarach 3x3 zostały kolejno wypełnione tekstem jawnym, z pominięciem znaków białych. Wiadomość ta zostanie zaszyfrowana dzięki zamianie domyślnej kolejności odczytu poszczególnych pól.

Tekst jawny:
ALA MA KOTA

A	L	A
M	A	K
O	T	A

Kryptogram będzie wynikiem odczytywania poszczególnych pól nie wierszami, ale kolumnami, czytanymi od strony lewej do prawej, od góry do dołu.

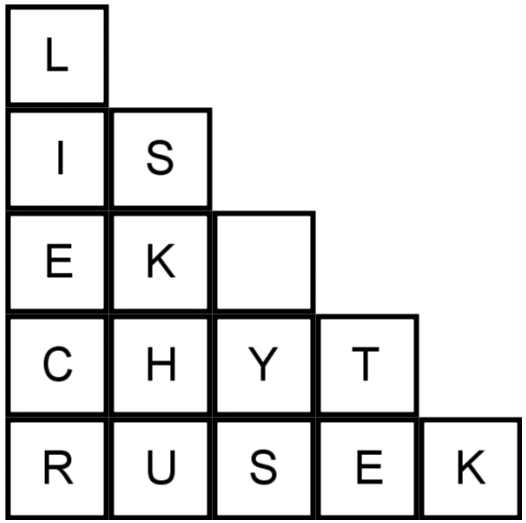
Tekst zaszyfrowany:
AMOLATAKA

Szyfrowanie przestawieniowe

Przykład 2

Tworzymy dowolną figurę geometryczną i wypełniamy ją wierszami tekstem jawnym (w tym przypadku razem ze znakami białymi). Następnie odczytujemy ją kolejnymi kolumnami, zaczynając od ostatniej (najbardziej z prawej) aż do pierwszej (najbardziej z lewej), od góry do dołu.

Tekst jawny:
LISEK
CHYTRUSEK



Tekst zaszyfrowany:
KTE YSSKHULIECR

Szyfrowanie przestawieniowe

Przykład 3

Macierz wypełniona została tekstem jawnym, razem ze znakami białymi użytymi dowolną ilość razy. Jej pierwszy wiersz posłużył jako zbiór pól, które zawierają sumę znaków każdej kolumny. Zaszyfrowanie tych znaków będzie polegało na odczytywaniu ich kolumnami – od największej sumy do najmniejszej, przeszukując kolumny w kolejności od lewej do prawej, a więc w przypadku powtarzającej się sumy znaków, odczytujemy pierwszą z lewej.

Tekst jawny:

SIEROTKA MARYSIA

4	3	4	4	1
S	I		E	
R		O	T	
K	A	M	A	
R	Y	S	I	A

Tekst zaszyfrowany:

AI AY OMS SRKR ETAI

Szyfrowanie przestawieniowe

Przykład 4

Dana jest macierz 3x3, do której wprowadzono tekst jawny, bez użycia znaków białych. Szyfrowanie w tym przypadku będzie algorytmem, w którym odczytywane będą kolejne iteracje dla zamalowanych według indywidualnie zdefiniowanego schematu pól, zaczynając od pierwszej kolumny.

Tekst jawny: NIEDZIELA

Iteracja pierwsza:

N	I	E
D	Z	I
E	L	A

Iteracja druga:

N	I	E
D	Z	I
E	L	A

Iteracja trzecia:

N	I	E
D	Z	I
E	L	A

Tekst zaszyfrowany: NZADLEEII

Szyfrowanie podstawieniowe

Szyfry podstawieniowe to takie, w których każdy ze znaków tekstu jawnego jest zastępowany innym, w wyniku działania określonego lub indywidualnie zdefiniowanego algorytmu. Efektem jego użycia tekst jawny zostaje zaszyfrowany w sposób zrozumiały tylko dla odbiorcy, który może go odszyfrować odwracając wykonane podstawienie, tym samym uzyskując oryginalną wiadomość.

Proste szyfry podstawieniowe

Proste szyfry podstawieniowe wykorzystują jednoznaczne odwzorowanie:

$$f: m_i \rightarrow f(m_i)$$

Każdy znak tekstu jawnego zastępowany jest odpowiadającym mu innym znakiem. Tekst ten składa się ze znaków określonych m_1, m_2, … , m_i. Zaszyfrowanie prostym szyfrem podstawieniowym polega na przekształceniu każdego znaku tak, aby otrzymać:

$$E_f(m) = f(m_1)f(m_2) \ldots f(m_i)$$

Szyfrowanie podstawieniowe

Litera	Homofony			
P	14	37	59	23
O	45	06	33	12
L	54	88	22	13
I	77	69	21	02
T	99	11	83	55
E	07	60	44	42
C	32	46	91	94
H	16	82	39	25
N	04	09	01	19
K	28	38	48	58
A	53	93	65	92

Szyfr homofoniczny

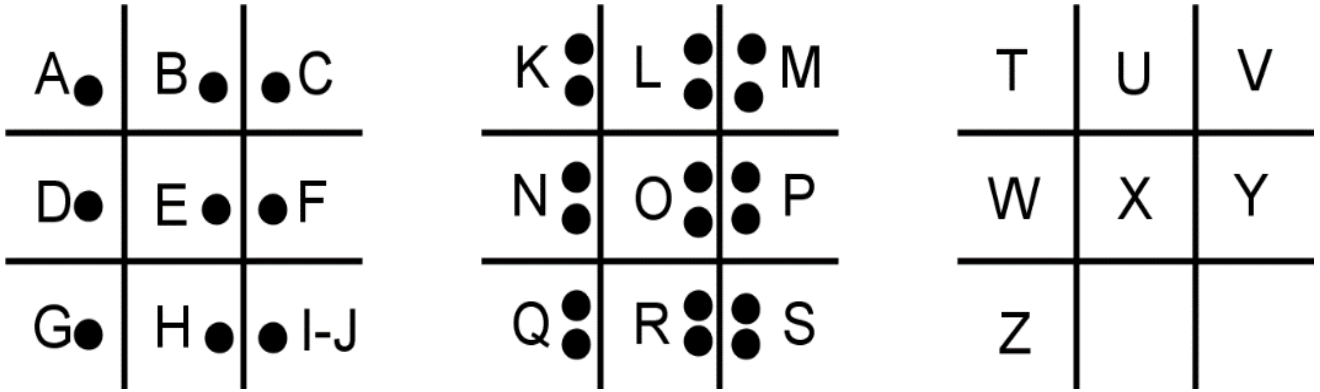
W szyfrze tym każdej literze tekstu jawnego odpowiada zbiór homofonów (kryptogramów). Liczba poszczególnych homofonów powinna być zależna od częstości występowania danej litery w tekście jawnym (nie mniejsza niż ilość powtarzających się liter). Przy szyfrowaniu każdej litery wybiera się losowo homofon, który jej odpowiada.

Tekst jawny:	P	O	L	I	T	E	C	H	N	I	K	A
Tekst zaszyfrowany:	23	06	88	77	11	60	91	16	01	69	38	92

Szyfrowanie podstawieniowe

Szyfr cmentarny

Szyfr ten polega na zapisywaniu tekstu jawnego za pomocą odpowiednich symboli, pokazanych niżej.

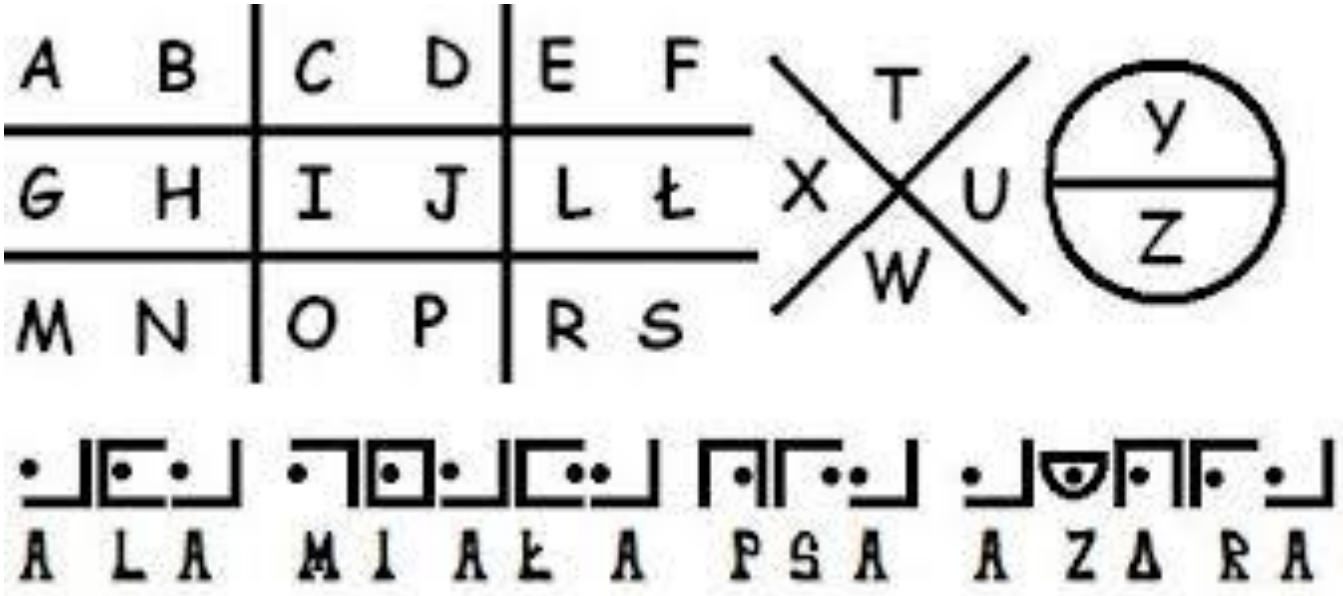


Przykład

Tekst jawny: POLITECHNIKA

Tekst zaszyfrowany:

Szyfr harcerski



Szyfrowanie podstawieniowe

Szyfr Cezara

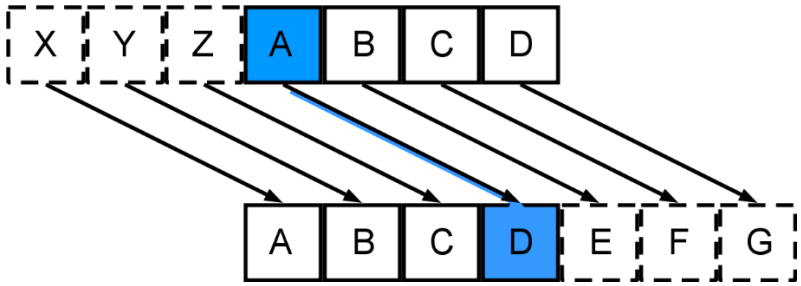
Szyfr Cezara jest odmianą prostego szyfru podstawieniowego monoalfabetycznego – zalicza się go szyfrów przesuniętych. Za jego pomocą Juliusz Cezar w I wieku p.n.e. szyfrował swoje listy do Cycerona. Pomimo prostoty używany był również przez armię rosyjską w czasie I wojny światowej.

Każda litera tekstu jawnego przesuwana jest o 3 miejsca w prawo w alfabecie. Proces ten można zapisać w następujący sposób:

$$E_n(x) \equiv x + n \pmod{32}$$

gdzie:

$$x - numer\ litery\ tekstu\ jawnego\ w\ alfabecie,$$
$$E_n(x) - numer\ litery\ szyfrogamu\ w\ alfabecie.$$



Szyfrowanie podstawieniowe

Szyfr Cezara

Algorytm deszyfrowania:

$$D_n(y) \equiv y - n \pmod{32}$$

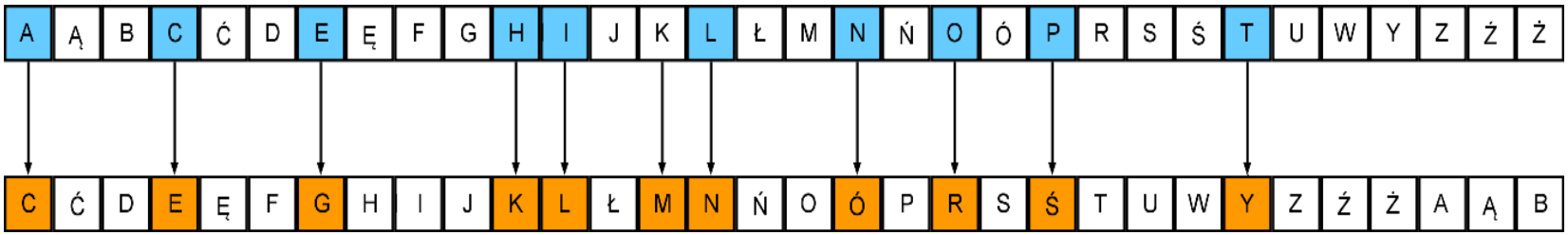
gdzie:

$$y - numer\ litery\ szyfrogramu\ w\ alfabecie,$$
$$D_n(y) - numer\ litery\ tekstu\ jawnego\ w\ alfabecie.$$

Przykład

Zaszyfrowanie słowa z wykorzystaniem polskiego alfabetu.

Tekst jawny: POLITECHNIKA



Tekst zaszyfrowany: ŚRNLYGEKÓLMC

Szyfrowanie podstawieniowe

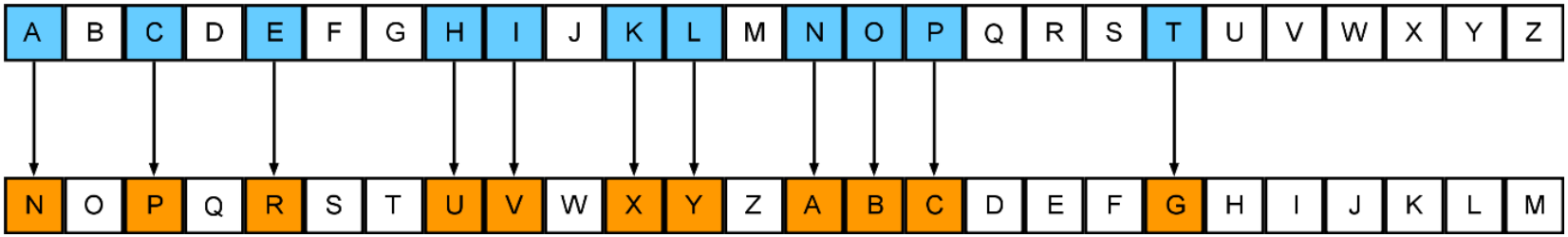
Szyfr ROT-13

Używany był do komunikacji w grupach dyskusyjnych, głównie w celu cenzurowania niedozwolonych słów. Zasada działania jest analogiczna do szyfru Cezara z tym wyjątkiem, że przesunięcie odbywa się co 13 znaków, a nie 3.

Przykład

Zaszyfrowanie słowa z wykorzystaniem alfabetu łacińskiego.

Tekst jawny: POLITECHNIKA



Tekst zaszyfrowany: CBYVGRPUAVXN

Szyfrowanie podstawieniowe

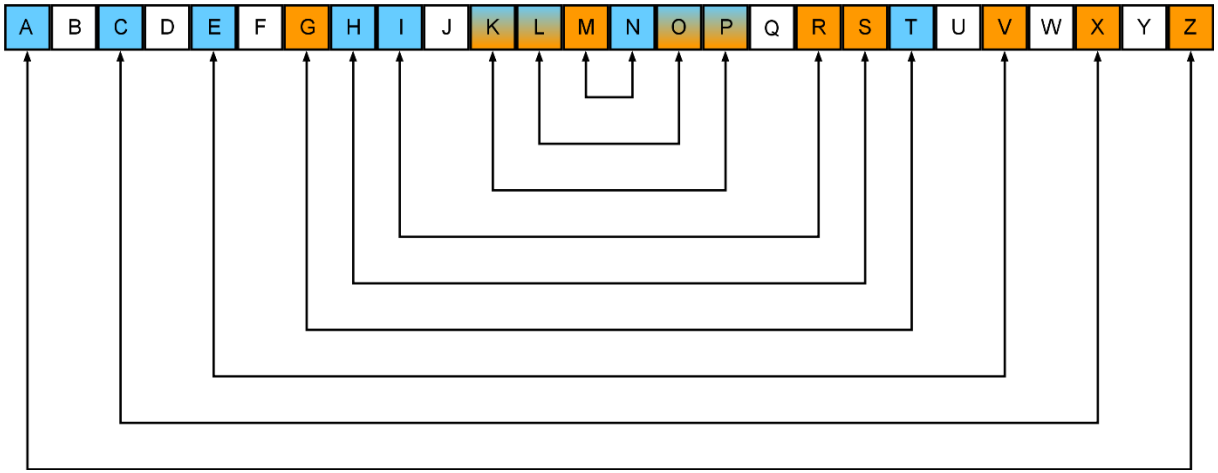
Szyfr AtBash

Działanie szyfru AtBash opiera się na podstawieniu pod każdą literę tekstu jawnego inną leżącą po drugiej stronie alfabetu w takiej samej odległości od końca, jak w tekście jawnym znajduje się od początku.

Przykład

Zaszyfrowanie słowa z wykorzystaniem alfabetu łacińskiego.

Tekst jawny: POLITECHNIKA



Tekst zaszyfrowany: KLORGVXSMRPZ

Szyfrowanie podstawieniowe

Szyfr Vigenere'a

Został stworzony przez Blaise de Vigenere'a w XVI wieku. Tekst jawny szyfrowany jest na podstawie hasła. Jego każda litera szyfrowana jest alfabetem zaczynającym się od znaku, który odpowiada odpowiedniej literze z ustalonego wcześniej hasła.

Przykład

Tekst jawny:	P	O	L	I	T	E	C	H	N	I	K	A
Klucz:	T	A	J	N	E	T	A	J	N	E	T	A
Tekst zaszyfrowany:	I	O	U	V	X	X	C	Q	A	M	D	A

Algorytm odszyfrowujący:

$$K2(i) = [26 - K(i)] \, mod \, 26$$

gdzie:

$K(i) - kolejne\ litery\ słowa\ kluczowego, numerowane\ A = 0, B = 1 \ldots$
$K2(i) - kolejne\ litery\ odwróconego\ klucza$

W wyniku tego klucz „TAJNE" będzie stanowić „HARNW". Następnie należy na tekście zaszyfrowanym wykonać operację szyfrowania z otrzymanym nowym kluczem, w wyniku czego otrzymuje się tekst jawny.

Szyfr Vigenere'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	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
B	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
C	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	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

Szyfrowanie podstawieniowe

Szyfr Playfaira

Został wynaleziony w XIX wieku, podobnie jak szyfr Cezara był stosowany podczas I wojny światowej. Kluczem w szyfrze Playfaira jest losowa macierz o wymiarach 5x5 z i/lub niewystępującą literą J.

Algorytm ten przewiduje szyfrowanie par liter zgodnie z poniższymi zasadami:

- Jeżeli m_1 i m_2 znajdują się w tym samym wierszu, to znakami kryptogramu c_1 i c_2 są litery leżące z prawej strony m_1 i m_2, a pierwsza kolumna stanowi kolumnę położoną na prawo od ostatniej,

- Jeżeli m_1 i m_2 znajdują się w tej samej kolumnie, to znakami kryptogramu c_1 i c_2 są litery leżące poniżej m_1 i m_2, a pierwszy wiersz stanowi wiersz położony pod ostatnim,

- Jeżeli m_1 i m_2 znajdują się w różnych kolumnach i wierszach, to znakami kryptogramu c_1 i c_2 są litery leżące w narożnikach prostokąta wyznaczonego przez m_1 i m_2, a c_1 pochodzi z wiersza posiadającego m_1, zaś c_2 – z wiersza posiadającego m_2,

- Jeżeli $m_1=m_2$, to do tekstu jawnego pomiędzy te litery wstawia się nieznaczącą literę, np. Q. Sytuacja wygląda analogicznie jeśli ostatnia litera nie ma pary, dopisuje się nieznaczącą literę na końcu tekstu jawnego.

Szyfr Playfaira

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

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

Tekst jawny:	PO	LI	TE	CH	NI	KA
Tekst zaszyfrowany:	EQ	GS	RP	SY	GX	FT

Szyfrowanie podstawieniowe

Algorytm XOR

Algorytm XOR nazywany jest również alternatywą wykluczającą lub binarnym sumowaniem. Nie gwarantuje on dość dobrego zabezpieczenia informacji. Zasada działania:

$$0\ XOR\ 0 = 0$$
$$1\ XOR\ 1 = 0$$
$$0\ XOR\ 1 = 1$$
$$1\ XOR\ 0 = 1$$

Zamiana tekstu jawnego na wiadomość binarną.

Zamiana klucza na wiadomość binarną. Poddanie operacji XOR kolejnych bitów binarnego tekstu jawnego z binarnym kluczem.

Przykład

Tekst jawny:	P
Klucz:	J
Tekst jawny binarnie:	01010000
Klucz binarnie:	01001010
XOR:	00011010