Szyfrowanie jest sposobem ochrony informacji przed zinterpretowaniem ich przez osoby niepowołane, lecz nie chroni przed ich odczytaniem lub skasowaniem.

Informacje niezaszyfrowane przechowywane czy przesyłane w systemach informatycznych (sieciach) można traktować jako informacje ujawnione, pomimo użycia innych środków ochrony przed niepowołanym dostępem.

Szyfrowanie to jedyny znany, skuteczny sposób realizacji ochrony informacji przesyłanej w sieci. W szyfrowaniu informacji wykorzystuje się szyfry – tj. rodzinę przekształceń służących do nadawania informacji postaci niezrozumiałej lub bezużytecznej dla napastnika.

Sam proces szyfrowania polega na przekształceniu informacji (jawnej) w inną (tzw. kryptogram lub tekst zaszyfrowany) za pomocą funkcji matematycznej oraz hasła szyfrowania (tzw. klucza). Proces odwrotny, nazywany deszyfrowaniem polega na tym, że kryptogram jest przekształcany z powrotem w oryginalną informację jawną za pomocą pewnej funkcji matematycznej i klucza.

W praktyce zachodzi potrzeba szyfrowania łańcuchów znaków (hasła, dane informacyjne), liczb (dane typu byte, word, integer, longint) oraz rekordów i zbiorów. Rodzaj szyfrowanej informacji, a przede wszystkim sposób jej wykorzystania, wpływa na wybór systemu kryptograficznego (systemu szyfrowania).

Z szyfrowaniem związane są takie pojęcia jak:

- **kryptologia** – nauka o szyfrach;
- **kryptografia** – nauka o konstruowaniu i stosowaniu szyfrów;
- **kryptoanaliza** – nauka o łamaniu szyfrów.

ROT 13

Rot13 jest to prosty szyfr przesuwający (właściwie kodowanie), polegający na zamianie każdego znaku alfabetu łacińskiego na znak występujący 13 pozycji po nim, przy czym wielkość liter nie ma przy przekształcaniu znaczenia.

Najważniejszą cechą kodowania rot13 w porównaniu z innymi szyframi jest to, że sam jest swoją odwrotnością, to znaczy tej samej funkcji używa się do kodowania i dekodowania wiadomości.

Algorytm tenużywany był w grupach dyskusyjnych. Stosowanie jego nie miało jednak zapewnić tajemnicy. Szyfrowane były teksty często niecenzuralne tak, aby odczytywane były przez osoby, które sobie tego życzą. Dodatkowo zaszyfrowany tekst zawierający jakieś zabronione słowa przechodził bez problemu przez wszystkie filtry wyszukujące określonych wyrazów czy też fraz w tekstach. W późniejszym okresie filtry umiały poradzić sobie z tak prostym szyfrem. Przykładowo program Netscape Messenger zawiera funkcję dekodowania wiadomości zaszyfrowanych metodą Rot13.

Tabela 1

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

Szyfr Cezara

Metody podstawieniowe, są najpowszechniej stosowane w kryptografii, polegają za zamianie liter innymi literami. Litery tworzące wiadomość, nie zmieniają swojego miejsca, lecz zmieniają swoje znaczenie.

Jednym z najstarszych szyfrów z rodzaju podstawieniowych jest szyfr Cezara, który polega na zastąpieniu tekstu jawnego literą położną trzy miejsca dalej.

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

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

Dla przykładu zaszyfrujmy słowo informatyka:

I N F O R M A T Y K A

L Q I R U P D W B N D

Szyfrowanie przez przestawianie – metoda płotu

Szyfr przestawieniowy - metoda szyfrowania należąca do grupy klasycznych metod szyfrowania Szyfry te charakteryzują się tym, że w zaszyfrowanym tekście występują wszystkie znaki z tekstu jawnego, ale w innej kolejności, a tak powstałe słowo nazywamy anagramem.

Najprostszym przykładem szyfru przestawieniowego jest pisanie wspak.

S P O D E K -> K E D O P S

My natomiast zajmiemy się inną metodą szyfrowania – **metodą płotu**. Polega ona na tym, aby kolejne litery tekstu jawnego były zapisywane co najmniej w dwóch rzędach, a następnie za kryptogram przyjmujemy ciąg kolejnych liter z kolejnych rzędów począwszy od pierwszego.

SZYFROWANIE

Na początek zaszyfrujmy słowo: *Steganografia* stosując dwa rzędy.

I S E A O R F A

II T G N G A I

Kryptogram: *Seaorfatgngai*

DESZYFRACJA

Znając liczbę rzędów która jest kluczem możemy łatwo odszyfrować informację, dzieląc całkowicie liczbę liter tekstu przez liczbę rzędów, jeżeli zostaje reszta litery te dokładamy do pierwszych rzędów. Następnie odczytujemy litery po kolei w kolumnach.

Mamy odszyfrować kryptogram : *Seaorfatgngai,* znamy klucz, więc dzielimy liczbę liter w teście i wpisujemy w dwa rzędy.

SEAORFA | TGNGAI

I S E A O R F A

II T G N G A I

Zaszyfrowana wiadomość to : *Steganografia.*

W przedstawionej metodzie szyfrowania należy wyróżnić dwa elementy:

- **algorytm szyfrowania**, polegający na ustawieniu kolejnych liter tekstu jawnego w kilku rzędach i zwijaniu kolejno rzędów,
- **klucz**, którym jest liczba rzędów, dzięki niemu ogólny algorytm staje sie procedurą szyfrowania.

Powyżej przedstawiona metoda szyfrowania z użyciem płotu nie jest najlepszym przykładem bezpiecznego klucza szyfrującego, ponieważ możliwych jest w niej niewiele kluczy i bez większego problemu można je szybko sprawdzić.

Oto najpopularniejsze sposoby łamania tego typu szyfru:

- metoda słów prawdopodobnych. Dopasowanie fragmentu znanego (lub odszyfrowanego) tekstu do szyfru pozwala na znalezienie zasady przestawiania,
- wykorzystanie znajomości zasad tworzenia wiadomości - jednakowe szablony dokumentów szyfrowanych, często spotykane zwroty, nagłówki, podpisy czy stopki wiadomości,
- wykorzystuje się też błędy i przyzwyczajenia osób posługujących się tą metodą szyfrowania.

Szyfr monoalfabetyczny ze słowem kluczowym

Szyfrowanie ze słowem kluczowym polega na wybraniu dowolnego słowa kluczowego i wstawieniu go na początek alfabetu szyfrowego oraz kontynuowaniu alfabetu począwszy od litery kończącej słowo kluczowe. Należy pamiętać, aby usunąć powtarzające się litery ze słowa kluczowego.

Przykład szyfrowania:

Słowo kluczowe: *poczta*

Tworzymy alfabet jawny: 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

Tworzymy alfabet szyfrowy: p o c z t a b d e f g h i j k l m n q r s u v w x y

Zaszyfrujmy słowo: *FOLDER*

F O L D E R

A K H Z T N

Otrzymany kryptogram: **A K H Z T N**

Aby odszyfrować wiadomość, odbiorca musi znać słowo kluczowe, a procedura przebiega tak jak przy szyfrowaniu.

Szyfr Playfair

Szyfr ten został wymyślony przez sirCharlesa Wheatstone'aw1854, a spopularyzowany przez baronaLyona Playfaira. Aby móc stosować ten szyfr, nadawca i odbiorca muszą wybrać słowo kluczowe. Załóżmy, że jest to słowo BAJT. Na podstawie słowa kluczowego jest tworzona tabliczka złożona z 25 (5 na 5) pół, służąca do szyfrowania i deszyfrowania wiadomości. Umieszczamy w niej najpierw słowo kluczowe, a następnie pozostałe litery alfabetu łacińskiego (I oraz J zapisujmy w jednym polu i pomijamy znaki diakrytyczne w polskich literach). Tekst jawny przed zaszyfrowaniem dzielimy na pary różnych liter – takie same litery przedzielamy

najczęściej literą *x*, i ostatnią pojedynczą literę również uzupełniamy do pary literą *x*.

B

A

J/I

T

U

V

W

X

Y

Z

C

D

E

F

G

H

K

L

M

N

O

P

Q

R

S

Tekst jawny:**kryptoanaliza** przyjmuje postać:**kr|yp|to|an|al|iz|ax**

Tekst jawny szyfrujemy następująco:

- Jeśli obie litery znajdują się w tej samej kolumnie, to zastępujemy je literami leżącymi bezpośrednio poniżej, gdy jedna z liter znajduje się na końcu kolumny to zastępujemy ją pierwszą literą tej kolumny,
- Jeśli obie litery znajdują się w tym samym wierszy, to zastępujemy je sąsiednimi literami z prawej strony, gdy jedna z liter znajdzie się na końcu wiersza zastępujemy ją pierwsza litera w wierszu,
- Jeśli obie litery nie znajdują się ani w tym samym wierszu, ani w tej samej kolumnie, to bierzemy literę znajdująca się w tym samym wierszu i tej samej kolumnie, w której znajduje się druga litera.

naszego słowa*kryptoanaliza:*

kr | **yp** | **to** | **an** | **al** | **iz** | **ax -**podzielenie testu

mp wr br uk ik ux iw - tekst zaszyfrowany

Deszyfracja przebiega podobnie jak szyfracja:

- Jeśli obie litery znajdują się w tej samej kolumnie, to zastępujemy je literami leżącymi bezpośrednio powyżej,
- Jeśli obie litery znajdują się w tym samym wierszu, to zastępujemy je sąsiednimi literami z lewej strony,
- Jeśli obie litery nie znajdują się ani w tym samym wierszu, ani w tej samej kolumnie, to bierzemy literę znajdująca się w tym samym wierszu i tej samej kolumnie, w której znajduje się druga litera.

Szyfr polialfabetyczny

Kolejną metodą szyfrowania jaką chcemy przedstawić jest szyfr polialfabetyczny.

Taki szyfr uniemożliwia użycie prostej analizy częstości, gdyż w tworzonych kryptogramach za daną literę jest podstawianych wiele różnych liter. Słowo kluczowe w tym przypadku służy do określenia alfabetów – są nimi alfabety Cezara wyznaczone przez kolejne jego litery.

Przykładowo, niech słowem kluczowym będzie *BIT*:

Alfabet jawny: 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

Alfabety szyfrowe: 1 *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

2 *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

3 *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

Utworzyliśmy alfabety szyfrowe zaczynając od liter B, I, T. następnie zaszyfrujmy słowo:*INFOR MATYKA*
. Pierwszą literę jawnego tekstu szyfrujemy posługując się pierwszym alfabetem szyfrowym, drugą drugim, trzecią trzecim, czwartą pierwszym itd.

1 2 3 1 2 3 1 2 3 1 2

I N F O R M A T Y K A

J VY P Z F B B R L I

Otrzymujemy kryptogram ***J V Y P Z F B B R L I,*** w którym każda z powtarzających się liter w tekście jawnym jest za każdym razem szyfrowana przez inna literę.

Deszyfracje przeprowadzamy w sposób odwrotny do szyfracji, a kluczem jest słowo BIT (w tym przypadku).