|  |  |  |  |
| --- | --- | --- | --- |
| ***KOLEGIUM KARKONOWSKIE***  ***WYDZIAŁ TECHNICZNY*** | | | |
| ***KODOWANIE I KRYPTOGRAFIA W TELEKOMUNIKACJI LABORATORIUM*** | | | |
| *Numer grupy: 4* | *Prowadzący: mgr inż. Andrzej Rehlis* | | |
| *Wykonał:* | *Temat ćwiczenia:*  *Szyfr Vigenere’a* | | |
| *Data wykonania:*  *29.04.2009 r.* | *Ocena:* | *Podpis:* |

1. **Wstęp**

**Algorytm Vigenère'a** jest jednym z klasycznych algorytmów szyfrujących. Należy on do grupy tzw. wieloalfabetowych szyfrów podstawieniowych. Szyfr ten błędnie został przypisany twórcy bardziej skomplikowanego szyfru Blaise'owi de Vigenère.

Szyfr, który obecnie nazywamy szyfrem Vigenère'a po raz pierwszy został opisany przez Giovana Batista Belaso w 1553 w broszurze zatytułowanej *La cifra del. Sig. Giovan Batista Belaso*

Działanie szyfru Vigenere’a oparte jest na następującej tablicy:

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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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

Jak można zauważyć, każdy z wierszy tablicy odpowiada szyfrowi Cezara, przy czym w pierwszym wierszu przesunięcie wynosi 0, w drugim 1 itd.

Aby zaszyfrować pewien tekst, potrzebne jest słowo kluczowe. Słowo kluczowe jest tajne i mówi, z którego wiersza (lub kolumny) należy w danym momencie skorzystać.

Przypuśćmy, że chcemy zaszyfrować prosty tekst, np.:

TO JEST BARDZO TAJNY TEKST

Do tego celu użyjemy znanego tylko nam słowa kluczowego, np. TAJNE

Na początku zauważamy, że użyte słowo kluczowe jest zbyt krótkie, by wystarczyło do zaszyfrowania całego tekstu, więc należy użyć jego wielokrotności. Będzie to miało następującą postać:

TO JEST BARDZO TAJNY TEKST

TA JNET AJNETA JNETA JNETA

Następnie wykonujemy szyfrowanie w następujący sposób: litera szyfrogramu odpowiada literze z tabeli znajdującej się na przecięciu wiersza, wyznaczanego przez literę tekstu jawnego i kolumny wyznaczanej przez literę słowa kluczowego, np. po kolei T i T daje M, O i A daje O itd. W efekcie otrzymujemy zaszyfrowany tekst:

MO SRWM BJEHSO CNNGY CROLT

Warto zauważyć, że tak naprawdę nie ma znaczenia, czy litera tekstu jawnego będzie wyznaczała wiersz, a słowa kluczowego kolumnę, czy na odwrót, efekt szyfrowania będzie zawsze taki sam.

Odszyfrowywanie przebiega bardzo podobnie. Bierzemy kolejne litery szyfrogramu oraz odpowiadające im litery słowa kluczowego (podobnie, jak przy szyfrowaniu). Wybieramy kolumnę odpowiadającą literze słowa kluczowego. Następnie w tej kolumnie szukamy litery szyfrogramu. Numer wiersza odpowiadający znalezionej literze jest numerem litery tekstu jawnego. Np. w kolumnie T litera M znajduje się w wierszu T, w kolumnie A litera O znajduje się w wierszu O itd.

Istnieje jednakże prostszy, szczególnie dla celów implementacyjnych, sposób deszyfrowania. Wymaga on wykonania prostej operacji "odwrócenia" hasła, jak poniżej:

K2(i) = [26 – K(i)] mod 26

gdzie K(i) – kolejne litery słowa kluczowego, numerowane A=0, B=1 itd., a K2(i) – kolejne litery hasła "odwróconego". 26 oznacza liczbę liter alfabetu łacińskiego.

Efektem działania takiego przekształcenia dla hasła "TAJNE" będzie słowo "HARNW".

Następnie należy na szyfrogramie wykonać operację szyfrowania z otrzymanym hasłem. Wynikiem, jak można się przekonać, będzie postać jawna tekstu.

### Kryptoanaliza

Oba szyfry były często mylone i określane terminem "le chiffre indéchiffrable" (nierozszyfrowalny szyfr).

Pierwszy opis złamania szyfru Vigenère'a, został opublikowany w książce pruskiego dowódcy Fryderyka Kasiskiego - 'Die Geheimschriften und die Dechif-frir-kunst' (Szyfrogramy i sztuka deszyfracji) opublikowanej w 1863.

Metoda złamania opierała się na obserwacji, że powtórzenia w szyfrogramie mogą odpowiadać powtórzeniom w tekście jawnym i kluczu. To z kolei ułatwiało odgadnięcie długości klucza, następnie samego klucza i odszyfrowania szyfrogramu.

Oczywiście metoda ta dotyczyła historycznej wersji szyfru Vigenère'a, która miała skończoną (i w praktyce zazwyczaj krótką) długość klucza.

Pierwsze złamanie szyfru nastąpiło jednak wcześniej w roku 1854 przy użyciu kryptoanalizy statystycznej i zostało dokonane przez Charles'a Babbage'a. Istotą złamania szyfru było podzielenie wiadomości na części w ilości równej długości klucza. W wyniku podziału otrzymywano urywki wiadomości, które można było traktować jak zaszyfrowane szyfrem monoalfabetycznym.

Charles Babbage prawdopodobnie złamał również szyfr Vigenère'a z autokluczem.

### Bezwarunkowe bezpieczeństwo

Szyfr Vigenère'a może być szyfrem nie do złamania (zostało to udowodnione w 1949 przez Claude'a Elwood'a Shannon'a) przy zachowaniu trzech reguł:

* klucz użyty do szyfrowania wiadomości był dłuższy lub równy szyfrowanej wiadomości,
* klucz musi być wygenerowany w sposób całkowicie losowy (nie może istnieć sposób na odtworzenie klucza na podstawie znajomości działania generatorów liczb pseudolosowych),
* klucz nie może być użyty do zaszyfrowania więcej niż jednej wiadomości.

1. **Kod źródłowy programu**

Program VIGENERE;

uses Crt;

var

LST, LKL, i, j, k: integer;

ST, KL, SZYFR: string;

AA: array[32..127,32..127] of integer;

BT, BK: array[1..256] of byte;

begin

ClrScr;

gotoXY(10,4);

write('Podaj tekst do zasyfrowania: ');

read(ST);

readln;

gotoXY(10,6);

write('Podaj tekst klucza (do 20 znakow): ');

read(KL);

LST:=length(ST);

LKL:=length(KL);

for i:=32 to 127 do

for j:=32 to 127 do

begin

AA[i,j]:=i+j-32;

if AA[i,j]>127 then AA[i,j]:=AA[i,j] mod 127;

end;

for i:=1 to LST do BT[i]:=ord(ST[i]);

for i:=1 to LST do

begin

k:=i mod LKL;

if k=0 then k:=LKL;

BK[i]:=ord(KL[k]);

end;

SZYFR:='';

for i:=1 to LST do

begin

SZYFR:=SZYFR+chr(AA[BT[i],BK[i]]);

end;

gotoXY(10,8);

write('Tekst zaszyfrowany ma postac: ');

for j:=1 to LST do

begin

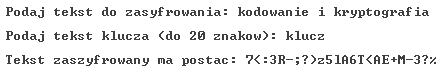
write(SZYFR[j]);

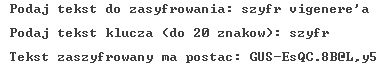
end;

repeat until keypressed;

end.

1. **Wynik działania programu**





1. **Wnioski**

Na zajęciach laboratoryjnych napisaliśmy program do szyfrowania informacji za pomocą szyfru Vigenere’a. Program ten wykorzystywał kod ASCII od znaku 32 (spacja) do znaku 126 (tylda). Działanie programu polegało na podaniu tekstu do zaszyfrowania oraz klucza, a program generował gotowy już zaszyfrowany tekst.