

**Akademia Techniczno-Humanistyczna**

**w Bielsku-Białej**

Wydział Budowy Maszyn i Informatyki

**Bezpieczeństwo technologii informatycznych**

**(ćwiczenia laboratoryjne)**

**Ćwiczenie numer:**

**2**

**Czas realizacji zajęć:** 135 min.

**Temat ćwiczenia:**

**Szyfr Vigenère'a**

**1. Wstęp teoretyczny.**

**Szyfr Vigenère'a**

Algorytm Vigenère'a (IPA [viʒˈnɛːʁ]) jest jednym z klasycznych algorytmów szyfrujących. Należy on do grupy tzw. polialfabetycznych 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.

**Historyczny szyfr Vigenère'a**

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](https://pl.wikipedia.org/wiki/Szyfr_Cezara" \o "Szyfr 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](https://pl.wikipedia.org/wiki/Szyfrogram_(kryptografia)" \o "Szyfrogram (kryptografia)) wykonać operację szyfrowania z otrzymanym hasłem. Wynikiem, jak można się przekonać, będzie postać jawna tekstu.

**Oryginalny szyfr Vigenère'a**

Oryginalny szyfr Vigenère'a używał autoklucza, pierwsza litera klucza była ustalana, a kolejnymi literami były kolejne litery tekstu jawnego.

Niech naszą literą szyfrującą, będzie N

tekst jawny: TO JEST BARDZO TAJNY TEKST

klucz: NT OJES TBARDZ OTAJN YTEKS

tekst zaszyfrowany: GH XNWL UBRUCN HTJWL RXOCL

Odszyfrowanie przebiega w następujący sposób, pierwszą literę szyfrogramu, odszyfrowywujemy ustaloną literą (N), kolejne litery, dopiero co odszyfrowanymi literami:

G N → **T**  
H **T** → **O**  
X **O** → J

...

szyfrogram: G H X N W L ...

klucz: N T O J E S ...

tekst odszyfrowany: T O J E S T ...

Szyfr ten ze względu na to, że długość klucza była równa długości tekstu jawnego, opierał się analizie statystycznej

**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.

**2. Plan wykonania ćwiczenia.**

1. Napisz program, który szyfruje tekst zgodnie z algorytmem szyfru Vigenère'a.
2. Napisz program, który odszyfrowuje tekst zgodnie z algorytmem szyfru Vigenère'a.
3. Napisz sprawozdanie.