www.ekspres.ubb.edu.pl

Szyfr Vigenère'a

mgr inż. Daniel Jancarczyk
Wydział Budowy Maszyn i Informatyki

Uniwersytet Bielsko-Bialski

Algorytm Vigenère'a

Algorytm Vigenère'a 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.

Algorytm 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

Algorytm Vigenère'a

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.

Algorytm Vigenère'a

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:

Algorytm Vigenère'a

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 li**terę tekstu jawnego** i kolumny wyznaczanej przez **literę słowa kluczowego**, np. po kolei **T i T** daje **M**, **O i A** daje **O** itd.

Algorytm Vigenère'a

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.

Algorytm Vigenère'a

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.

Algorytm Vigenère'a

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.

Algorytm Vigenère'a

Implementacja programowa:

```
def generateKey(string, key):
    key = list(key)
    if len(string) == len(key):
        return (key)
    else:
        for i in range(len(string) -
                       len(key)):
            key.append(key[i % len(key)])
    return ("".join(key))

def cipherText(string, key):
    cipher_text = []
    for i in range(len(string)):
        x = (ord(string[i]) +
             ord(key[i])) % 26
        x += ord('A')
        cipher_text.append(chr(x))
    return ("".join(cipher_text))

string = "Wiadomosc zostanie zaszyfrowana"
keyword = "jablko"
key = generateKey(string, keyword)
cipher_text = cipherText(string, key)
print("Ciphertext :", cipher_text)
```

Wynik szyfrowania:

```
Ciphertext : LUNAKMJEPKVONFNKEEILNPVYADBTWNV

Process finished with exit code 0
```