

Ministry of Education, Culture and Research of the Republic of Moldova

Technical University of Moldova

Department of Software and Automation Engineering

**REPORT**

Laboratory work No. 3

**Discipline**: Cryptography and Security

Elaborated: Macrii Danu FAF-222,

Checked: asist. univ. Dumitru Nirca,

Chișinău 2023

## Topic: Mono-alphabetic Cipher

## Tasks:

De implementat algoritmul Vigenere în unul din limbajele de programare

pentru mesaje în limba română (31 de litere), acestea fiind codificate cu numerele 0, 1, ... 30.

Valorile caracterelor textului sunt cuprinse între ‘A’ și ’Z’, ’a’ și ’z’ și nu sunt premise alte

valori. În cazul în care utilizatorul introduce alte valori - i se va sugera diapazonul corect al

caracterelor. Lungimea cheii nu trebuie să fie mai mică de 7. Criptarea și decriptarea se va

realiza în conformitate cu formulele din modelul matematic prezentat mai sus. În mesaj mai

întâi trebuie eliminate spațiile, apoi toate literele se vor transforma în majuscule. Utilizatorul

va putea alege operația - criptare sau decriptare, va putea introduce cheia, mesajul sau

criptograma și va obține criptograma sau mesajul decriptat.

## Theoretical notes:

Metoda de criptare cunoscută sub numele de „cifrul Vigenère” a fost atribuită greșit lui

Blaise de Vigenère în secolul al XIX-lea și, de fapt, a fost descrisă pentru prima dată de Giovan

Battista Bellaso în cartea sa din 1553 La cifra del. Sig. Vigenère a creat un cifru asemănător, dar

totuși diferit și mai puternic în 1586.

Pe da altă parte, cifrul Vigenere folosește aceleași operații ca și cifrul Cezar. Cifrul

Vigenere și fel deplasează literele, dar, spre deosebire de Cezar, nu se poate sparge ușor în 26

combinații. Cifrul Vigenere folosește o deplasare multiplă. Cheia nu este constituită de o singură

deplasare, ci de mai multe, fiind generate de câțiva întregi ki, unde 0 ≤ ki ≤ 25, dacă luăm ca reper

alfabetul latin cu 26 de litere. Criptarea se face în felul următor:

ci = (mi + ki) mod 26.

Cheia poate fi, de exemplu, k = (5, 20, 17, 10, 20, 13) și ar provoca deplasarea primei litere

cu 5, c1=m1 + 5 (mod 26), a celei de a doua cu 20, c2 = m2 + 20 (mod 26), ș.a.m.d. până la sfârșitul

cheii și apoi de la început, din nou. Cheia este de obicei un cuvânt, pentru a fi mai ușor de memorat

– cheia de mai sus corespunde cuvântului „furtun”. Metoda cu deplasare multiplă oferă protecție

suplimentară din două motive:

• primul motiv este că ceilalți nu cunosc lungimea cheii;

• cel de al doilea motiv este că numărul de soluții posibile crește odată cu mărimea cheii;

de exemplu, pentru lungimea cheii egală cu 5, numărul de combinații care ar fi

necesare la căutarea exhaustivă ar fi 265 = 11 881 376.

Decriptarea pentru cifrul Vigenere este asemănătoare criptării. Diferența constă în faptul

că se scade cheia din textul cifrat,

mi = (ci – ki) mod 26.

Pentru simplificarea procesului de cifrare se poate utiliza următorul tabel, numit Tabula

Recta (tabelul 3.1), care se utiliza de către Vigenere. Aici toate cele 26 cifruri sunt situate pe

orizontală și fiecărui cifru îi corespunde o anumită literă din cheie, reprezentată în colana din

stânga tabelului. Alfabetul corespunzător literelor textului clar se află în prima linie de sus a

tabelului. Procesul de cifrare este simplu – este necesar ca având litera mi din mesaj și litera ki din1cheie să găsim litera textului cifrat ci, care se află la intersecția liniei mi și coloanei ki. În exemplul

din tabelul 3.1 este prezentat cazul mi = M și ki = H, iar în rezultat se obține ci = T.

**Implementation(Var. Nr.12)**

De implementat algoritmul Vigenere în unul din limbajele de programare

pentru mesaje în limba română (31 de litere), acestea fiind codificate cu numerele 0, 1, ... 30.

Valorile caracterelor textului sunt cuprinse între ‘A’ și ’Z’, ’a’ și ’z’ și nu sunt premise alte

valori. În cazul în care utilizatorul introduce alte valori - i se va sugera diapazonul corect al

caracterelor. Lungimea cheii nu trebuie să fie mai mică de 7. Criptarea și decriptarea se va

realiza în conformitate cu formulele din modelul matematic prezentat mai sus. În mesaj mai

întâi trebuie eliminate spațiile, apoi toate literele se vor transforma în majuscule. Utilizatorul

va putea alege operația - criptare sau decriptare, va putea introduce cheia, mesajul sau

criptograma și va obține criptograma sau mesajul decriptat.

def encrypt\_vigenere(msg, key):

encrypted\_text = []

key = generate\_key(msg, key)

for i in range(len(msg)):

char = msg[i]

if char.isupper():

encrypted\_char = chr((ord(char) + ord(key[i]) - 2 \* ord('A')) % 26 + ord('A'))

elif char.islower():

encrypted\_char = chr((ord(char) + ord(key[i]) - 2 \* ord('a')) % 26 + ord('a'))

else:

encrypted\_char = char

encrypted\_text.append(encrypted\_char)

return "".join(encrypted\_text)

def decrypt\_vigenere(msg, key):

decrypted\_text = []

key = generate\_key(msg, key)

for i in range(len(msg)):

char = msg[i]

if char.isupper():

decrypted\_char = chr((ord(char) - ord(key[i]) + 26) % 26 + ord('A'))

elif char.islower():

decrypted\_char = chr((ord(char) - ord(key[i]) + 26) % 26 + ord('a'))

else:

decrypted\_char = char

decrypted\_text.append(decrypted\_char)

return "".join(decrypted\_text)