

Nr. 3. Criptare Vigenere

Criptarea este un proces de mascare a unei informații pentru a o face ilizibilă pentru utilizatorii neautorizați. Una dintre cele mai simple metode de criptare este criptarea Vigenere. Fie M mesajul (textul) în clar ce urmează a fi secretizat și C mesajul cifrat, secretizat. Realizați un program care să creeze un mesaj M , folosind cifrul de codare Vigenere (Vezi figura 1). Procedul de criptare presupune stabilirea unui cuvânt de cod secret S , citit de la tastatură, și repetarea acestuia, caracter cu caracter până când se ajunge la lungimea mesajului în clar M . Pentru a cripta o literă, se parcurge textul M , caracter cu caracter, și se selectează, pe rând litera din textul în clar M și litera din codul secret S de la indexul curent, și se caută celula din matricea Vigenere, la care se intersectează coloana corespunzătoare literei din codul secret S și linia corespunzătoare literei din mesajul în clar M , obținând astfel litera codată. Să se afișeze mesajul cifrat C obținut în consolă.

	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
A	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Figura 1. Matricea cifrului Vigenere

Să se realizeze în limbajul C următoarele:

1. O funcție care determină și returnează dimensiunea unui șir de caractere;
2. O funcție care creează un șir de caractere $S1$, format prin repetarea unui alt șir de caractere $S2$, caracter cu caracter, până se ajunge la o lungime k , transmisă ca argument;
3. O funcție care codează un șir de caractere folosind procedeul de criptare Vigenere;
4. O funcție ce integrează funcțiile realizate anterior pentru a rezolva problema enunțată. Aceasta va primi datele de intrare și va returna rezultatele conform cerințelor de mai jos.

Date de intrare:

Se va citi de la tastatură:

- o matrice de caractere de dimensiune 26×26 ;
- o valoare întreagă cuprinsă în intervalul **[1,5]**, în funcție de care se vor apela diferitele funcții prezentate anterior, astfel:

Pentru fiecare caz în parte, se vor citi suplimentar de la tastatură:

1. două șiruri de caractere astfel: un șir de caractere corespunzător textului în clar M , și un șir de caractere corespunzător codului secret S . Se testează cazul prin afișarea pe ecran a șirului de caractere M , urmat de o linie nouă (*newline*), și a șirului de caractere S ;
2. un șir de caractere corespunzător codului secret S , și o valoare întreagă k . Se testează funcția de creare a unui șir de caractere $S2$, format prin repetarea șirului de caractere S , până când $S2$ ajunge la lungimea k . Se va afișa în consolă șirul obținut.
3. un șir de caractere arbitrar. Se va testa funcția de determinare a lungimii unui șir de caractere, Se va returna și afișa în consolă lungimea șirului citit de la tastatură;
4. două șiruri de caractere astfel: un șir de caractere corespunzător textului în clar M , și un șir de caractere corespunzător codului secret S . Se testează funcția de codare a unui șir de caractere folosind procedeul de criptare Vigenere prin afișarea rezultatului criptării în consolă;
5. testare program complet. Se repetă șirul S până se ajunge la dimensiunea k a șirului M , unde k este lungimea șirului M , se codează șirul de caractere M folosind procedeul de criptare Vigenere, și se afișează în consolă șirul codat C obținut.

Restricții și precizări:

1. Un șir de caractere se termină întotdeauna cu caracterul **nul** ('0');
2. Rutinele de intare pentru șiruri de caractere nu pot citi corect caractere care conțin spații sau linii noi. Astfel, se va lua în vedere eliminarea fiecărui spațiu sau linie nouă introdusă între citirile succesive ale unor caractere sau șiruri de caractere.

Exemplu:

Intrare:	Ieșire:
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	

Explicație:
Se citește de la tastatură o matrice de caractere de dimensiune 26 × 26.

Pentru fiecare caz în parte:

1.

Intrare: 1 CRIPTOGRAFIE CHEIE	leșire: CRIPTOGRAFIE CHEIE
--	---

Explicație:
Se citește de la tastatură șirul de caractere corespunzător mesajului în clar M , și respectiv, codului secret S , separate de o linie nouă (*newline*).
Comanda **1** corespunde afișării celor două șiruri în consolă.

2.

Intrare: 2 CHEIE 12	leșire: CHEIECHEIECH
--	--------------------------------

Explicație:
Se citește de la tastatură șirul de caractere corespunzător codului secret S , respectiv valoarea lui k , separate de o linie nouă (*newline*).
Comanda **2** corespunde funcției de creare a unui șir de caractere, format prin repetarea unui alt șir de caractere până se ajunge la lungimea k a șirului M . Se va afișa în consolă șirul obținut.

3.

Intrare: 3 TEST	leșire: 4
-------------------------------------	---------------------

Explicație:
Se citește de la tastatură șirul de caractere corespunzător mesajului în clar M , urmat de o linie nouă (*newline*).
Comanda **3** corespunde funcției de determinare a lungimii unui șir de caractere arbitrar. Se va afișa în consolă lungimea determinată.

4.

Intrare: 4 CRIPTOGRAF PAROLAPARO	leșire: RRZDEOVRT
---	-----------------------------

Explicație:

Se citesc de la tastatură șirul de caractere corespunzător mesajului în clar M , și respectiv, codului secret S repetat, până s-a ajuns la dimensiunea șirului M separate de o linie nouă (*newline*).

Comanda **3** corespunde funcției de codare a unui șir de caractere folosind procedeul de criptare Vigenere.

5.

Intrare:

5

CRIPTOGRAFIE

CHEIE

Ieșire:

EYMXXQNV IJKL

Explicație:

Se citesc de la tastatură șirul de caractere corespunzător mesajului în clar M , și respectiv, codului secret S , separate de o linie nouă (*newline*).

Comanda **5** corespunde rulării întregului program. Se repetă șirul S până se ajunge la dimensiunea k a șirului M , unde k este lungimea șirului M , se codează șirul de caractere M folosind procedeul de criptare Vigenere, și se afișează în consolă șirul codat C obținut.