

Ministerul Educatiei, Culturii și Cercetarii al Republicii Moldova Universitatea Tehnic**ă** a Moldovei

Facultatea Calculatoare, Informatic**ă ş**i Microelectronic**ă** Departamentul Ingineria Software și Automatica

# Raport

pentru lucrarea de laborator Nr. 1

la cursul „Metode criptografice de protecție a informației”

A efectuat:Ceban Andrei, gr. FAF-211

A verificat: Cǎtǎlin MÎŢU

Chișinău – 2023

**Subiectul:** Cifrul lui Cesar

## Sarcini:

1. De implementat algoritmul Cezar pentru alfabetul limbii engleze în unul din limbajele de programare. Utilizați doar codificarea literelor cum este arătat în tabelul 1 (nu se permite de folosit codificările specificate în limbajul de programare, de ex. ASCII sau

Unicode). Valorile cheii vor fi cuprinse între 1

și 25 inclusiv

și nu se permit alte valori.

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.

Înainte de criptare textul va fi transformat în majuscule și vor fi eliminate spațiile.

Utilizatorul va putea alege operația - criptare sau decriptare, va putea introduce cheia, mesajul sau criptograma și va obține respectiv criptograma sau mesajul decriptat.

1. De implementat algoritmul Cezar cu 2 chei, cu păstrarea condițiilor exprimate în

Sarcina 1. În plus, cheia 2 trebuie să conțină doar litere ale alfabetului latin, lungime nu mai mică de 7.

și să aibă o

## Cifrul lui Cesar

În acest cifru fiecare literă a textului clar este înlocuită cu o nouă literă obţinută printr-o

deplasare alfabetică. Cheia secretă

k, care este aceeaşi la criptare cât

şi la decriptare,

constă în numărul care indică deplasarea alfabetică, adică k∈{1, 2, 3,…, n–1}, unde n este lungimea alfabetului. Criptarea **ş**i decriptarea mesajului cu cifrul Cezar poate fi definit**ă** de formulele

c = ek(x) = x + k (mod n), m = dk(y) = y – k (mod n),

unde x

și y sunt reprezentarea numerică

a caracterului respectiv al textului clar. Funcţia

numită *Modulo* (a mod b) returnează restul împărţirii numărului întreg a la numărul întreg

b. De exemplu, pentru k = 3 avem (fig 1):

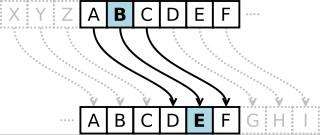


Figura 1 – Exemplu de deplasare alfabetica

Pentru a spori criptorezistența cifrului Cezar se poate de aplicat o permutare a alfabetului prin aplicarea unui cuvânt-cheie (a nu se confunda cu cheia de bază a cifrului). Această cheie poate fi orice consecutivitate de litere a alfabetului - fie un cuvânt din vocabular, fie unul fără sens.

Fie cheia a doua este k2 =cryptography. Aplicăm această cheie asupra alfabetului 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

și obținem:

C R Y P T O G A H B D E F I J K M L N Q S U V W X Z

Această

ordine nouă

am obținut-o prin plasarea literelor lui k2 la început, apoi urmează

celelalte litere ale alfabetului în ordinea lor naturală. Vom ține cont de faptul că literele nu se vor repeta, adică dacă litera se întâlnește de câteva ori, ea se plasează doar o singură dată.

## Rezultatul efectuarii sarcinilor:

Initial, dacă utilizatorul nu introduce nici un argument, va fi afisat mesajul cu instrucțiuni (figura 2).



Figura 2 – Mesajul informational

Pentru a cripta un mesaj se introduce acțiunea „1”, mesajul, cheia de deplasare și optional cheia secundara. Un exemplu de criptare cu o cheie este afisat în figura 3.

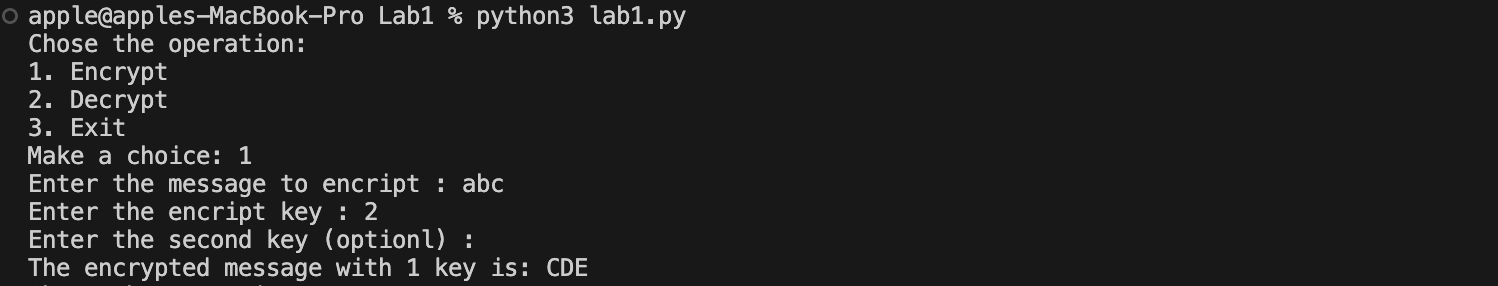


Figura 3 – Criptarea mesajului cu o cheie Un exemplu de criptare cu doua chei este afisat în figura 4.



Figura 4 – Criptarea mesajului cu doua chei

Pentru a decripta un mesaj, e nevoie de introdus acțiunea „2”, mesajul și cheia de

decriptare și la necesitate cheia secundara. Un exemplu de decriptare cu o cheie este afisat în figura 5.



Figura 5 – Decriptarea cu o cheie

Un exemplu de decriptare cu doua chei este afisat în figura 6.

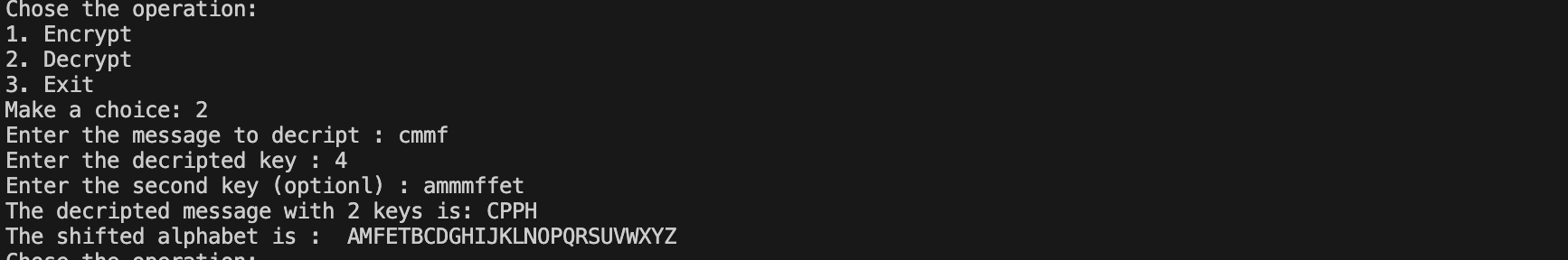


Figura 6 – Decriptarea cu doua chei

**Concluzie:** În cadrul acestei activități de laborator, am înțeles modul de funcționare a algoritmului de criptare Cezar. Am dezvoltat o aplicație care folosește cifrul Cezar cu una sau două chei pentru a encripta și decripta mesaje. Deși varianta cu două chei poate părea mai complexă la prima vedere, aceasta contribuie semnificativ la sporirea securității cifrului în comparație cu varianta cu o singură cheie. Dacă am folosi o metodă exhaustivă pentru a încerca să decriptăm mesajul, ar trebui să evaluăm 26! \* 25 opțiuni, ceea ce este extrem de dificil și consumator de timp.

Git-link : https://github.com/andeiceban0352/Criptography-Labs/tree/main/Lab1