Laborator 1

- ✓ Terminologie
- ✓ Sistemul de cifrare Cezar
- ✓ Sistemul de cifrare Vigenère

1. Terminologie

Text (în) clar (engl. Plain Text)	Mesajul inițial, înainte de a fi criptat
Criptare (cifrare)	Transformarea textului clar într-un text neinteligibil
Text criptat (text cifrat, criptograma) (engl. Ciphertex)	Versiunea criptată a mesajului inițial (rezultatul operației de criptare)
Decriptare	Procesul de transformare a criptogramei îm textul original
Cifru	Pereche de algoritmi care efectuează criptarea și decriptarea
Cheie	Informaţie secretă utilizată de un cifru, cunoscută doar de expeditor şi de destinatar.
Criptografie	Ştiinţa criptării şi decriptării mesajelor cu cheie sau sistem de criptare cunoscute.
Criptanaliză	Ştiinţa decriptării mesajelor fără a cunoaşte cheia sau algoritmul de criptare folosit.
Criptare prin substituţie	Metodă de criptare în care fiecare caracter sau grup de caractere din textul clar este înlocuit cu un alt caracter sau grup de caractere.
Criptare prin transpoziţie	Metodă de criptare în care litere sunt reordonate (amestecate).
Substituţie monoalfabetică	Metodă de criptare prin care o literă din mesajul inițial este întotdeauna înlocuită de o aceeaşi literă în mesajul criptat.
Substituţie polialfabetică	Metodă de criptare prin care o literă din mesajul inițial nu este întotdeauna înlocuită de aceeaşi literă în mesajul criptat.

2. Sistemul de cifrare Cezar

2.1.Breviar teoretic

Algoritmul de cifrare al lui Cezar (cifrul lui Cezar, codul lui Cezar) este unul dintre cei mai simpli și mai cunoscuți algoritmi de criptare Textul clar este construit din literele alfabetului latin *A-Z*. Cheia de cifrare este reprezentată de un număr întreg $k \in \{0, \ldots, 25\}$.

În faza de preprocesare, delimitatorul de spațiu este ignorat sau înlocuit cu caracterul cel mai puțin frecvent din limba în care este textul clar (în limba română Q).

Cifrul lui Cezar înlocuiește fiecare literă din textul inițial cu litera aflată la distanța *k* (litera obținută prin permutarea circulară a alfabetului cu k poziții).

Exemplu:
Să se cifreze mesajul:

CRIPTOGRAFIE

utilizând cifrul lui Cezar cu cheia de cifrare k = 7.

Alfabetul va fi permutat ciclic cu 7 poziții:

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
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

Literei C îi corespunde litera J, literei R îi corespunde Y, etc. Textul criptat este:

JYPWAVNYHMPL

Pentru decriptare permutarea alfabetului se realizează invers.

Această metodă de criptare poate fi reprezentată utilizând aritmetica modulară. Fiecarei litere din textul sursă i se asociază ordinea lexicografică *x* (pentru litera A, $x = 0$). Pentru cifrare, aceasta se înlocuiește prin caracterul care are poziția $(x + k) \bmod 26$.

În exemplu de mai sus:

- literei C îi corespunde $x = 2$, deci se va cifra în $(2 + 7) \bmod 26 = 9$ adică J
- literei R îi corespunde $x = 17$, deci se va cifra în $(17 + 7) \bmod 26 = 24$, adică Y
- literei T îi corespunde $x = 19$, deci se va cifra în $(19 + 7) \bmod 26 = 0$, adică A

Se continuă în mod analog pentru fiecare literă și se obține JYPWAVNYHMPL.

Pentru descifrare se utilizează regula inversă: $(x- k) \bmod 26$.

2.2.Exerciții propuse

1. Să se cifreze mesajul:
   CALCULATOR
   utilizând cifrul lui Cezar cu cheia de cifrare k = 9.
2. Să se cifreze mesajul:
   DIGITAL SIGNATURE
   utilizând cifrul lui Cezar cu cheia de cifrare k = 3.
3. Să se decripteze mesajul:
   WIGYVMXEXIMR JSVQEXMSREPE
   utilizând cifrul lui Cezar. Indicați cheia de cifrare.
4. Să se decripteze mesajul:
   YZKBKPUHY
   utilizând cifrul lui Cezar. Indicați cheia de cifrare.

5. Scrieți o aplicație care să implementeze următoarele funcții:
   - cifrarea unui text cu ajutorul algoritmului de cifrare Cezar
   - decriptarea unui text cifrat cu algoritmul lui Cezar

   Funcțiile vor avea doi parametri: textul clar / textul criptat și cheia de cifrare.

3. Sistemul de cifrare Vigenère

3.1.Breviar teoretic

Acest cifru este o generalizare a cifrului Cezar. Se consideră, ca și la sistemele anterioare, cele 26 litere ale alfabetului, numerotate de la 0 (pentru A) până la 25 (pentru 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	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

O cheie k este un cuvânt având codificarea numerică $k_0k_1 \ldots k_{p-1}$.
Dacă textul clar t are codificarea $t = t_0t_1 \ldots t_n$ atunci textul criptat c va fi:
$c = c_0c_1 \ldots c_n$, unde
$c_i = (t_i + k_{i \pmod p}) \bmod 26$

Exemplu:
Să se cripteze textul clar NU POT VENI AZI utilizând cheia FOCAR.

Deci p = 5 și codificarea numerică a cheii este k = 5 14 2 0 17.
Codificarea textului clar este t = 13 20 15 14 19 21 4 13 8 0 25 8.

Sub fiecare număr din t se așează câte un număr din k; când cheia se termină, se reia ciclic, până se termină t.

N	U	P	O	T	V	E	N	I	A	Z	I
13	20	15	14	19	21	4	13	8	0	25	8
5	14	2	0	17	5	14	2	0	17	5	14
18	8	17	14	10	0	18	15	8	17	4	22
S	I	R	O	K	A	S	P	I	R	E	W

Linia a patra conține suma modulo 26 a numerelor de pe primele două linii.
Ultima linie conține textul criptat rezultat: SIROKASPIREW

Decriptarea se realizează similar, scăzând (modulo 26) din codul caracterului criptat, codul caracterului corespunzător din cheie.

3.2. Exerciţii propuse

6. Să se cifreze mesajul:
   CRIPTOGRAFIE
   utilizând cifrul lui Vigenère cu parola TEST.

7. Să se cifreze mesajul:
   THE ART OF PROGRAMMING
   utilizând algoritmul lui Vigenère și parola PYTHON.

8. Să se decripteze mesajul:
   PCWKPOVVIEMFPSOWROVABWTDI
   utilizând algoritmul lui Vigenère și parola PASSWORD.

9. Să se decripteze mesajul:
   WRKADIXNBKUNJBZSMTMBVGXA
   algoritmul lui Vigenère și parola ENIGMA.

10. Scrieți o aplicație care să implementeze următoarele funcții:
    - criptarea unui text cu ajutorul algoritmului lui Vigenère
    - decriptarea unui text cifrat cu algoritmul lui Vigenère

    Funcțiile au ca parametri textul clar / textul criptat și parola.