CURS 2
CIFRURI CLASICE

1. Cifrul lui Cezar

- Textul clar este format din literele mari ale alfabetului latin.
- Cheia secretă comună este un număr natural $k \in \{0,1, \dots ,25\}$.
- O cheie secretă $k \geq 26$ este echivalentă cu cheia $k \bmod 26$.
- Două criptări succesive cu cheile secrete k_1 și k_2 sunt echivalente cu o criptare folosind cheia $(k_1 + k_2) \bmod 26$, deci nu se îmbunătățește securitatea!
- Un caracter x din textul clar se criptează prin:
$$enc_k(x) = (x + k) \bmod 26$$
- Un caracter x din textul criptat se decriptează prin:
$$dec_k(x) = (x - k) \bmod 26$$

Exemplu: Criptarea mesajului **CRIPTOGRAFIE** folosind cheia secretă $k = 7$

Alfabet:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Criptare:

- literei **C** îi corespunde $x = 2 \Rightarrow$ se va cripta în $(2 + 7) \bmod 26 = 9 \Rightarrow$ litera **J**
- literei **R** îi corespunde $x = 17 \Rightarrow$ se va cripta în $(17 + 7) \bmod 26 = 24 \Rightarrow$ litera **Y**
- ……
- literei **E** îi corespunde $x = 4 \Rightarrow$ se va cripta în $(4 + 7) \bmod 26 = 11 \Rightarrow$ litera **L**

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

Decriptare:

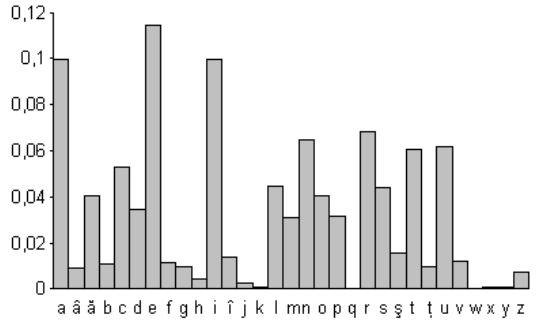
- literei **J** îi corespunde $x = 9 \Rightarrow$ se va decripta în $(9-7) \bmod 26 = 2 \Rightarrow$ litera **C**
- ……
  - literei **A** îi corespunde $x = 0 \Rightarrow$ se va decripta în $(0-7) \bmod 26 = (-7) \bmod 26 = 19 \Rightarrow$ litera **T**
  - ……

Se continuă în mod analog pentru fiecare literă și final se obține cuvântul **CRIPTOGRAFIE**.

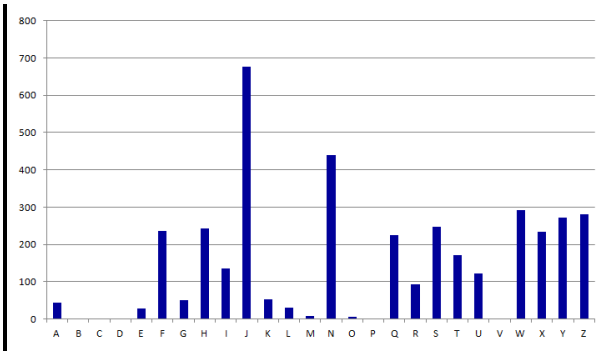
Modalități de criptanaliza ale cifrului Cezar

Forţă brută: Spaţiul cheilor este mulțimea {0,1,…,25}, deci un criptanalist poate obţine textul clar prin încercarea celor 25 de posibile chei.

Frecvenţa de apariţie: Fiind un cifru de substituție monoalfabetică, litera cu frecvența maximă din textul criptat va corespunde literei cu frecvență maximă din alfabetul limbii respective.



Frecvențele literelor din limba română

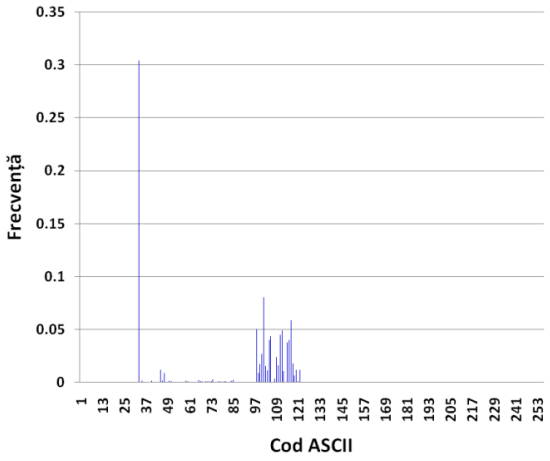


Frecvențele literelor unui text criptat folosind cifrul Cezar

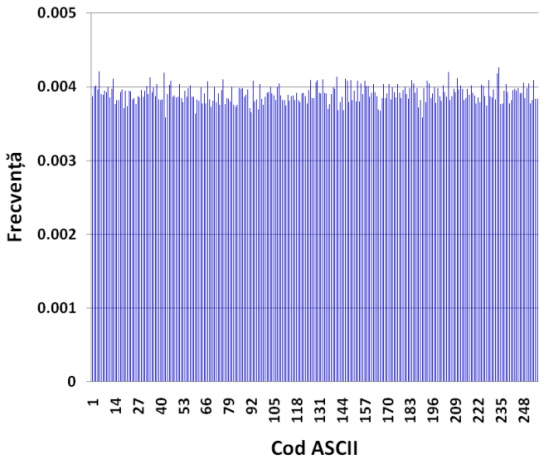
Din analiza frecvențelor literelor textului criptat se deduce faptul ca litera **J** din textul criptat are frecvența maximă, deci ei îi corespunde litera **E**, de unde deducem faptul că a fost folosită cheia de criptare $k = 9 - 4 = 5$.

În general, pentru a rezista în faţa atacurilor criptanalitice, un criptosistem trebuie să producă, indiferent de cheia secretă utilizată, texte cifrate cu o distribuţie uniformă a caracterelor care să mascheze distribuţia neuniformă a caracterelor inerentă oricărui text clar.

Unul dintre instrumentele utilizate în acest scop îl constituie **histograma** caracterelor ASCII dintr-un text, o reprezentare grafică a frecvenţelor lor.



Histograma textului clar



Histograma textului cifrat

2. Cifrul de permutare

Exemplu: Criptarea mesajului **EXEMPLU** cu cheia secretă $p = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$

Criptare:

	1	2	3	4	1	2	3	4
Mesaj clar	E	X	E	M	P	L	U	Q
	4	3	1	2	4	3	1	2
Mesaj criptat	E	M	X	E	U	Q	L	P

Observație: Dacă lungimea mesajului clar nu este un multiplu al lungimii permutării, atunci se vor adăuga la sfârșitul mesajului de mai multe ori litera Q (litera cu cea mai mică frecvență de utilizare în limba română).

Decriptare:

Vom folosi inversa permutării inițiale p:

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} \Rightarrow p^{-1} = \begin{pmatrix} 4 & 3 & 1 & 2 \\ 1 & 2 & 3 & 4 \end{pmatrix} \Rightarrow p^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

	1	2	3	4	1	2	3	4
Mesaj criptat	E	M	X	E	U	Q	L	P
	3	4	2	1	3	4	2	1
Mesaj decriptat	E	X	E	M	P	L	U	Q

Observație: Există $n!$ permutări de ordin/lungime n.
$4! = 24$
$5! = 120$
$6! = 720$
$7! = 5.040$
$8! = 40.320$
$9! = 362.880$
$10! = 3.628.800$

Securitatea acestui cifru este mult mai mare decât securitatea cifrului lui Cezar deoarece spațiul cheilor de criptare este mult mai mare și analiza frecvenței literelor din textul criptat nu ajută la spargerea cifrului!

3. Cifrul de transpoziție columnară

Text clar = UNEXEMPLUFOARTESIMPLUSICLAR
Cheia secretă = TESTARE

CRIPTARE:
1. Se creează un tabel având un număr de coloane egal cu numărul de litere distincte din cheia secretă (pe prima linie, literele distincte sunt în ordinea din cheia secretă) și se scrie textul clar pe linii:

T	E	S	A	R
U	N	E	X	E
M	P	L	U	F
O	A	R	T	E
S	I	M	P	L
U	S	I	C	L
A	R	Q	Q	Q

2. Se ordonează coloanele tabelului după prima linie (cheia secretă):

A	E	R	S	T
X	N	E	E	U
U	P	F	L	M
T	A	E	R	O
P	I	L	M	S
C	S	L	I	U
Q	R	Q	Q	A

3. Textul criptat se obține parcurgând tabelul pe coloane:

Textul criptat = XUTPCQNPAISREFELLQELRMIQUMOSUA

DECRIPTARE:

Text criptat = XUTPCQNPAISREFELLQELRMIQUMOSUA
Cheia secretă = TESTARE

1. Se creează un tabel având un număr de coloane egal cu numărul de litere distincte din cheia secretă (pe prima linie, literele distincte sunt în ordine alfabetică) și se scrie textul criptat pe coloane. Numărul de linii de pe fiecare coloană se obține împărțind lungimea textului criptat la numărul de litere distincte din cheia secretă:

A	E	R	S	T
X	N	E	E	U
U	P	F	L	M
T	A	E	R	O
P	I	L	M	S
C	S	L	I	U
Q	R	Q	Q	A

2. Se ordonează coloanele tabelului conform cheii secrete

T	E	S	A	R
U	N	E	X	E
M	P	L	U	F
O	A	R	T	E
S	I	M	P	L
U	S	I	C	L
A	R	Q	Q	Q

3. Textul decriptat se obține parcurgând tabelul pe linii

Text decriptat = UNEXEMPLUFOARTESIMPLUSICLAR

4. Pătratul lui Polybius

Un **pătrat Polybius** este un careu de dimensiune 5x5 în care literele alfabetului sunt așezate într-o ordine dată de literele distincte dintr-o cheie secretă.

Criptarea unui mesaj constă în înlocuirea fiecărei litere cu coordonatele sale din pătrat (sub forma unui număr de două cifre, prima reprezentând linia, iar cea de-a doua coloana), iar decriptarea se realizează simetric.

Exemplu:

	1	2	3	4	5
1	S	E	C	R	T
2	I/J	G	U	A	B
3	D	F	H	K	L
4	M	N	O	P	Q
5	V	W	X	Y	Z

Cheia secretă = SECRETSIGUR
Text clar = EXEMPLU
Textul criptat = 12 53 12 41 44 35 23

Cheia secretă ideală = propoziție holoalfabetică / pangramă = conține toate literele alfabetului

Exemple:
1. The quick brown fox jumps over the lazy dog.
2. Muzicologă în bej, vând whisky și tequila, la preț fix.

Analizând exemplele de mai sus, putem identifica următoarele primitive criptografice:

1. substituție: înlocuirea unui caracter din textul clar cu un alt caracter (sau mai multe) în textul criptat, fără a-i modifica poziția (cifrul lui Cezar și pătratul lui Polybius)

2. permutare: modificarea poziției unui caracter din textul clar în textul criptat, fără a-i modifica valoarea (cifrul de permutare și cifrul de transpoziție columnară)

3. fracționare: înlocuirea unui caracter/simbol din textul clar cu cel puțin două caractere/simboluri în textul criptat (pătratul lui Polybius)

Metode de substituție:
- tabel de substituție
- formulă de calcul

Metode de fracționare:
- pătrat Polybius (1 literă = 2 cifre)
- cod Baudot (1 literă = 5 simboluri +/-)
- cod ASCII (1 literă = 8 biți)