



Criptografie și Securitate

- Prelegerea 2 - Sisteme istorice de criptare

Adela Georgescu, Ruxandra F. Olimid

Facultatea de Matematică și Informatică
Universitatea din București

Cuprins

1. Cifruri de permutare / transpoziție
2. Cifruri de substitutie

Cifruri de permutare / transpoziție

Definitie

*Un **cifru de permutare** presupune rearanjarea literelor în textul clar pentru a obține textul criptat.*

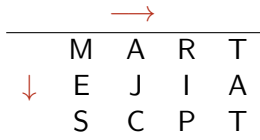
Cifruri de permutare / transpoziție

- ▶ sistemul Rail Fence
- ▶ cifruri generale de transpoziție

Cifruri de permutare / transpoziție

- ▶ sistemul Rail Fence >>> curs
- ▶ cifruri generale de transpoziție >>> seminar

Rail Fence



A diagram illustrating the Rail Fence cipher with $k=3$. It consists of three horizontal rails. The top rail contains the letters M, A, R, T. The middle rail contains E, J, I, A. The bottom rail contains S, C, P, T. A red arrow points right above the top rail, and a red arrow points down to the left of the middle rail, indicating the zigzag pattern of the encryption.

	M	A	R	T
↓	E	J	I	A
	S	C	P	T

Text clar: mesaj criptat

Cheia: $k = 3$

Text criptat: MARTEJIASCPT

Cifruri de substituție

Definitie

*Un **cifru de substituție** presupune înlocuirea unui caracter (set de caractere) cu un alt caracter (set de caractere).*

Clasificare:

- ▶ **monoalfabetice**: pentru o cheie dată, un caracter este întotdeauna înlocuit în textul cifrat de același caracter
- ▶ **polialfabetice**: pentru o cheie dată, un caracter este înlocuit în textul cifrat de caractere diferite

Cifruri de substituție monoalfabetice

- ▶ cifrul lui Cezar
- ▶ substituție simplă
- ▶ sistemul Cavalerilor de Malta

Cifruri de substituție monoalfabetice

- ▶ cifrul lui Cezar >>> curs, seminar
- ▶ substituție simplă >>> curs, seminar
- ▶ sistemul Cavalerilor de Malta >>> seminar

Cifrul lui Cezar

a	b	c	d	e	f	g	h	i	j	k	l	m
D	E	F	G	H	I	J	K	L	M	N	O	P

n	o	p	q	r	s	t	u	v	w	x	y	z
Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Text clar: mesaj criptat

Text criptat: PHVDM FULSWDW

Cifrul lui Cezar

- ▶ \mathcal{K}
- ▶ \mathcal{M}
- ▶ \mathcal{C}
- ▶ $\text{Enc} : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C}$

- ▶ $\text{Dec} : \mathcal{K} \times \mathcal{C} \rightarrow \mathcal{M}$

Cifrul lui Cezar

- ▶ $\mathcal{K} = \{0, 1, \dots, 25\}$

- ▶ \mathcal{M}

- ▶ \mathcal{C}

- ▶ $\text{Enc} : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C}$

- ▶ $\text{Dec} : \mathcal{K} \times \mathcal{C} \rightarrow \mathcal{M}$

Cifrul lui Cezar

- ▶ $\mathcal{K} = \{0, 1, \dots, 25\}$
- ▶ $\mathcal{M} = \{a, b, \dots, z\}^*$
- ▶ \mathcal{C}
- ▶ $\text{Enc} : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C}$

- ▶ $\text{Dec} : \mathcal{K} \times \mathcal{C} \rightarrow \mathcal{M}$

Cifrul lui Cezar

- ▶ $\mathcal{K} = \{0, 1, \dots, 25\}$
- ▶ $\mathcal{M} = \{a, b, \dots, z\}^*$
- ▶ $\mathcal{C} = \{A, B, \dots, Z\}^*$
- ▶ $\text{Enc} : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C}$

- ▶ $\text{Dec} : \mathcal{K} \times \mathcal{C} \rightarrow \mathcal{M}$

Cifrul lui Cezar

- ▶ $\mathcal{K} = \{0, 1, \dots, 25\}$
- ▶ $\mathcal{M} = \{a, b, \dots, z\}^*$
- ▶ $\mathcal{C} = \{A, B, \dots, Z\}^*$
- ▶ $\text{Enc} : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C}$

$$\text{Enc}_k(m) = m + k \pmod{26}$$

- ▶ $\text{Dec} : \mathcal{K} \times \mathcal{C} \rightarrow \mathcal{M}$

Cifrul lui Cezar

- ▶ $\mathcal{K} = \{0, 1, \dots, 25\}$
- ▶ $\mathcal{M} = \{a, b, \dots, z\}^*$
- ▶ $\mathcal{C} = \{A, B, \dots, Z\}^*$
- ▶ $\text{Enc} : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C}$

$$\text{Enc}_k(m) = m + k \pmod{26}$$

- ▶ $\text{Dec} : \mathcal{K} \times \mathcal{C} \rightarrow \mathcal{M}$

$$\text{Dec}_k(c) = c - k \pmod{26}$$

Criptanaliză - Atac prin forță brută

- ▶ $|\mathcal{K}| = 26$
- ▶ atac prin forță brută (căutare exhaustivă): încercarea, pe rând, a tuturor cheilor posibile până când se obține un text clar cu sens

Principiul cheilor suficiente: O schemă sigură de criptare trebuie să aibă un spațiu al cheilor suficient de mare a.î. să nu fie vulnerabilă la căutarea exhaustivă.

Substituția simplă

a	b	c	d	e	f	g	h	i	j	k	l	m
F	I	L	O	R	U	X	A	D	G	J	M	P

n	o	p	q	r	s	t	u	v	w	x	y	z
S	V	Y	B	E	H	K	N	Q	T	W	Z	C

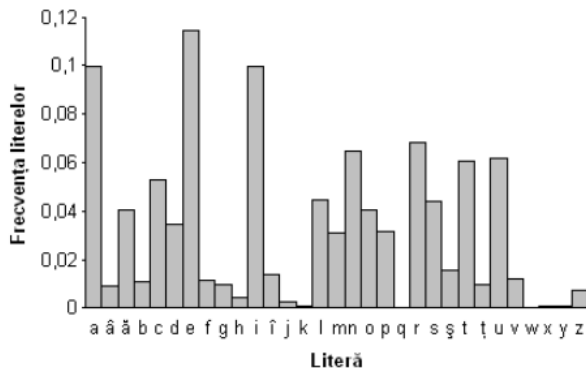
Text clar: mesaj criptat

Text criptat: PRHFG LEDYKFK

Criptanaliză - Analiza de frecvență

- ▶ $|\mathcal{K}| = 26!$
- ▶ atacul prin forță brută devine mai dificil
- ▶ **analiza de frecvență**: determinare corespondenței între alfabetul clar și alfabetul criptat pe baza frecvenței de apariție a literelor în text, cunoscând distribuția literelor în limba textului clar
 - ▶ se cunoaște limba textului clar
 - ▶ lungimea textului permite analiza de frecvență

Criptanaliză - Analiza de frecvență



[Wikipedia]

Cifruri de substituție polialfabetice / poligrafice

- ▶ sistemul Playfair
- ▶ sistemul Vigenère

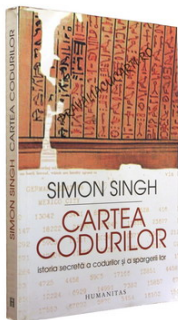
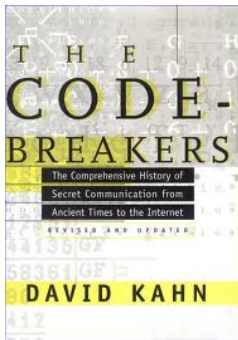
Cifruri de substituție polialfabetice / poligrafice

- ▶ sistemul Playfair >>> seminar
- ▶ sistemul Vigenère >>> laborator

Important de reținut!

- ▶ Tipuri de cifruri: transpoziție, substituție
- ▶ Astfel de sisteme sunt total nesigure!

Referințe bibliografice



<http://simonsingh.net/books/the-code-book/>