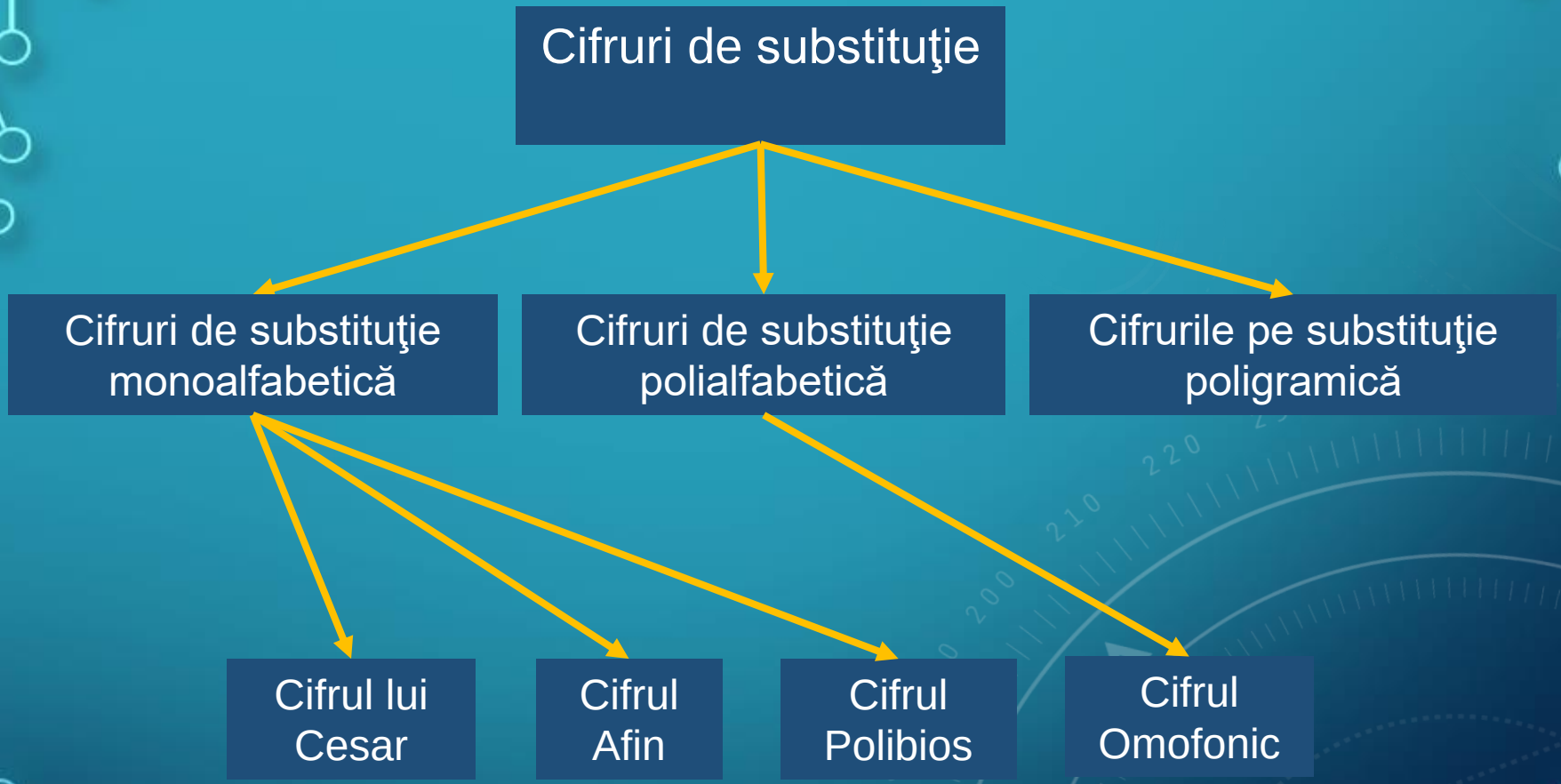
TEMA 2.
Cifruri clasice

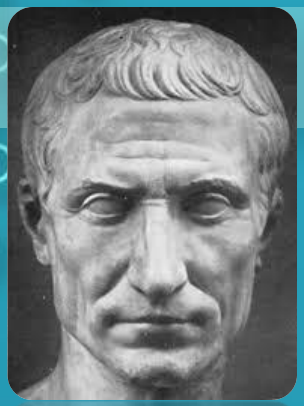
Repere

- Cifruri de substituţie
- Cifrul de transpoziţii

CIFRURI DE SUBSTITUȚIE

- 1900 î.Hr. Mormântul lui Khnumhotep II
- 1500 î.Hr. Mesopotamia: semnături
- 800 î.Hr. Homer, Iliada, Bellerophon


Cifruri de substituţie
Cifruri de substituţie monoalfabetică
Cifruri de substituţie polialfabetică
Cifrurile pe substituţie poligramică
Cifrul lui Cesar
Cifrul Afin
Cifrul Polibios
Cifrul Omofonic



Cifrul lui Cesar:

- Fiecare literă a textului în clar este înlocuită cu o nouă literă obţinută printr-o deplasare alfabetică;
- Cheia (aceeaşi la criptare cât şi la decriptare) constă în numărul care indică deplasarea alfabetică;

$$c = e_k(\mathrm{x}) = \mathrm{x} + \mathrm{k} (\mathrm{mod}\ \mathrm{n})$$
$$m = d_k(\mathrm{y}) = \mathrm{y} - \mathrm{k} (\mathrm{mod}\ \mathrm{n})$$

Să se cripteze mesajul: CRIPTOGRAFIE

K = 7

- Literei C îi corespunde $x = 2$, $(2 + 7) \bmod 26 = 9$ primim J;
- Literei R îi corespunde $x = 16$, $(16 + 7) \bmod 26 = 24$, primim Y;

Am obținut: JYPWA VNYHM PL

Să se decripteze mesajul:

JAJSN SHWDU YTQTL DXNQJ SHJNX LTQIJ SXXXX

x	0	1	2	3	4	5	6	...	25
Text clar	A	B	C	D	E	F	G	...	Z
K = 1	B	C	D	E	F	G	H	...	A
K = 2	C	D	E	F	G	H	I	...	B
K = 3	D	E	F	G	H	I	J	...	C
K = 4	E	F	G	H	I	J	K	...	D
K = 5	F	G	H	I	J	K	L		E
...	...	...	...	...	...	...	...	...	...

$K = 1$:

IZIRM RGVCT XSPSK CWMPI RGIMW KSPHI RWWWW

$K = 2$:

HYHQL QFUBS WRORJ BVLOH QFHLV JROGH QVVVV

$K = 3$:

GXGPK PETAR VQNQI AUKNG PEGKU IQNFG PUUUU

$K = 4$:

FWFOJ ODSZQ UPMPH ZTJMF ODFJT HPMEF OTTTT

$K = 5$:

EVENI NCRYP TOLOG YSILE NCEIS GOLDE NSSSS

EVEN IN CRYPTOLOGY SILENCE IS GOLDEN

Text clar: **AZI ESTE PRIMUL CURS**

K = **3**

Text cifrat: **?**

Text criptat: **F D H V D U**

K = **?**

Text clar: **?**

Cifrul lui Afin:

$\boldsymbol{k} = \{(a, b) \mid a, b \in Z\ 26 = \{0, 1, 2, \ldots, 25\},$ $\text{cmmdc}(a, 26) = 1\},$

$\boldsymbol{k} = (a, b))$

$e_k(\boldsymbol{x}) = a\boldsymbol{x} + b \pmod{26},$

$d_k(\text{y}) = a^{-1}\text{y} + a^{-1}(26 - b) \pmod{26}$

Să se cripteze mesajul: *LA MULTI ANI*

a = 7, b = 16 $e_k(x) = 7x + 16$

x	0	1	2	3	4	5	6	...	25
Text clar	A	B	C	D	E	F	G	...	Z
$e_k(x)$	16	23	4	11	18	25	6	...	9
Text cifrat	Q	X	E	L	S	Z	G	.....	J

Am obținut: *PQ WAPTU QDU*

Cifrul lui Polibius:

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

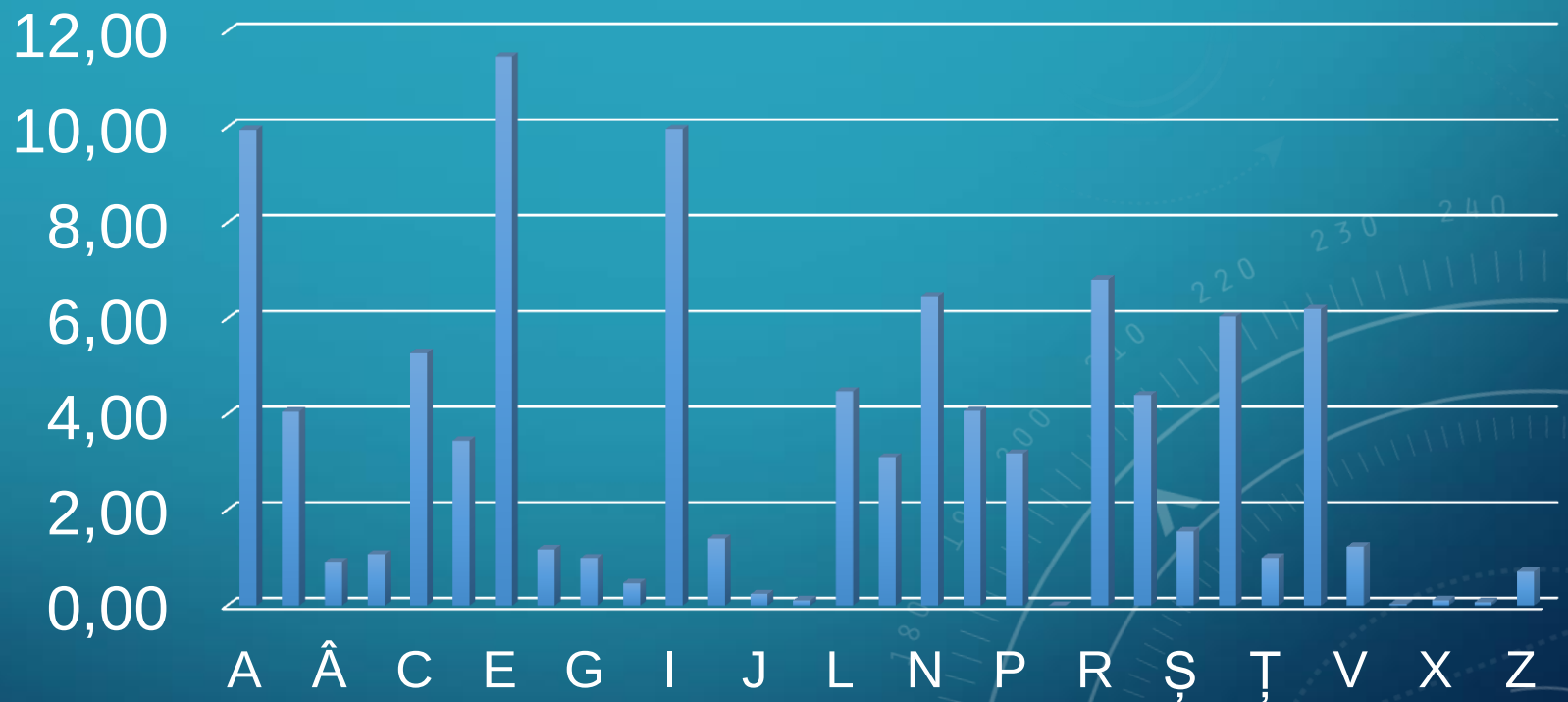
Text clar: A SOSIT TIMPUL

Text cifrat: 11 3443344244 444223535413

Frecvența literelor limbii române:

A	Ă	Â	B	C	D	E	F	G	H	I	Î	J	K	L	M
9.95	4.06	0.91	1.07	5.28	3.45	11.47	1.18	0.99	0.47	9.96	1.40	0.24	0.11	4.48	3.10
N	O	P	Q	R	S	Ș	T	Ț	U	V	W	X	Y	Z	
6.47	4.07	3.18	0.00	6.82	4.40	1.55	6.04	1.00	6.20	1.23	0.03	0.11	0.07	0,71	

Frecvența literelor



Cifruri de substituţie polialfabetică:

- Sunt formate din mai multe cifruri de substituţie simple;
- Utilizarea unor substituţii monoalfabetice diferite;
- Se consideră ca primul sistem de criptare polialfabetic a fost creat de Leon Battista in 1568.

Cifrul omofonic:

A – cu cea mai mare frecvenţă de apariţie în alfabetul primar – poate fi înlocuită cu F, * sau K;

- $F(a) \cap F(b) = \emptyset \leftrightarrow a \neq b$;
- Dacă *a* apare mai frecvent decat *b* în textele clare, atunci card

  ((*F*(*a*)) ≥ card(*F*(b)).

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
8	2	3	4	13	2	2	6	7	1	1	4	3	7	8	2	1	6	6	9	3	1	2	1	2	1
09	48	13	01	14	10	06	23	32	15	04	26	22	18	00	38	94	29	11	17	08	34	60	28	21	02
12	81	41	03	16	31	25	39	70			37	27	58	05	95		35	19	20	61		89		52	
33		62	45	24			50	73			51		59	07			40	36	30	63					
47			79	44			56	83			84		66	54			42	76	43						
53				46			65	88					71	72			77	86	49						
67				55			68	93					91	90			80	96	69						
78				57										99					75						
92				64															85						
				74															97						
				82																					
				87																					
				98																					

1. deşi mai greu de spart decât cifrurile de substituţie simple (monoalfabetice), ele nu maschează total proprietăţile statistice ale mesajului în clar.
2. în cazul unui atac cu text în clar cunoscut, cifrul se sparge extrem de uşor.
3. atacul cu text cifrat este mai dificil, dar unui calculator îi va lua doar câteva secunde pentru al sparge.

Cifrul lui Vigenere

- Criptarea:

$$c_i = m_i + k_i (\text{mod } 26)$$

- Decriptarea:

$$m_i = c_i - k_i (\text{mod } 26)$$

Cifrul lui Vegenere:

Text clar: SUBSTITUȚIE POLIALFABETICĂ;

Cheia: ACADEMIEACADEMIEACADEMIEA;

S + A = 18 + 0(mod 26) = 18(mod 26) = 18 = S

U + C = 20 + 2(mod 26) = 22(mod 26) = 22 = W

B + A = 1 + 0(mod 26) = 1(mod 26) = 1 = B

...

C + E = 2 + 4(mod 26) = 6(mod 26) = 6= G

A + A = 0 + 0(mod 26) = 0(mod 26) = 0 = A

Text cifrat: SWBVXUBYTKESSXQELHAEIFQGA

	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

Tabula Recta pentru cifrul Vigenere

Cifrul lui Playfair:

- *m1*, *m2* în vârfurile opuse ale unui dreptunghi → *c1*, *c2* caracterele din celelalte vârfuri ale dreptunghiului, *c1* fiind în aceeaşi linie cu *m1*.
- *m1* şi *m2* într-o linie → *c1* şi *c2* printr-o deplasare ciclică spre dreapta a literelor *m1* şi *m2*.
- *m1* şi *m2* în aceeaşi coloană → *c1* şi *c2* prin deplasarea ciclică a lui *m1*, *m2* de sus în jos.

CHEIE →

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

AB → ? AF → ? XM → ? RC → ? LU → ?

Întrebare de control

Text clar: Curs nou;

Cheia K = SUPER;

Text ctiptat: ?

Criptați și decriptați aplicând cirul Vigenere

CIFRUL DE TRANSPOZIŢII

Un **CIFRU DE PERMUTARE** presupune rearanjarea literelor în textul clar pentru a obține textul criptat.

Textul: „Misiunea a fost îndeplinită”

Lungimea = 24

	1	2	3	4	5	6
1	M	i	s	i	u	n
2	e	a	a	f	o	s
3	t	î	n	d	e	p
4	l	i	n	i	t	ă
5	x	y	z	t	w	u

	1	2	3	4	5	6
5	x	y	z	t	w	u
3	t	î	n	d	e	p
4	l	i	n	i	t	ă
1	M	i	s	i	u	n
2	e	a	a	f	o	s

Transpoziție cu cheie

- Alegerea unei cheii ale cărei literă determină ordinea în care se vor scrie coloanele din matricea aleasă;
- Se ordonează alfabetic literele din cheie, şi fiecărei litere i se asociază numărul de ordine din şirul ordonat.

Textul: „Misiunea a fost îndeplinită”

Cheia: VULTUR

	V	U	L	T	U	R
	6	4	1	3	5	2
1	M	i	s	i	u	n
2	e	a	a	f	o	s
3	t	î	n	d	e	p
4	l	i	n	i	t	ă
5	x	y	z	t	w	u

	1	2	3	4	5	6
1	s	n	i	i	u	M
2	a	s	f	a	o	e
3	n	p	d	î	e	t
4	n	ă	i	i	t	l
5	z	u	t	y	w	x

Întrebare de control

- Metoda transpoziției constă în ....?
- Enumerați cifrurile de substituție?

ÎNTREBĂRI RECAPITULATIVE

- Metoda transpoziției constă în ....?
- Enumerați cifrurile de substituție?

CIFRURI CLASICE