CURS 3
CIFRURI CLASICE
(continuare)

1. Cifrul nihilist (1880 – Rusia)

a) Se construiește un pătrat Polybius folosind prima cheie secretă

	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

b) Se codifică textul clar și a doua cheie secretă folosind pătratul Polybius

A doua cheie secretă = GARD

Text clar	E	X	E	M	P	L	U
	12	53	12	41	44	35	23
	22	24	14	31	22	24	14
A doua cheie secretă	G	A	R	D	G	A	R
Text criptat	34	77	26	72	66	59	37

c) Mesajul criptat se obține adunând numerele corespunzătoarele textului clar și celei de-a doua chei secrete:

Text criptat = 34 77 26 72 66 59 37

Decriptarea se realizează în mod simetric, scăzând a doua cheie secretă din textul criptat.

Observație: În textul cifrat se pot obține numere mai mari sau egale cu 100 doar adunând codurile literelor de pe ultima linie a pătratului Polybius sau 45+55.

2. Cifrul bifid (Felix Delastelle – 1901)

a) Se construiește un pătrat Polybius folosind cheia secretă

Cheia secretă = SECRETSIGUR

	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

CRIPTARE:

Text clar = UNEXEMPLUSIMPLU

1. Se scriu pe verticală coordonatele literelor textului clar folosind pătratul Polybius:

U	N	E	X	E	M	P	L	U	S	I	M	P	L	U
2	4	1	5	1	4	4	3	2	1	2	4	4	3	2
3	2	2	3	2	1	4	5	3	1	1	1	4	5	3

2. Se scriu cele două linii cu cifre una după alta și se grupează câte două:

24	15	14	43	21	24	43	23	22	32	14	53	11	14	53
A	T	R	O	I	A	O	U	G	F	R	X	S	R	X

3. Se înlocuiește fiecare grup de două cifre cu litera corespunzătoare din pătratul Polybius și se obține textul criptat:

Textul criptat = ATROIAOUGFRXSRX

DECRIPTARE: SIMETRICĂ!!!

3. Cifrul ADFGX (Fritz Nebel – 1918)

a) Se construiește un pătrat Polybius cu literele ADFGX în locul cifrelor de la 1 la 5 folosind prima cheie secretă:

Cheia secretă = SECRETSIGUR

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

Au fost alese cele 5 litere deoarece sunt foarte diferite în codul Morse, prevenind astfel posibilele erori de transmitere sau recepționare.

b) Se înlocuiește fiecare literă din textul clar cu perechea de litere corespunzătoare din pătratul Polybius:

Text clar = ATACAMLAORAOPTLASUD

A	T	A	C	A	M	L	A	O	R	A	O	P	T	L	A	S	U	D
DG	AX	DG	AF	DG	GA	FX	DG	GF	AG	DG	GF	GG	AX	FX	DG	AA	DF	FA

Text intermediar = DGAXDGAFDGGAFXDGGFAGDGGFGGAXFXDGAADFFA

c) Se aplică asupra textului intermediar un cifru de transpoziție columnară folosind a doua cheie secretă:

Text intermediar = DGAXDGAFDGGAFXDGGFAGDGGFGGAXFXDGAADFFA
A doua cheie secretă = TESTARE

T	E	S	A	R
D	G	A	X	D
G	A	F	D	G
G	A	F	X	D
G	G	F	A	G
D	G	G	F	G
G	A	X	F	X
D	G	A	A	D
F	F	A	Q	Q

d) Se ordonează alfabetic coloanele tabelului după prima linie:

A	E	R	S	T
X	G	D	A	D
D	A	G	F	G
X	A	D	F	G
A	G	G	F	G
F	G	G	G	D
F	A	X	X	G
A	G	D	A	D
Q	F	Q	A	F

d) Textul cifrat se obține scriind textul din tabel pe coloane:

Text cifrat = XDXAFFAQGAAGGAGF...

DECRIPTARE: SIMETRICĂ!!!

Cifrul ADFGX a fost criptanalizat în 1918 de către Georges Painvin.

4. Cifrul Playfair (Charles Wheatstone - 1854)

- A fost propus în anul 1854 de Charles Wheatstone, dar promovat pentru utilizare de Lordul Playfair.
- Este un cifru de substituție digrafică deoarece transformă un grup de două litere (o digramă) într-un grup de alte două litere.
- Se folosește alfabetul englez cu cele 26 de litere, din care se elimină caracterul cu frecvență minimă sau se asimilează litera J cu litera I.
- Se așază cele 25 de litere într-un careu cu dimensiunea 5×5.
- Se împarte textul clar în grupuri de câte două litere și, dacă există un grup format din litere identice, se elimină o literă din el. Se reia acest procedeu până când nu mai există niciun grup format din două litere identice. Dacă ultima grupă conține o singură literă, atunci se mai adaugă un caracter de completare (de obicei, caracterul cu frecvența minimă în limba respectivă).
- Se criptează fiecare digramă, astfel:
  - Dacă digrama nu are literele pe aceeași linie sau coloană, atunci regula de cifrare este regula dreptunghiului, traseul fiind pe verticală de la cea de-a doua literă a digramei către prima literă (prima litera a perechii cifrate este aceea care se găsește pe aceeași linie cu prima litera a perechii în clar).
  - Dacă digrama are literele pe aceeași linie, atunci se cifrează la dreapta și, respectiv, se descifrează la stânga.
  - Dacă digrama are literele pe aceeași coloană, atunci se cifrează în jos și, respectiv, se descifrează în sus.

Exemplu:

Cheia secretă = SECRETSIGUR

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

```
Text clar     = UN EX EM PL US IM PL UQ
Text criptat = GO CW SN QK IC DV QK BO

ER -> CT
TR -> ST

VS -> SI
```