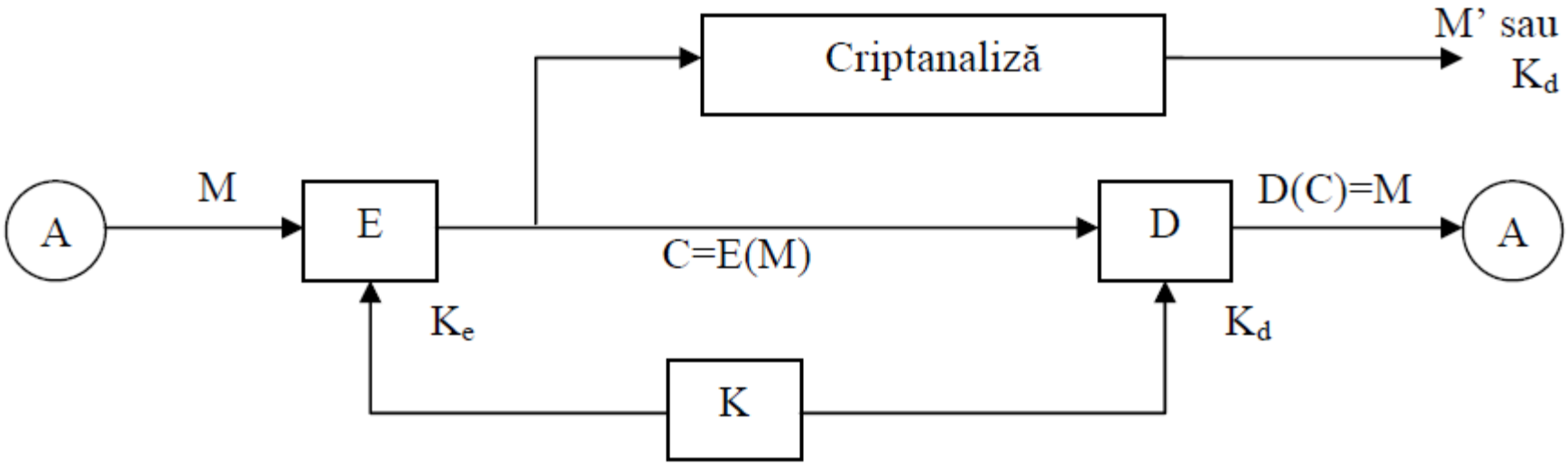
Tehnici criptografice

Criptare

- Criptografia = ştiinţa creării şi menţinerii mesajelor secrete, în sensul imposibiltăţii citirii lor de către neautorizaţi



Criptare

- **M** = mesaj (text) în clar (plain / clear text)
- **C** = mesaj cifrat (criptograma, cipher text)
- *Algoritm criptografic / cifru* = funcţia matematică utilizată pentru criptare / decriptare (2 funcții)
- **E** = criptare / cifrare

$$E(M) = C$$

- **D** = Decriptare / descifrare

$$D(C) = D(E(M))=M$$

Criptare

- *Cheia criptografica (K)* = mărimea necesară realizării criptării şi decriptării

- Un *criptosistem* este sistemul format din:
  - algoritm
  - toate mesajele în clar (M)
  - toate mesajele criptate (C)
  - toate cheile (K)

Criptare

- *Criptanaliza (cryptanalysis)* = ştiinţa spargerii cifrurilor
- *Steganografia (steganography)* = tehnica ascunderii mesajelor secrete în alte mesaje, în aşa fel încât existenta mesajelor secrete să fie invizibilă

Criptosistem

- Rolul unui criptosistem de a preveni sau detecta activităţile nepermise dintr-un sistem informatic:
  - consultarea neavizată a datelor transmise sau stocate
  - inserarea de mesaje false
  - modificarea, ştergerea sau distrugerea mesajelor existente
  - analiza traficului
  - conectările neautorizate

"poliţie informatică"

Obiectivele unui criptosistem

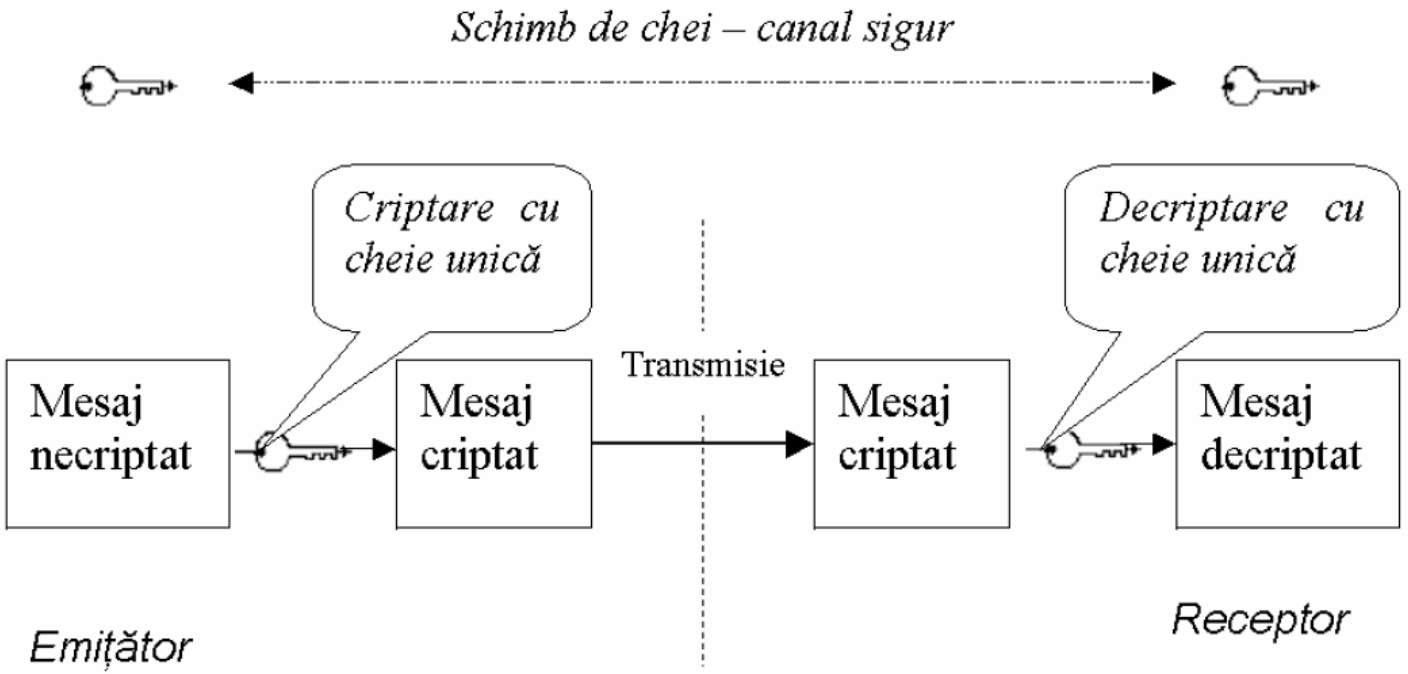
Obiectiv		Definire
Confidenţialitatea		păstrarea secretului pentru neavizaţi
Autentificarea	emiţător /identificare	legată de identitatea unei entităţi (persoană, terminal, carte de credit, etc.)
	originii datelor	legată de sursa de informaţie
	integrităţii datelor	asigură că informaţia nu a fost modificată de surse neautorizate
Semnătura digitală		mijlocul de a lega informaţia de entitate

Criptosisteme cu chei simetrice

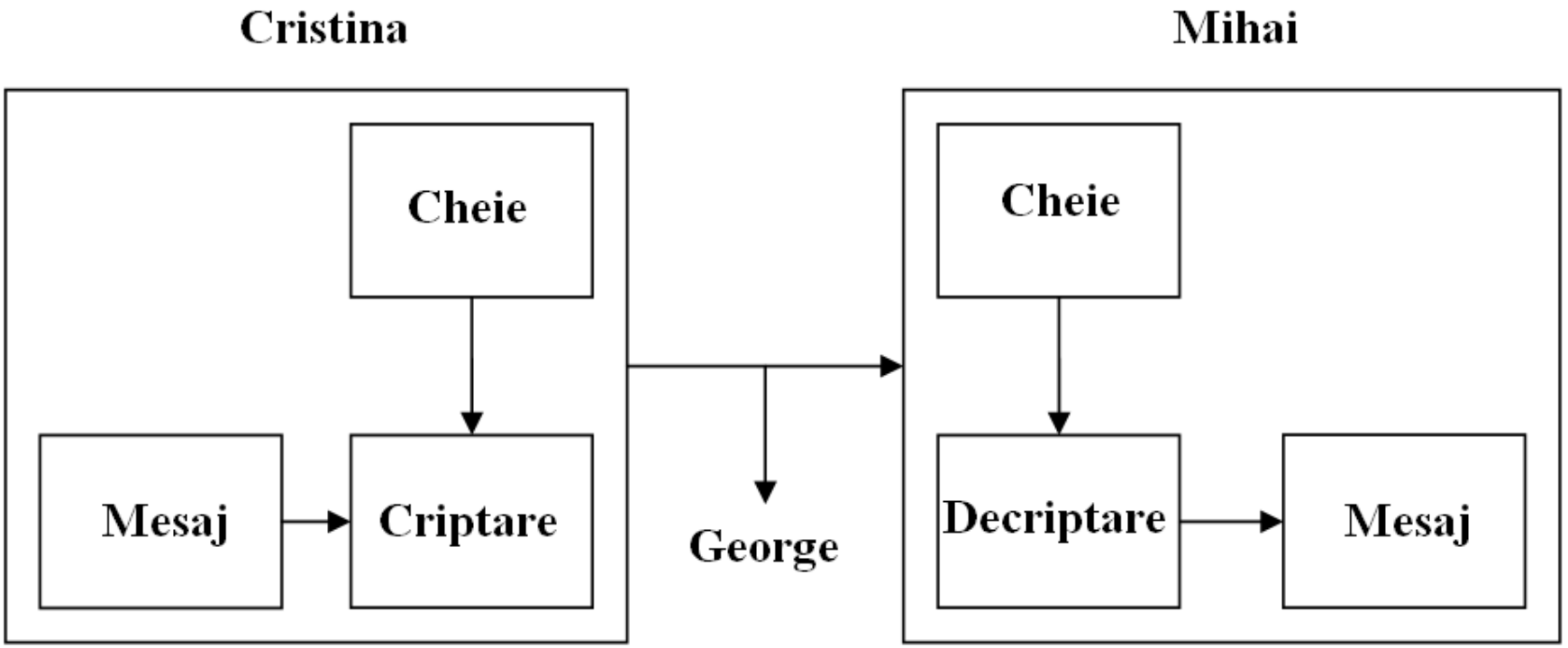
$$K_e = K_d = K$$

$$E_K(M) = C$$

$$D_K(C) = D_K(E_K(M)) = M$$



Criptosisteme cu chei simetrice



Criptosisteme cu chei simetrice

Clasificare în (funcție de modul în care acționează)*:*

- *cu cifruri bloc (block ciphers)*
  - acționează bloc cu bloc (de dimensiune fixă)
  - criptează un bloc la un moment dat
  - substituţii şi transpoziţii, eventual repetate iterativ
- *cu cifruri secvenţiale (stream ciphers):*
  - acționează bit cu bit
  - cheia K generată de un registru de deplasare digital având starea iniţială S_0
  - cheia K combinată cu simbolul original pentru a obține simbolul cifrat

Criptografia simetrică

- Clasificare (în funcție de operația pe care o realizează):
  - Cifruri substituţie;
  - Cifruri transpoziţie;
  - Cifruri combinate.

Criptografia simetrică - cifruri substituţie

- cifruri bloc
- fiecare caracter (sau grup de caractere) al lui M este substituit cu un alt caracter (sau grup de caractere) al textului cifrat (C)
- decriptarea = substituție inversă

Criptografia simetrică - cifruri substituţie

- 4 tipuri:

1. Cifruri de substituţie monoalfabetică

- fiecare caracter al textului în clar (M) este înlocuit cu un caracter corespondent al textului cifrat (C)
- **Exemplu:** cifrul CAESAR
  - translatere în față cu k

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

$$\alpha \rightarrow (\alpha + k) \bmod 26$$

Criptografia simetrică - cifruri substituţie

2. Cifruri de substituţie omofonica

- un caracter al alfabetului mesajului în clar (alfabet primar) poate să aibă mai multe reprezentări
- **Exemplu:**
  - Caracterul A (cu frecvență mare de apariție) poate fi înlocuit cu F, * sau K

Criptografia simetrică - cifruri substituţie

3. Cifruri de substituţie poligramică

- blocuri de caractere ale alfabetului primar – numite poligrame – substituite cu alte blocuri de caractere

Exemplu:

$$ABA \rightarrow RTQ$$

$$SLL \rightarrow ABB$$

Criptografia simetrică - cifruri substituţie

3. Cifrul de substituţie poligramică

Exemplu: 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.
  - GS → MN
- m1 şi m2 într-o linie → c1 şi c2 printr-o deplasare ciclică spre dreapta a literelor m1 şi m2.
  - AD → BF sau CF → DA
- m1 şi m2 în aceeaşi coloană → c1 şi c2 prin deplasarea ciclică a lui m1, m2 de sus în jos.
  - UO → BW sau EZ → FE

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

Cuvânt cheie

Criptografia simetrică - cifruri substituţie

4. Cifruri de substituţie polialfabetice

- sunt formate din mai multe cifruri de substituţie simple.
- utilizarea unor substituţii monoalfabetice diferite
- **Exemplu: cifrul lui Vigenère**

- text clar : SUBSTITUȚIE POLIALFABETICĂ ;

- cheia : ACADEMIEACADEMIEACADEMIEA;

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

U + C = 20 + 2 (mod26) = 22 (mod 26) = 22 = W

B + A = 1 + 0 (mod26) = 1 (mod26) = 1 = B

...

C + E = 2 + 4 (mod 26) = 6 (mod26) = 6 = G

A + A = 0 + 0 (mod26) = 0 (mod26) = 0 = A

- text cifrat : SWBVXUBYTKESSXQELHAEIFQGA .

Criptografia simetrică - cifruri cu transpoziţie

- reordonează literele din M, fără a le transforma
- mai multe transpoziții succesive pentru a mări securitatea

Exemplu: transpoziția pe coloane

- Text cifrat: NHFEEAELSDPT

N	E	E	D
H	E	L	P
F	A	S	T

Criptografia simetrică – mașini rotor

- metodele de substituţie şi permutare repetată sunt destul de complexe
- mecanizarea lor prin mașini rotor (1920)
- *maşina rotor* (rotor machine)
  - are o tastatură şi o serie de rotoare
  - Implementează o versiune a cifrului Vigenère.
  - Fiecare rotor face o permutare arbitrară a alfabetului, are 26 de poziţii şi realizează o simplă substituţie.
  - rotoarele se mişcă cu viteze de rotaţie diferite

  → perioada unei maşini cu n rotoare este 26^n
- **Exemplu:** maşina rotor Enigma

Criptografia simetrică – mașini rotor

- **Exemplu:** maşina rotor Enigma

Criptografia simetrică computaţională

Cifrul DES: Standard de criptare a datelor (Data Encryption Standard)

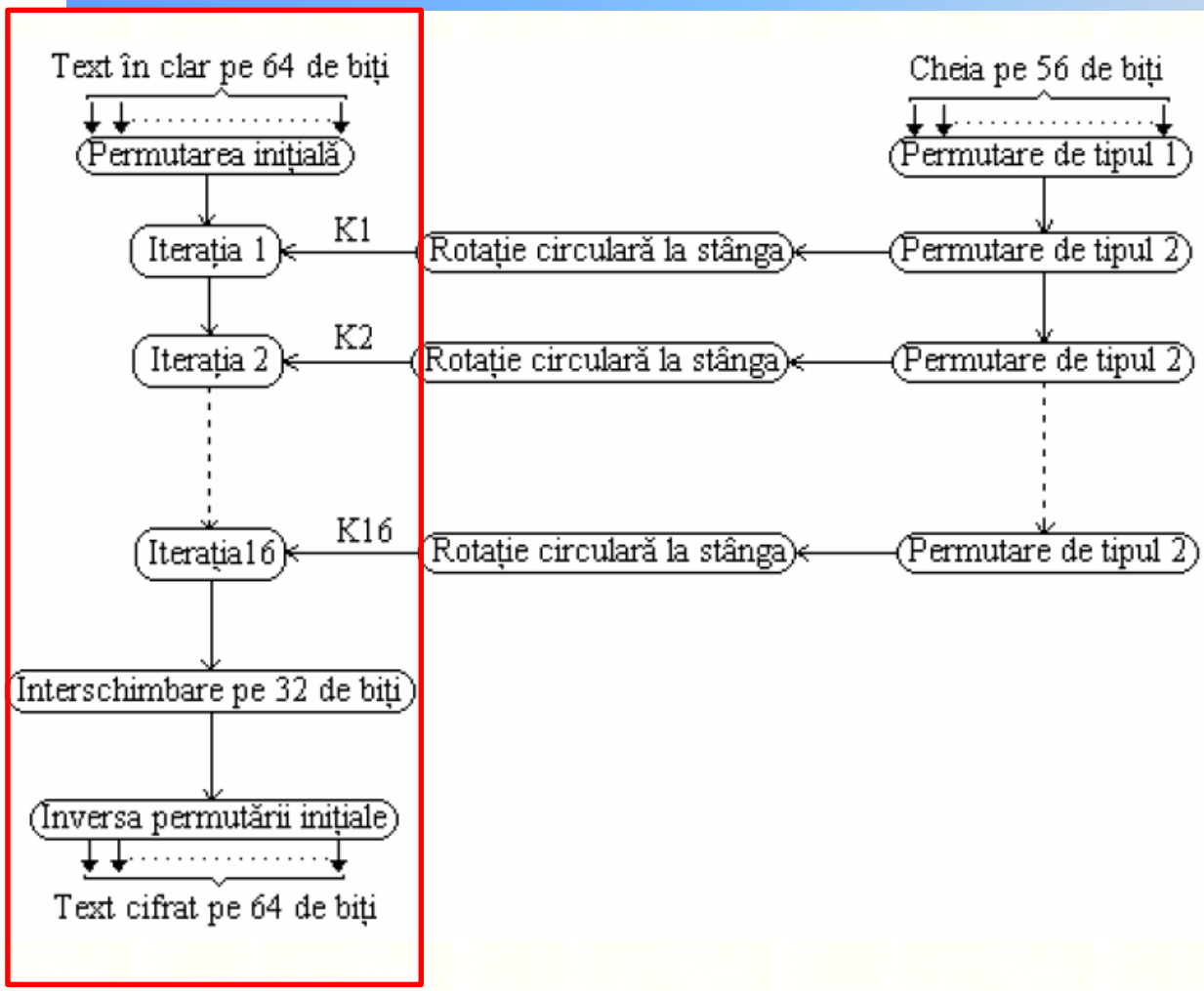
- dezvoltat de IBM în 1977, valabil până în 2001
- Algoritm utilizat pe majoritatea platformelor UNIX, pentru criptarea parolelor
- Primul algoritm criptografic publicat

DES (Data Encryption Standard)

Caracteristici:

- lungimea unui bloc este de 64 de biţi
- cheia este pe 56 de biţi (+8 biţi de paritate)
- fiecare bloc cifrat este independent de celelalte;
- nu este necesară sincronizarea între operaţiile de criptare/decriptare ale unui bloc;
- algoritmul T-DES (triplu DES) pentru creşterea securităţii
  - iterarea de trei ori a algoritmului DES
  - cheie de 168 biți

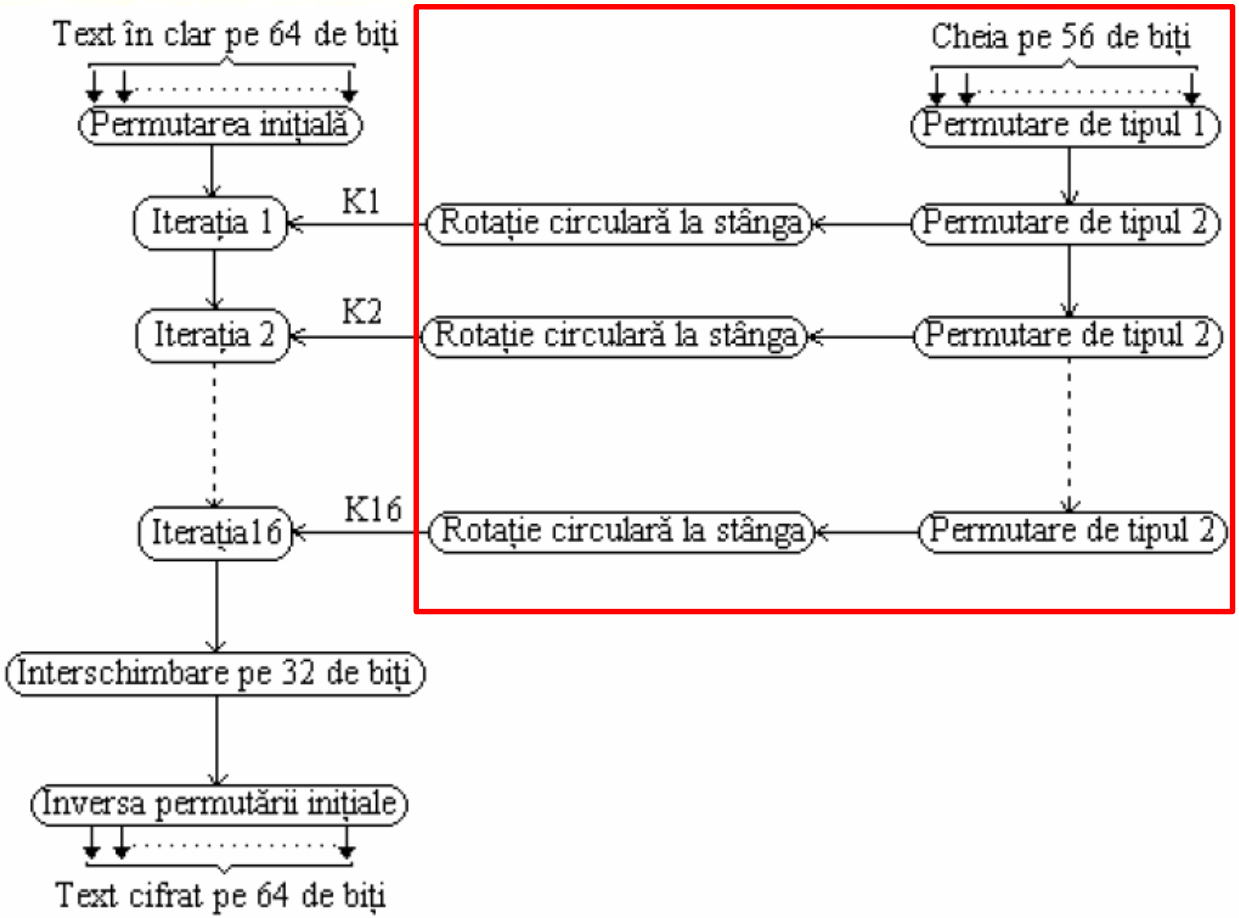
DES (Data Encryption Standard)



Operații pe bloc de 64 biți

- permutare inițială
- 16 iterații succesive
- o interschimbare pe 32 de biți
- inversa permutării inițiale

DES (Data Encryption Standard)



Operații pe cheia de 56 biţi

- permutare de tipul 1
- împărţire în două blocuri de 28 biţi.
- rotaţie circulară spre stânga cu un număr de biţi corespunzător numărului iteraţiei.

AES (Advanced Encryption Standard)

- Denumire originală: Rijndael (Vincent Rijmen and Joan Daemen)
- Câștigător în 2001 al procesului de selecție AES al National Institute of Standards and Technology (NIST)
- 3 variate: 128, 192, 256 biți

AES (Advanced Encryption Standard)

Caracteristici:

- 10-14 iterații (mai rapid ca 3DES)
- Acționează pe matrici de 4x4 bytes
- 4 transformări:
  - AddRoundKey – se adună cheia de rundă prin XOR
  - SubBytes – se substituie fiecare byte prin intermediul unei tabele de look-up (substituţie neliniară),
  - ShiftRows – se shiftează circular (rotire) fiecare linie
  - MixColumns – se amestecă coloanele prin aplicarea unei transformări de această dată liniară şi reversibilă (înmulțire matricială).