Tehnici criptografice

Criptare

- Criptografia = ştiinţa creării şi menţinerii mesajelor secrete, în sensul imposibiltăţii citirii lor de către neautorizaţi
- **M** = mesaj (text) în clar (plain / clear text) este mesajul ce urmează a fi secretizat
- **C** = mesaj cifrat (criptograma, cipher text) este mesajul secretizat, inaccesibil neavizaţilor
- **E** = criptare / cifrare este procedeul de ”ascundere” a unui mesaj în clar în mesajul secretizat.

$$E(M) = C$$

Criptare

- **D** = Decriptare / descifrare este procedeul de regăsire a mesajului în clar M din mesajul cifrat C

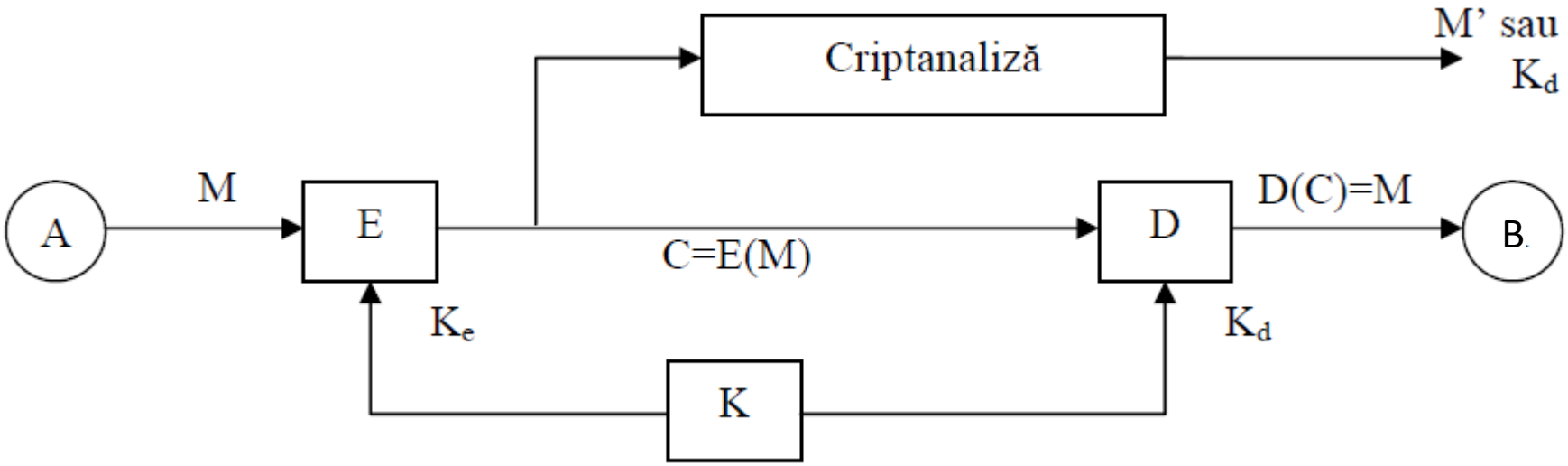
$$D(C) = D(E(M))=M$$

- *Algoritm criptografic / cifru* = funcţia matematică utilizată pentru criptare / decriptare (2 funcții)
- *Cheia criptografica (K)* = mărimea necesară realizării criptării şi decriptării
- *Criptosistem* este sistemul format din:
  - algoritm
  - toate mesajele în clar (M)
  - toate mesajele criptate (C)
  - toate cheile (K)

Criptare

- *Criptanaliza (cryptanalysis)* = ştiinţa spargerii cifrurilor, deci a obţinerii M sau K din C
- *Steganografia(steganography)* = tehnica ascunderii mesajelor secrete în alte mesaje, în aşa fel încât existenta mesajelor secrete să fie invizibilă

Schema bloc a unui criptosistem



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

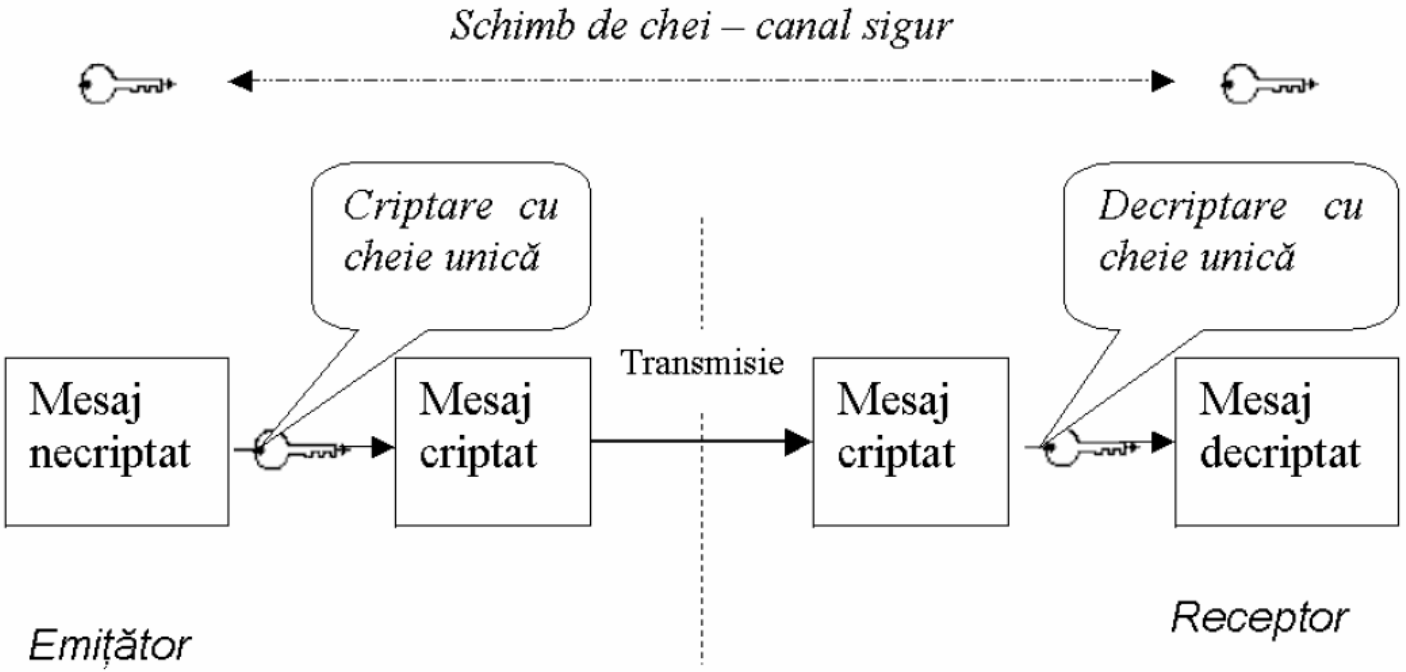
Obiectiv		Definire
Confidenţialitatea		păstrarea secretului pentru neavizaţi
Autentificarea	emiţător /identificare	legată de identitatea unei entităţi (persoană, terminal, carte de credit, etc.)
	originii datelor	legată de sursa de informaţie
	integrităţii datelor	asigură că informaţia nu a fost modificată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

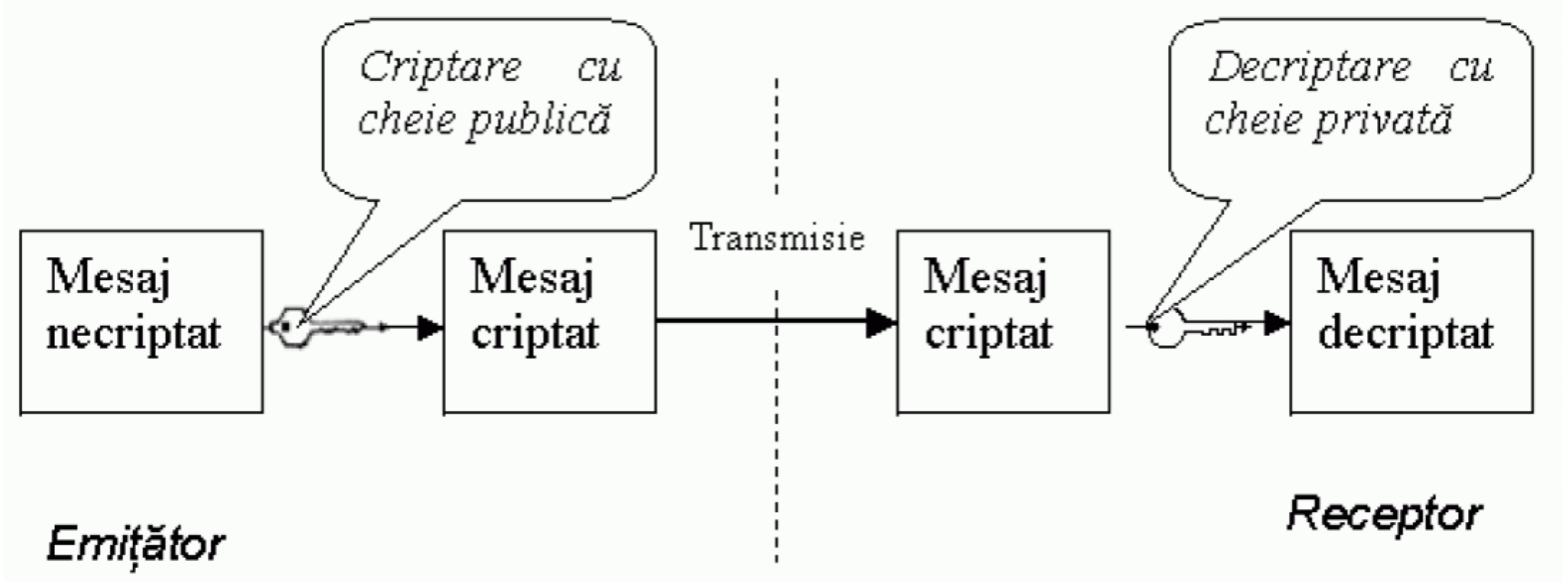
Clasificare*:*

- *cu cifruri bloc (block ciphers)*
  - Acționează pe subdiviziuni (blocuri)
  - lungimea tipică a blocurilor n=32 ÷ 128 biţi
  - substituţii şi transpoziţii, repetate iterativ
- *cu cifruri secvenţiale (stream ciphers):*
  - mesajul de la intrare = o succesiune (şir) de simboluri.
  - acționează simbol cu simbol
  - cheia K generată de un registru de deplasare cu reacţie (RDR) având starea iniţială S_0 controlată de o cheie compactă

Criptosisteme cu chei asimetrice

$$K_e \neq K_d$$

$$\begin{cases} E_{K_e}(M) = C \\ D_{K_d}(C) = M \end{cases}$$



Criptosisteme cu chei asimetrice

- E = funcţie neinversabilă cu trapă
- K_d = trapa care furnizează informaţia necesară calculării lui D

Exemple de funcţii neinversabile cu trapă

- Factorizarea unui produs de numere prime mari cu peste 100 de cifre zecimale (folosit în algoritmul RSA),
- găsirea logaritmului modulo un număr prim într-un câmp Galois GF(q) cu q foarte mare (folosit în algoritmii Rabin şi Diffie-Hellman)

Criptografia simetrică

- Clasificare:
  - 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

$$\alpha \rightarrow \mathrm{mod}\,26(\alpha + k)$$

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 frecvența cea mai mare de apariție) poate fi înlocuită cu F, * sau K

Criptografia simetrică - cifruri substituţie

3. Cifrul de substituţie poligramică

- se obţin substituind blocuri de caractere ale alfabetului primar – numite poligrame - 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 Vegenere**

- 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 permutări repetate sunt destul de complicate
- mecanizarea lor prin mașini rotor (1920)
- *maşina rotor* (rotor machine)
  - are o tastatură şi o serie de rotoare
  - Implementează o versiune a cifrului Vigénère.
  - 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 computaţională

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

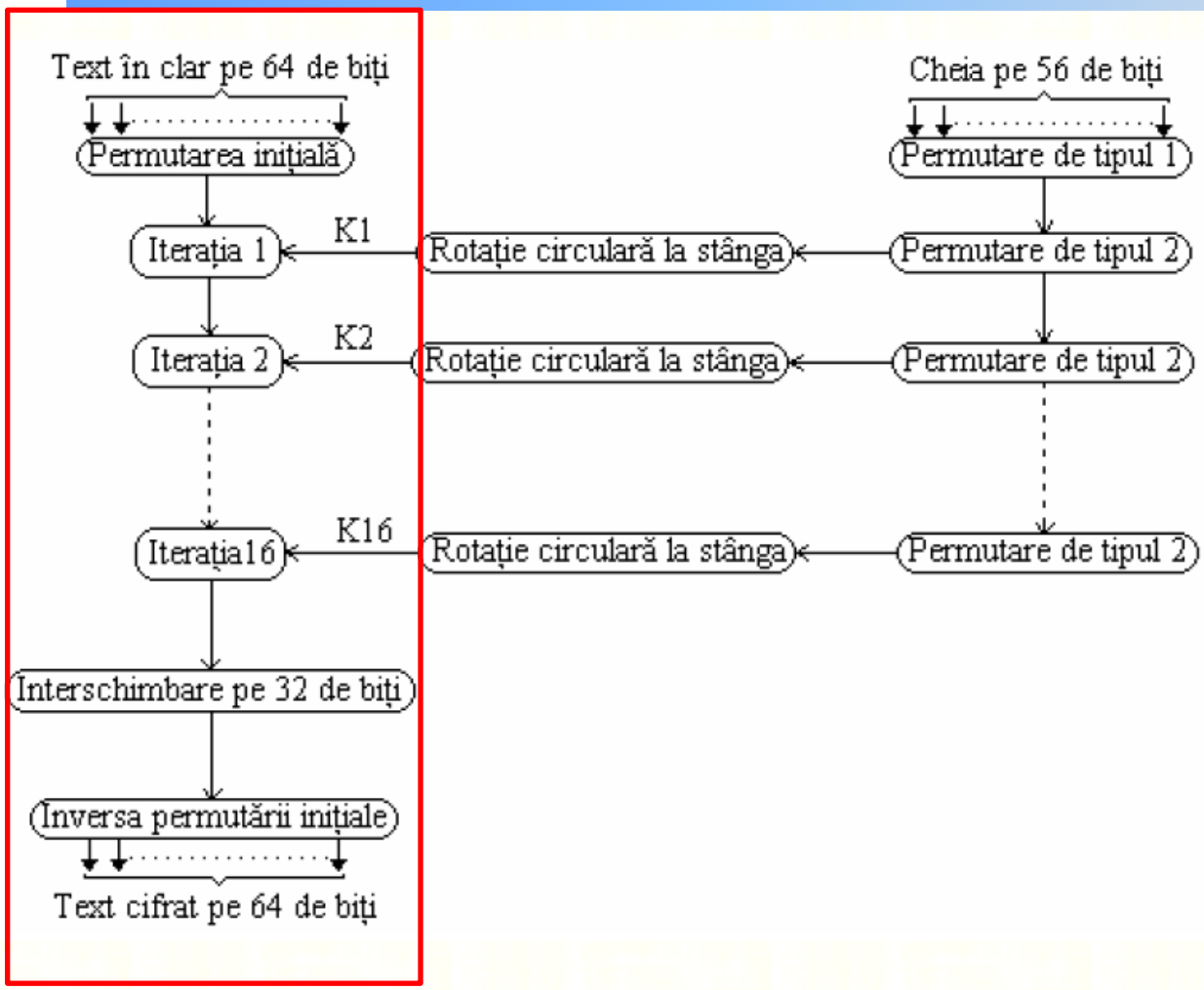
- dezvoltat de IBM în 1977
- Algoritm utilizat pe majoritatea platformelor UNIX, pentru criptarea parolelor
- Primul algoritm criptografic publicat

DES (Data Encryption Standard)

Caracteristici:

- lungimea unui bloc este de 64 de biţi
- cheia este pe 64 de biţi (8 sunt 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

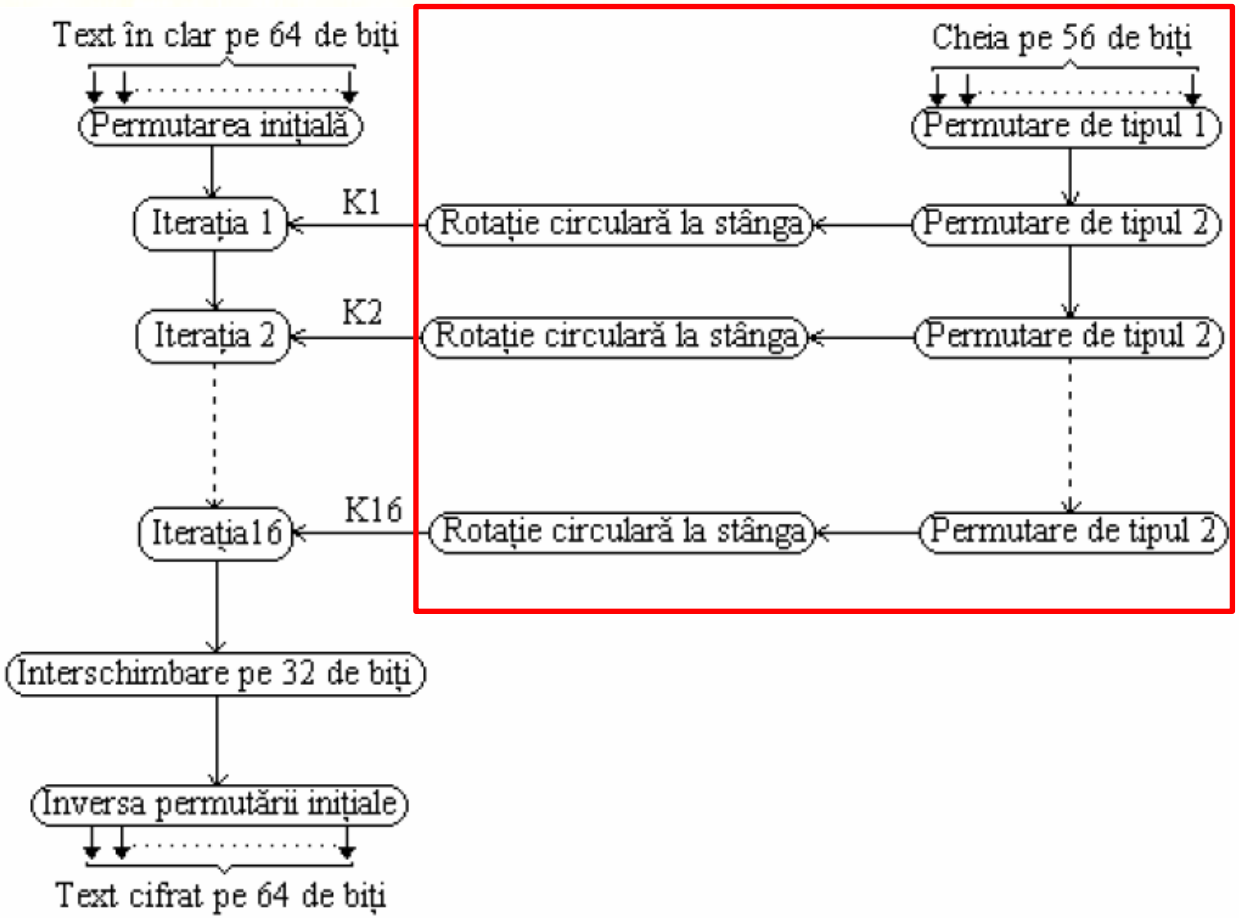
DES (Data Encryption Standard)



Operații pe bloc de 64 biți

- permutare iniţială
- 16 iteraţii succesive,
- o interschimbare pe 32 de biţi
- inversa permutării iniţiale

DES (Data Encryption Standard)



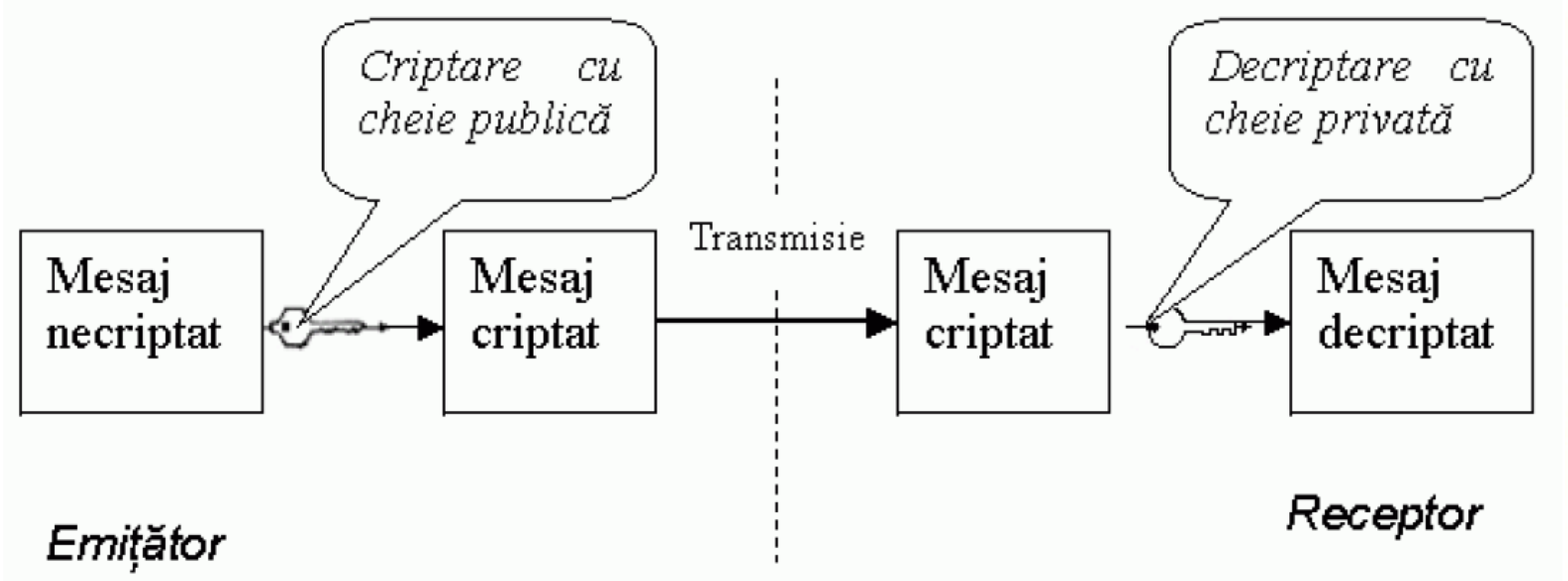
Operații pe cheia de 56 biţi

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

Criptografia asimetrică

$$K_e \neq K_d$$

$$\begin{cases} E_{K_e}(M) = C \\ D_{K_d}(C) = M \end{cases}$$



Criptografia asimetrică

- metodă de criptare publică
- cheie de criptare publică
- cheie de decriptare secretă
- decriptarea de către o terță parte durează foarte mult
- **Exemplu simplu:** carte de telefon dintr-un oraș mare

Criptografia asimetrică

Text clar	Nume ales	Text criptat
A	Asiminei	7134267
C	Cazacu	3214327
U	Ursanu	2653598
M	Moldovan	9767121
S	Scutaru	4002132
T	Tudor	2147877
A	Aliuță	1671873
U	Ursachi	2355510

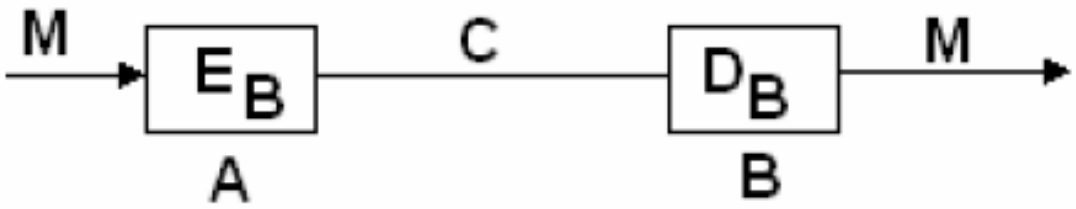
- receptor legal al mesajului trebuie să aibă o carte de telefon, cu numere aranjate în ordine crescătoare.
- Lista numerelor de telefon ordonate crescător constituie *trapa secretă*

Criptografia asimetrică

Funcția de protecție

- A doreşte să transmită M unui B
- A cunoaște cheia publică a lui B (E_B),
- transmite criptograma $C=E_B(M)$, asigurând astfel funcţia de protecţie
- La recepţie, B descifrează criptograma C utilizând transformarea D_B secretă:

$$D_B(C)=D_B(E_B(M))=M$$



Oricine poate trimite mesaje criptate lui B

Criptografia asimetrică

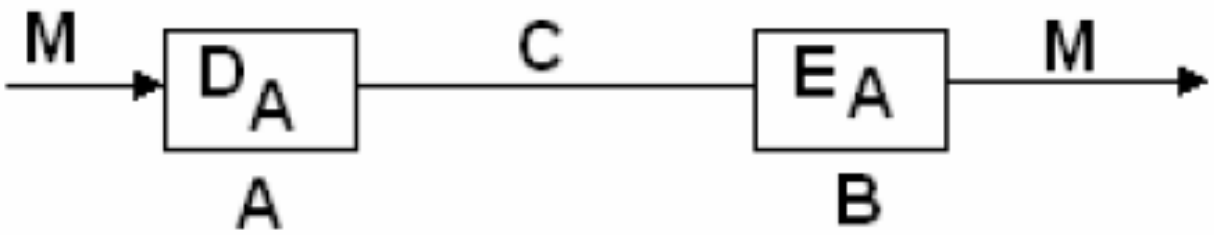
Funcția de autentificare

- se aplică lui M transformarea secretă D_A.
- Către B se va transmite:

$$C=D_A(M)$$

- La recepţie, B va aplica transformarea publică E_A corespunzătoare lui A:

$$E_A(C)=E_A(D_A(M)=M$$



Oricine poate decripta C

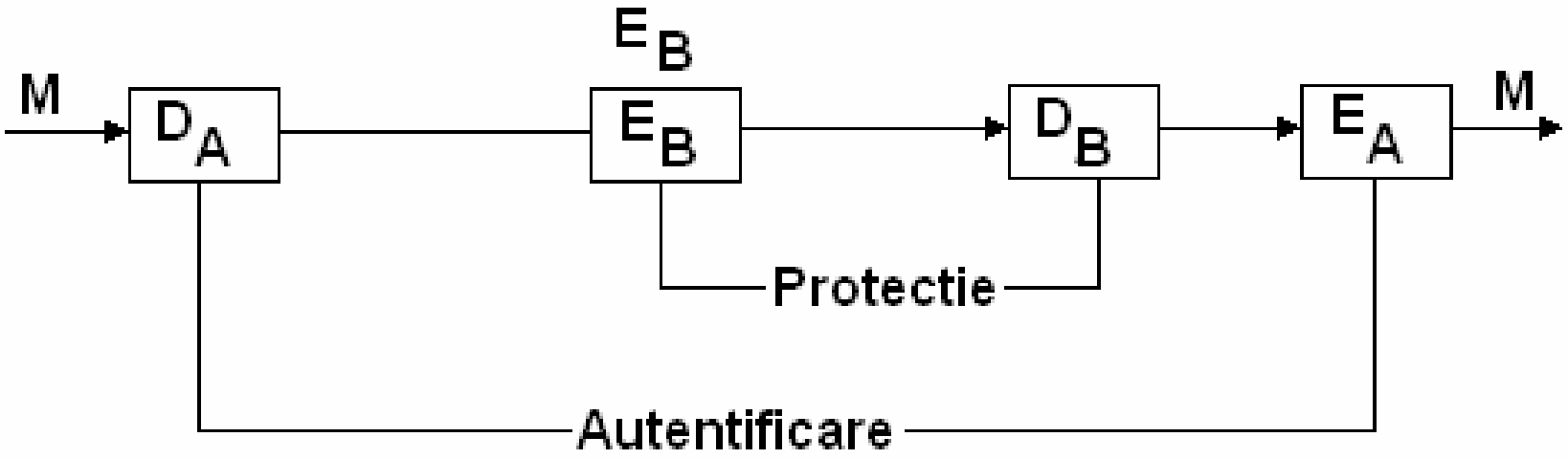
Criptografia asimetrică

Funcția de protecție și autentificare simultan

- spaţiul M trebuie să fie echivalent lui C astfel încât:

$$E_A(D_A(M))=D_A(E_A(M))=M$$

$$E_B(D_B(M))=D_B(E_B(M))=M$$



Criptografia asimetrică

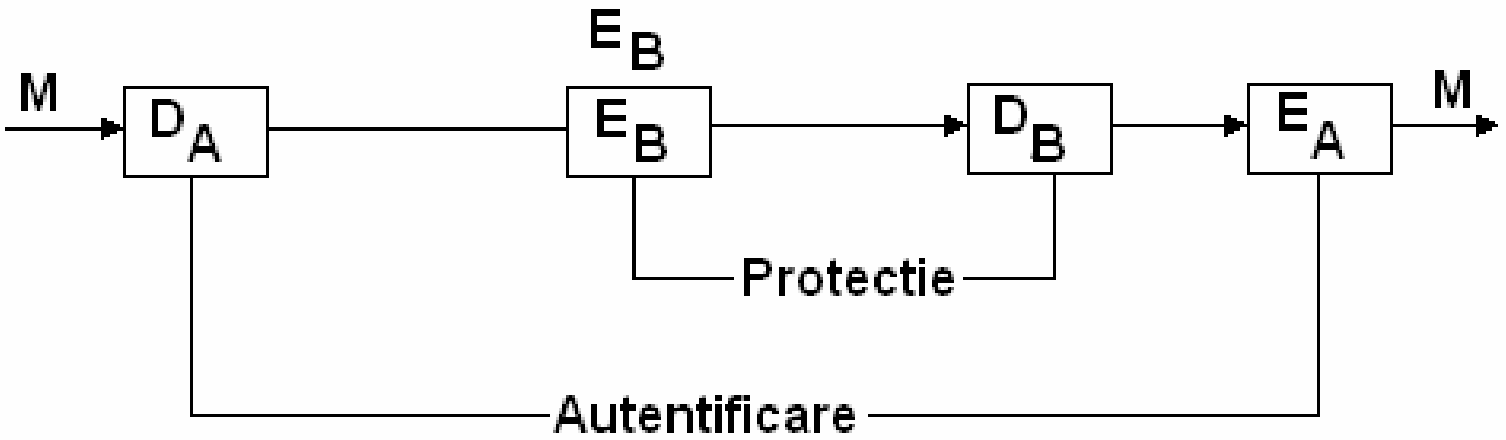
Funcția de protecție și autentificare simultan

- A aplică mai întâi transformarea secretă D_A, după care transmite lui B criptograma:

$$C=E_B(D_A(M))$$

- B aplică criptogramei propria funcţie de descifrare D_B şi apoi transformarea publică a lui A, E_A:

$$E_A(D_B(C)=E_A(D_B(E_B(D_A(M))))=E_A(D_A(M))=M$$



Criptografia asimetrică - semnătura digitală

- fie mesajul semnat de A, transmis către receptorul B.
- semnătura lui A trebuie să aibă următoarele proprietăţi:
  - B trebuie să fie capabil să valideze semnătura lui A;
  - să fie imposibil pentru oricine, inclusiv B, să falsifice semnătura lui A;
  - în cazul în care A nu recunoaşte semnătura unui mesaj M, să existe un „judecător” care să rezolve disputa dintre A şi B.

Criptografia asimetrică - semnătura digitală

- Protocolul semnăturii digitale se desfăşoară astfel:
  - A semnează M : $S=D_A(M)$;
  - A trimite lui B criptograma : $C=E_B(S)$;
  - B validează semnătura lui A, verificând dacă $E_A(S)=M$;

$$D_B(C)=D_B(E_B(S))=S$$

$$E_A(S)=E_A(D_A(M))=M$$

Sisteme de cifrare cu chei publice exponenţiale

Diffie şi Hellman - implementare practică

- utilizarea unor funcţii greu inversabile:
  - este uşor să se calculeze y din x, y=f(x);
  - există inversa funcţiei $x=f^{-1}(y)$;
  - este computaţional imposibilă determinarea inversei funcţiei
- funcţie greu inversabilă cu trapă dacă:
  - f^{-1} este uşor de calculat numai dacă se dispune de o informaţie numită **trapă**
  - necunoaşterea acestei informaţii face ca funcţia să fie greu inversabilă
- $(f, f^{-1}) = (E, D)$ a unui criptosistem cu chei publice

Sisteme de cifrare cu chei publice exponenţiale

- scheme bazate pe operaţii modulo n cu elemente din grupul ciclic al claselor de resturi modulo n

Câmp Galois

- GF(p^n) este un câmp finit cu p^n elemente cu p = număr prim
- mulţimea elementelor nenule ale câmpului Galois este un grup ciclic în raport cu operaţia de înmulţire

Sisteme de cifrare cu chei publice exponenţiale

- grup ciclic: clasele de resturi modulo p;
- dacă p = număr prim → $GF(p^n)$
- g = element generator (primitiv) al câmpului dacă $\{g^1, g^2, ..., g^{p-1}\}$ mod p = {1,2,...,p-1}
- Exemplu:
  - G = {0,1,2,3,4} este un $GF(5^1)$ cu adunarea modulo 5
  - elemente generatoroare: 2; 3

Schimbul de chei Diffie-Hellman

- A și B hotărăsc să folosească p=23 și g=5
- A alege un număr secret $\mathbf{X_A=6}$ și îi trimite lui B

  $Y_A = g^{XA} \bmod p$

  $Y_A = 5^{\mathbf{6}} \bmod 23 = 15.625 \bmod 23 = 8$
- B alege un număr secret $\boldsymbol{X_B}\mathbf{=15}$ și îi trimite lui A

  $Y_B = g^{XB} \bmod p$

  $Y_B = 5^{15} \bmod 23 = 30.517.578.125 \bmod 23 = 19$
- A calculează $\mathbf{s} = g^{XA\ XB} \bmod p = Y_B^{\ XA} \bmod p$

  $\mathbf{s} = 19^{\mathbf{6}} \bmod 23 = 47,045,881 \bmod 23 = \mathbf{2}$
- B calculează $\mathbf{s} = g^{XA\ XB} \bmod p = Y_A^{\ XB} \bmod p$

  $\mathbf{s} = 8^{\mathbf{15}} \bmod 23 = 35.184.372,088.832 \bmod 23 = \mathbf{2}$

Schimbul de chei Diffie-Hellman

- A și B au acum un secret: **s** = **2**
- deoarece 6*15 = 15*6.
- C (atacator) are la dispoziție Y_A și Y_B și trebuie să calc.:

  s = $g^{XA\ XB} \bmod p = Y_B^{XA} \bmod p = Y_A^{XB} \bmod p$
- deci trebuie să rezolve una dintre ecuațiile:

  $Y_A = g^{XA} \bmod p \rightarrow 5^{XA} \bmod 23 = 8$

  $Y_B = g^{XB} \bmod p \rightarrow 5^{XB} \bmod 23 = 19$

Schimbul de chei Diffie-Hellman

- *p*= număr prim pe 300 digiți și X_A și X_B pe 100 digiți
- *g* nu trebuie să fie mare (de regulă 2 sau 5)

  → X_A sau X_B nu pot fi calculați nici dacă am avea la dispoziție toată puterea de calcul a omenirii
- "Problema logaritmului discret"

Cifrul Rivest-Shamir Adleman (RSA)

- cel mai larg utilizat şi verificat criptosistem cu chei publice
- una dintre cele mai sigure metodă de cifrare şi autentificare disponibilă comercial
- Idee:
  - uşor să înmulţeşti două numere prime mari
  - extrem de greu să se factorizeze produsul lor
- produs - public şi utilizat ca o cheie de criptare
- numerele prime - necesare pentru decriptare

Cifrul Rivest-Shamir Adleman (RSA)

- p şi q două numere prime mari distincte şi aleatoare (având ~100 cifre zecimale)

$$n = pq$$

- Φ = funcţia totient a lui Euler
- $\Phi(n)$ = nr. de întregi nenegativi mai mici decât n care sunt relativ primi cu n

n	$\phi(n)$	n	$\phi(n)$	n	$\phi(n)$
1	0	10	4	19	18
2	1	11	10	20	8
3	2	12	4	21	12
4	2	13	12	22	10
5	4	14	6	23	22
6	2	15	8	24	8
7	6	16	8	25	20
8	4	17	16	26	12
9	4	18	6	27	18

Cifrul Rivest-Shamir Adleman (RSA)

- Cateva valori importante ale lui $\Phi(n)$ *:*

n	$\Phi(n)$	Condiții
p	p-1	p – prim
p^n	$p^n - p^{n-1}$	p – prim
$s*t$	$\Phi(s)\ \Phi(t)$	c.m.m.d.c.(s,t)=1
$p*q$	(p-1) (q-1)	*p,q - prime*

Cifrul Rivest-Shamir Adleman (RSA)

- Se alege un număr aleator mare $D>1$ astfel încât

$$\text{c.m.m.d.c.}(D,\Phi(n)) = 1$$

- se calculează numărul E , $1<E<\Phi(n)$ care să satisfacă:

$$ED(\text{mod}\Phi(n)) = 1$$

- n = modulul de criptare/decriptare
- E = exponentul de criptare
- D = exponentul de decriptare
- (n,E) = cheia publică de criptare
- $(p, q, \Phi(n),D)$ = trapa secretă (ajunge p)

Cifrul Rivest-Shamir Adleman (RSA)

- **Criptarea RSA:**

$$C = M^E (\text{mod } n)$$

- **Decriptarea RSA:**

$$M = C^D (\text{mod } n)$$

- **Pentru ca algoritmul să funcționeze:**

$$M = C^D (\text{mod n}) = M^{ED} (\text{mod n})$$

Cifrul Rivest-Shamir Adleman (RSA)

Demonstrație:

- Deoarece $ED(\text{mod } \Phi(n))=1$

  $ED = k\Phi(n)+1 = k(p-1)(q-1)+1$

  $M^{ED}(\text{mod } n) = M^{k(p-1)(q-1)+1} (\text{mod } n) = MM^{k(p-1)(q-1)} (\text{mod } n)$
  $= [M(\text{mod } n)\, M^{k(p-1)(q-1)} (\text{mod n})](\text{mod } n)$

Teorema lui Fermat: Dacă p este prim si p nu divide pe a atunci $a^{p-1} (\text{mod } p) = 1$

→ $M^{k(p-1)(q-1)} (\text{mod } n) = 1 (\text{mod } n)$

→ $M^{ED}(\text{mod } n) = M (\text{mod } n)$

Cifrul Rivest-Shamir Adleman (RSA)

- $n=pq$, unde p,q – numere prime mari
- $\Phi(n)=(p-1)(q-1)$
- greu de determinat p,q având la dispoziţie n
- (E, n) cheia publică;
- (D, n) cheia secretă;

Cifrul Rivest-Shamir Adleman (RSA)

Exemplu

- alegem p=47 şi q=79 prime
- $n = pq =$ 3713
- alegem D=47 (trebuie ca c.m.m.d.c.(D, (p-1)(q-1)) = 1)
- E trebuie să satisfacă: ED = 1(mod(p-1)(q-1))

  → E = [(p-1)(q-1)+1]/D = 37
- dorim să codăm mesajul „A sosit timpul”
- Codăm fiecare literă a alfabetului:

  A=00, B=01,...,Y=25, Z=26, spațiu=27

Cifrul Rivest-Shamir Adleman (RSA)

Exemplu

- M=„A sosit timpul”
- M=0018 1418 0819 1908 1215 2011
- Codăm fiecare grup de 4:

$0018^E \pmod n = 0018^{37} \pmod{3713} = 3091$

$1418^E \pmod n = 1418^{37} \pmod{3713} = 0943$

$0819^E \pmod n = 0819^{37} \pmod{3713} = 3366$

$1908^E \pmod n = 1908^{37} \pmod{3713} = 2545$

$1215^E \pmod n = 1215^{37} \pmod{3713} = 0107$

$2011^E \pmod n = 2011^{37} \pmod{3713} = 2965$

→ C = 3091 0943 3366 2545 0107 2965

Cifrul Rivest-Shamir Adleman (RSA)

Exemplu

- C = 3091 0943 3366 2545 0107 2965
- la decriptare se vor calcula:

  $3091^{D} \pmod{n} = 3091^{47} \pmod{3713} = 0018$

  $0943^{D} \pmod{n} = 0819^{47} \pmod{3713} = 1418$

  ……

- Mesajul decriptat:

  M=0018 1418 0819 1908 1215 2011

- dacă *n, D, E* pe 512 biţi sistemul este deocamdată imposibil de spart