TEMA 7.
Algoritmi de criptare cu cheie publică

Cuprins

- Criptosisteme cu cheie publică
- Canalul RSA

CRIPTOSISTEME CU CHEIE PUBLICĂ

In 1976, **W. Diffie și M. Hellman** au descoperit un sistem revoluționar de criptare a informației, criptografia cu cheie publică.

- Necesită o comunicare prealabilă partenerilor, pentru stabilirea cheilor;
- Permit doar un număr limitat de participanți datorită numărului mare de chei necesare;
- Cheile trebuiesc schimbate frecvent, eventual la fiecare comunicare.

Avantaje

- Pot fi proiectate pentru a cripta mesaje în clar foarte mari;
- Cheile sunt relativ scurte (128 b);
- Pot fi utilizate pentru construcția unor mecanisme criptografice diverse;

- Pot fi compuse pentru a obține sisteme de criptare puternice;
- Doar cheia de decriptare trebuie păstrastă secretă;
- Aceeași pereche de chei poate fi utilizată pentru perioade lungi de timp;

- Numărul perechilor de chei necesare crește liniar în raport cu numărul utilizatorilor;
- Permit construcția unor protocoale de semnătură digitală.

Dezavantaje:

- Ambele chei trebuie să rămână secrete;
- Numărul cheilor necesare crește pătratic în raport cu numărul utilizatorilor;
- Cheile trebuiesc schimbate frecvent (eventual la fiecare comunicare);

- Mecanismele de semnătură digitală necesită chei mari;
- Viteza algoritmilor de criptare este de câteva ori mai mică;
- Lungimea cheilor este mult mai mare, pentru un nivel de securitate;

- Comparabil necesită un sistem de autentificare a cheilor efficient;
- Nici un criptosistem cu cheie publică nu a fost certificat, matematic.

Intr-un sistem cu cheie publică, un utilizator deţine două chei:

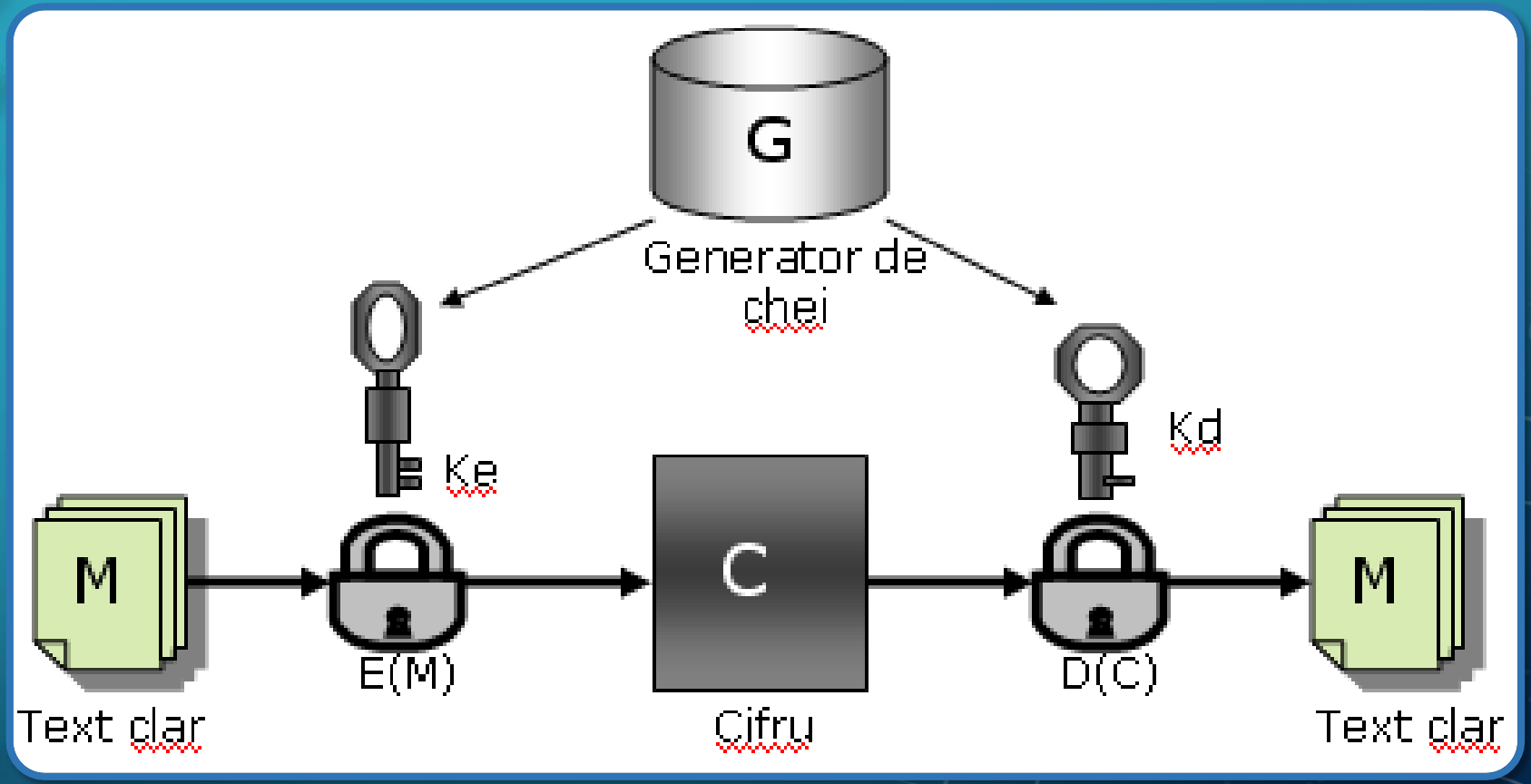
1. O cheie publică - **SK**
2. O cheie privată - **PK**

$$m = d(SK, e(PK, m))$$

$$m = d(PK, e(SK, m))$$

- *Generatorul de chei*, care returnează i pereche cheie secretă-cheie publică (SK, PK);
- *Algoritmul de criptare*, care primeşte la intrare un mesaj *m* din mulţimea mesajelor posibile, o cheie publică PK şi returnează criptotextul *c*.

Algoritmul de decriptare, care ia ca intrare un text cifrat *c* din mulţimea textelor cifrate, o cheie secretă *SK* şi returnează un mesaj *m*.


G
Generator de chei
Ke
Kd
M
E(M)
C
D(C)
M
Text clar
Cifru
Text clar

- *Receptorul B* poate uşor să genereze cheia publică PK_B şi cheia privată SK_B.

- *Emiţătorul A*, ştiind cheia publică a lui *B* şi mesajul clar *m*, poate să genereze textul cifrat corespunzător:

$$c = e_{pk_B}(m)$$

- *Receptorul B* poate uşor să decripteze textul cifrat *c*:

$$m = d_{Sk_B(c)} = d_{Sk_B\left(e_{pk_B(m)}\right)}$$

- Un atacator care ştie PK_B nu poate să determine cheia private SK_B.

- Un atacator care ştie cheia publică PK_B şi textul cifrat *c* nu poate să determine mesajul original *m*.
- **Are loc următoarea relație:**

$$m = d_{Sk_B(c)} = d_{Sk_B\left(e_{pk_B(m)}\right)}$$

- **Sistemul RSA:** se bazează pe dificultatea descompunerii în factori primi a numerelor mari
- **Sistemul El Gamal:** se bazează pe dificultatea calculului logaritmului discret intr-un corp finit
- **Sistemul Merkle-Hellman:** primul sistem definit cu cheie publică, bazat pe problema {0, 1} a rucsacului

- **Sistemul McEliece:** este bazat pe teoria algebrică a codurilor, decodificarea unui cod linear

- **Curbe eliptice:** Sunt sisteme de criptare care îşi desfăşară calculele pe mulţimea punctelor unei curbe eliptice

Întrebare de control

- Enumerați **algoritmii** de criptare cu cheie publică:...?
- În ce caz **aplicați** cheile publice și private?

ALGORITMUL DIFFIE-HELMAN

Algoritmul Diffie-Hellman:

- Este un algoritm de generare a unei chei simetrice între 2 părţi (A și B) folosind un canal nesigur şi fără vre-o cunoştinţă iniţială;
- Acest algoritm nu criptează date.

Alice

Bob

a, p, α

A = α^{α} (mod p)

k = B^{α} (mod p)

a, p, A

A

b

B = α^{b} (mod p)

k = A^{b} (mod p)

- Alice şi Bob convin asupra lui $p = 23$ şi $\alpha = 5$.
- Alice alege aleatoriu $a = 6$ şi trimite lui Bob $A = 5^6 \bmod 23 = 8$.
- Bob alege aleatoriu $b = 15$ şi trimite lui Alice $5^{15} \bmod 23 = 19$.

- Alice calculează $19^6 \ mod \ 23 = 2$.
- Bob calculează $8^{15} \ mod \ 23 = 2$.
- Alice şi Bob au abţinut aceleşi rezultat, deci cheia secretă comună este ***k* = 2**.

Întrebare de control

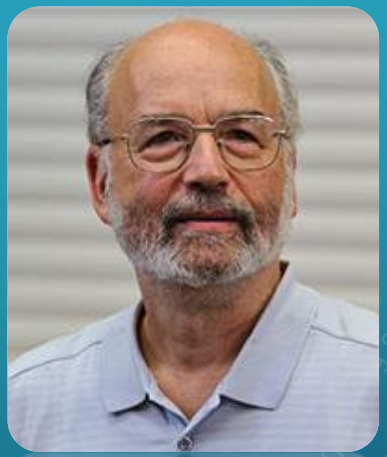
- Determinați proprietatea pe care se bazează aloritmul Diffie Hellman?
- Enumerați cazurile când poate fi utilizat Algoritmul Diffie-Hellman:...?

CANALUL RSA

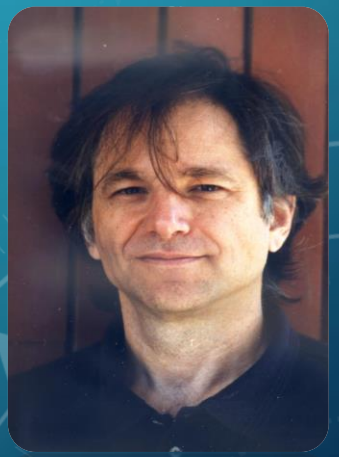
Apărut în 1977 de:

R. L. Rivest,

A. Shamir,



L. M. Adleman



Sistemul *RSA*:

Se bazează pe dificultatea descompunerii în factori primi a numerelor mari (de sute de cifre).

Alice

Bob

Cheie

Cheie

Mesaj

Criptare

Descriptare

Mesaj

Eve

Bob

Cheia secretă

Generator Key

Descriptare

Mesaj

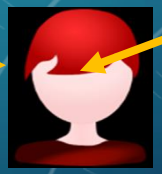
Alice

Cheie publică

Cheie publică

Mesaj

Criptare



Eve

Generarea cheilor

1. Generaţi 2 numere prime *p* şi *q* cât mai mari
2. Fie *n = p * q*
3. Fie *m = (p-1)*(q-1)*
4. Alegeţi e astfel încât *cmmdc(e,m) = 1*
5. Găsiţi *d* astfel încât *(d*e) mod m = 1*

Criptarea mesajelor RSA

- *B* primește cheia de criptare a lui *A* $K^{eA} = (e_A, n_A)$
- *B* reprezintă mesajul ca un număr natural $0 \leq m \leq n_A - 1$
- *B* calculează $c := m^{eA} \pmod{n_A}$
- *B* trimite *c*

Decriptarea mesajelor RSA

- A prime¸ste mesajul criptat c
- A calculeaza $m' = c^{d_A} \ (mod \ n^A)$ (utilizând cheia de decriptare K_{d_A} care este cunoscută doar de A)

1. p = 7, q = 19

2. Fie n = p * q
   n= 7 * 19
   n = 133

3. Fie m = (p-1)*(q-1)
   m = (7-1)*(19-1)
   m = 6 * 18
   m = 108

p = 7, q = 19

n = 133, m = 108

e = ?

d = ?

Cheia publica = (e,n) = ?

Cheia privata = (d,n) = ?

4. Alegeţi e astfel încât cmmdc(e,m) = 1

e = 2 => cmmdc(e, 108) = 2 (NU)

e = 3 => cmmdc(e, 108) = 3 (NU)

e = 4 => cmmdc(e, 108) = 4 (NU)

e = 5 => cmmdc(e, 108) = 1 (DA)

p = 7, q = 19

n = 133, m = 108

e = 5

d = ?

Cheia publica = (e,n) = ?

Cheia privata = (d,n) = ?

5. Găsiţi *d* astfel încât (d*e) % m = 1 sau
d*e = 1 + x*m

(unde x poate fi orice număr întreg)
=> d = (1 + x*m)/e

x = 0 => d = 1/5 (NU)
x = 1 => d = 109/5 (NU)
x = 2 => d = 217/5 (NU)
x = 3 => d = 325/5 (DA)

d = 65

p = 7, q = 19

n = 133, m = 108

e = 5

d = 65

Cheia publica = (e,n) = (5,133)

Cheia privata = (d,n) = (65,133)

Întrebare de control

- Ce funcție poate fi aplicată la calculul numerelor prime?
- Enumerați pașii de alegerea cheilor...?
- Enumerați pașii de criptarea și decriptarea mesajelor...?

ÎNTREBĂRI RECAPITULATIVE

- Enumerați algoritmii de criptare cu cheie publică:...?
- În ce caz aplicați cheile publice și private?

- Determinați proprietatea pe care se bazează aloritmul Diffie Hellman?
- Enumerați cazurile când poate fi utilizat Algoritmul Diffie-Hellman:...?

ALGORITMI DE CRIPTARE CU CHEIE PUBLICĂ