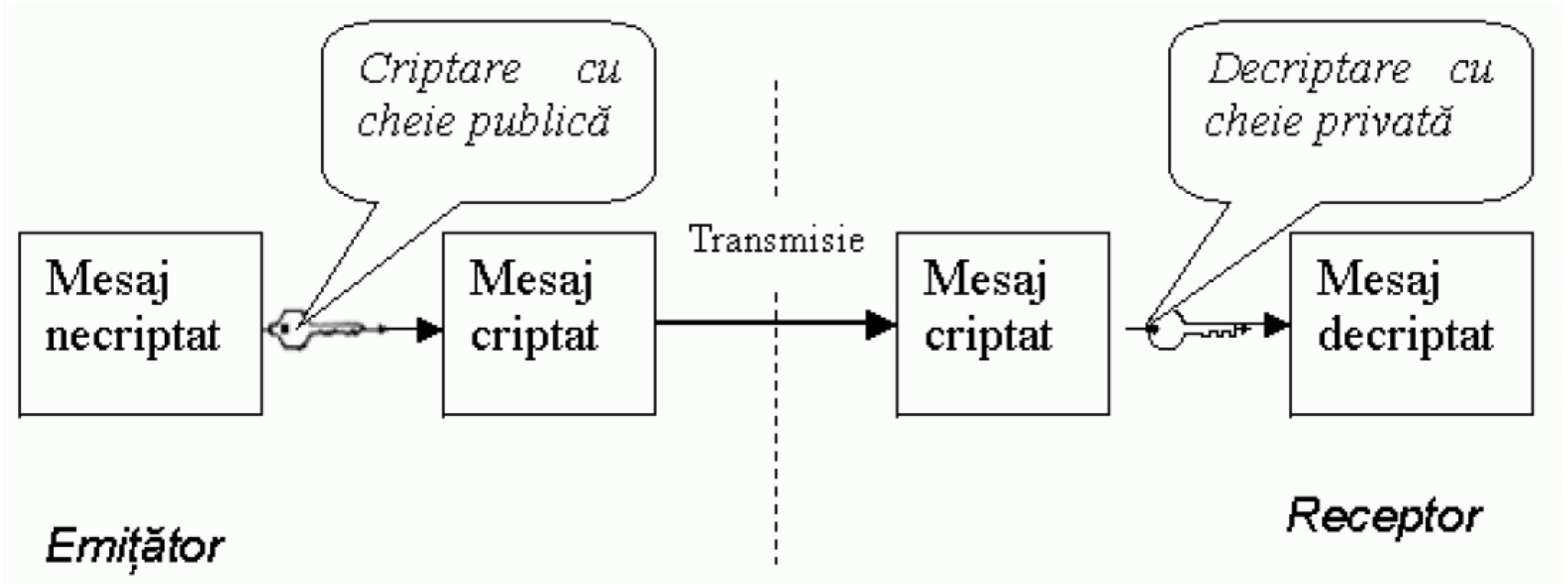
Criptografia asimetrică

$$K_e \neq K_d$$

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



Criptografia asimetrică

- metodă de criptare publică
- cheie de criptare publică
- cheie de decriptare secretă
- decriptarea de către o terță parte durează foarte mult

Criptografia asimetrică

E = funcţie neinversabilă cu trapă

K_d = trapa care furnizează informaţia necesară calculării lui D

Exemplu simplu: carte de telefon dintr-un oraș mare

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

Alte exemple de funcţii neinversabile cu trapă:

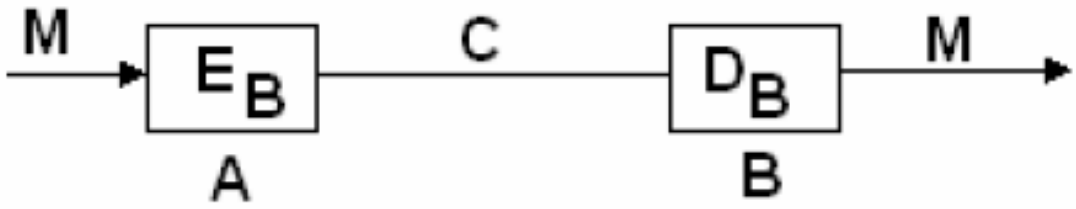
- Factorizarea unui produs de numere prime mari cu peste 100 de cifre zecimale (folosit în algoritmul RSA),
- găsirea logaritmului modulo un număr prim într-un câmp Galois $GF(q^n)$ cu q foarte mare (folosit în algoritmii Rabin şi Diffie-Hellman)

Criptografia asimetrică

Funcția de protecție

- A doreşte să transmită M unui B
- A cunoaște cheia publică a lui B (E_B),
- transmite criptograma $C=E_B(M)$
- 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

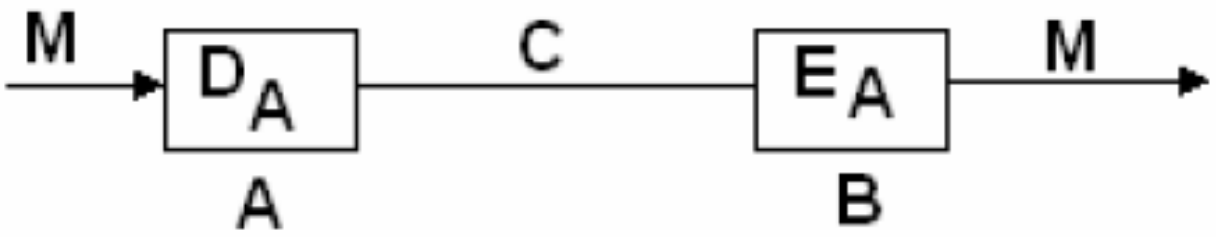
Funcția de autentificare

- 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

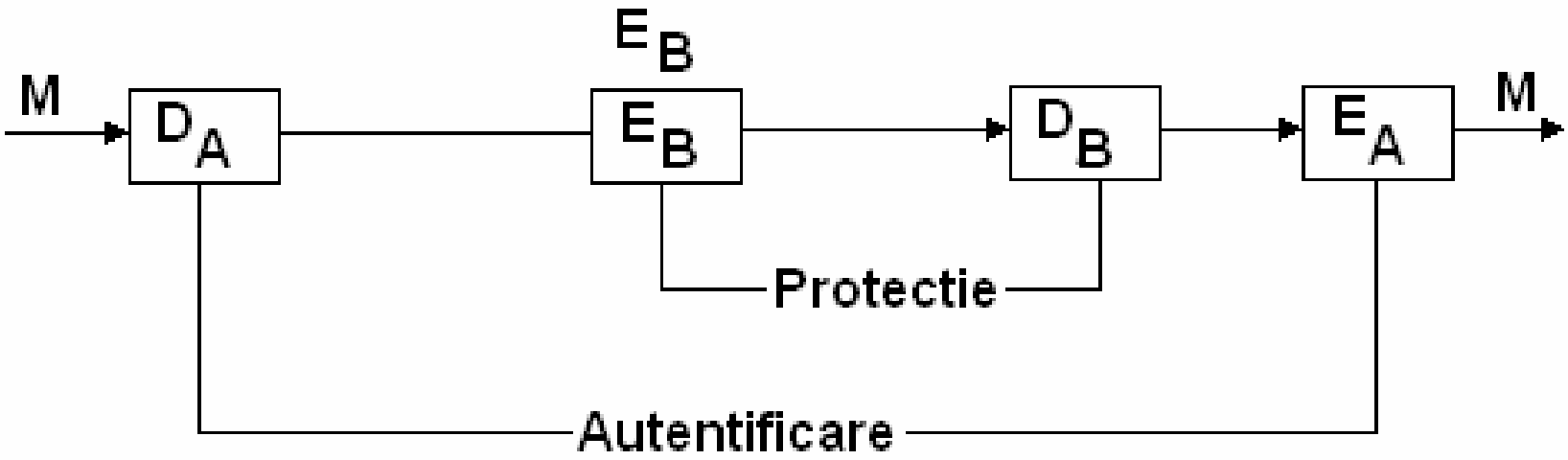
Criptografia asimetrică

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

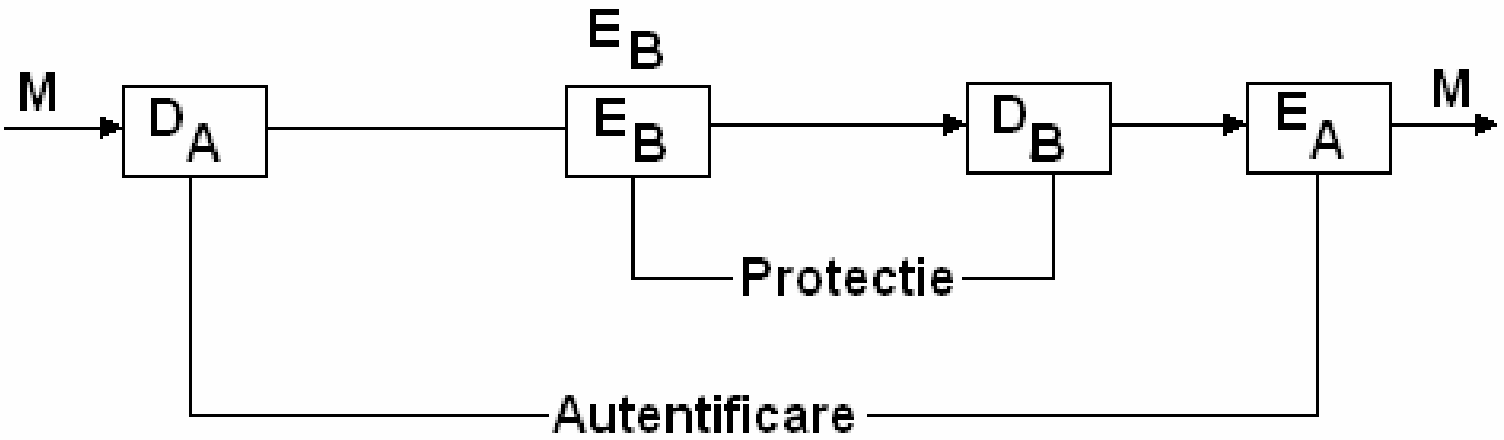
Funcția de protecție și autentificare simultan

- 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

- 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 y
- 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
- $(f, f^{-1}) = (E, D)$ ale 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 $GF(5^1)$
  - 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 **X_A=6** și îi trimite lui B

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

  $Y_A = 5^{6} \bmod 23 = 15.625 \bmod 23 = 8$
- B alege un număr secret ***X_B*=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 **s** = $g^{XA\ XB} \bmod p = Y_B^{XA} \bmod p$

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

  s = $8^{15} \bmod 23 = 35.184.372,088.832 \bmod 23 =$ **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)

- $n=pq$, 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: $ED = 1(\mathrm{mod}(p-1)(q-1))$

  → $E = [(p-1)(q-1)+1]/D = 37$
- 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 mai mult de 768 biţi sistemul este deocamdată imposibil de spart

Cifrul Rivest-Shamir Adleman (RSA)

- dacă *n* pe mai mult de 768 biţi sistemul este deocamdată imposibil de spart
- RSA-768 a fost spart în 2009 pe durata a 2 ani folosind multe computere în paralel
- Echivalentul a 2000 de ani de calcul folosind un computer cu procesor la 2,2 GHz