CRIPTOGRAFIE APLICATĂ

Conf.univ.dr. Radu Boriga

SISTEME DE CRIPTARE ASIMETRICE (CU CHEIE PUBLICĂ)

- Ideea inovatoare de a utiliza o **cheie publică** pentru procesul de criptare şi o **cheie secretă** pentru procesul de decriptare se consideră că a fost propusă de către cercetătorii **Whitfield Diffie** şi **Martin Hellman** în anul 1976.

- **Primul sistem de criptare cu cheie publică** se consideră că a fost realizat în anul 1977 de către **Ron Rivest**, **Adi Shamir** şi **Leonard Adleman** de la Massachusetts Institute of Technology (MIT), fiind în prezent cel mai cunoscut și mai utilizat sistem de criptare asimetric.

- În realitate, matematicienii **James Ellis**, **Clifford Cocks** și **Malcolm Williamson** de la Government Communications Headquarters (GCHQ) din Marea Britanie au conceput primul sistem de criptare cu cheie publică între anii 1970 și 1974, însă acest lucru a rămas secret până în anul 1997!

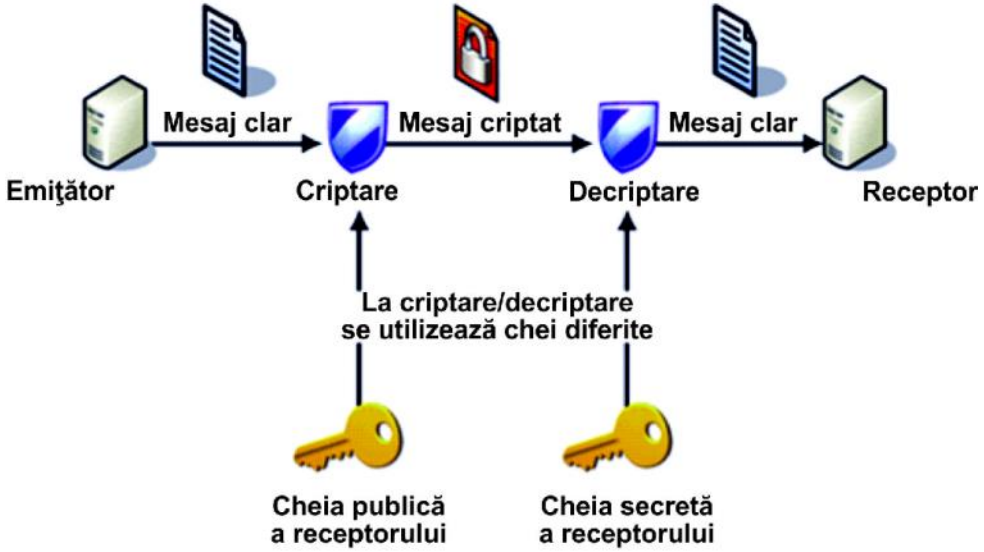
- Confidenţialitatea datelor într-o schemă de criptare asimetrică este asigurată de faptul că este imposibil de obţinut din punct de vedere computaţional cheia secretă utilizată pentru decriptarea datelor din cheia publică utilizată pentru criptarea datelor.

SISTEME DE CRIPTARE ASIMETRICE (CU CHEIE PUBLICĂ)

- Într-o schemă de criptare cu cheie publică, fiecare utilizator deţine câte o pereche de chei (K_{pub}, K_{priv}), cheia de criptare, K_{pub} fiind publică.

- În cazul în care utilizatorul A doreşte să transmită un mesaj secret M lui B, acesta va folosi cheia publică a lui B, obţinând mesajul criptat $C = K_{pub}^{B}(M)$.

- La decriptare, utilizatorul B foloseşte cheia sa secretă K_{priv}^{B} pentru a obţine mesajul clar $M = K_{priv}^{B}(C)$.



- **Sistemele asimetrice nu asigură autentificarea datelor**, deoarece cheia de criptare utilizată K_{pub}^{B} este publică, ceea ce permite altui utilizator să-i trimită un mesaj fals utilizatorului B în numele utilizatorului A!

- Pentru a se asigura şi autentificarea utilizatorului A, acesta va aplica mai întâi cheia sa secretă K_{priv}^{A} asupra textului clar M, după care va aplica cheia publică K_{pub}^{B} a lui B, obţinându-se textul criptat:

$$C = K_{pub}^{B}(K_{priv}^{A}(M))$$

- Utilizatorul B va aplica mai întâi cheia sa secretă K_{priv}^{B} asupra textului criptat C, iar apoi cheia publică K_{pub}^{A} a lui A, obținând textul clar M:

$$K_{pub}^{A}\left(K_{priv}^{B}(C)\right) = K_{pub}^{A}\left(K_{priv}^{B}\left(K_{pub}^{B}(K_{priv}^{A}(M))\right)\right) = K_{pub}^{A}\left(K_{priv}^{A}(M)\right) = M$$

- Această metodă poartă numele de **semnătură digitală**, fiind utilizată pentru autentificarea utilizatorilor.

- În funcţie de problemele greu rezolvabile pe care se bazează, sistemele de criptare cu cheie publică se împart în următoarele categorii:
  - **sisteme cu cheie publică bazate pe probleme NP-complete:** Merkle-Hellman
  - **sisteme cu cheie publică bazate pe dificultatea factorizării întregilor:** RSA
  - **sisteme cu cheie publică bazate pe dificultatea problemei logaritmului discret:** ElGamal
  - **sisteme cu cheie publică bazate pe grupuri de curbe eliptice:** Koblitz-Miller

- Principalul avantaj al sistemelor de criptare cu cheie publică îl constituie stocarea cheii secrete într-un singur loc (la receptor).

- Principalul dezavantaj al sistemelor de criptare cu cheie publică îl constituie timpul de criptare/decriptare mult mai mare decât cel necesar sistemelor de criptare simetrice, indus de utilizarea operaţiilor cu numere întregi foarte mari.

➢ Algoritmul de generare a cheilor:

1. Se selectează două numere naturale prime p şi q
2. Se calculează produsul $n = p * q$
3. Se calculează indicatorul lui Euler $\Phi(n) = (p-1) * (q-1)$
4. Se selectează un număr natural e astfel încât:

$$cmmdc(\Phi(n), e) = 1, \qquad 1 < e < \Phi(n)$$

5. Se determină numărul natural d astfel încât $e * d \equiv 1 \pmod{\Phi(n)}$
6. Cheia publică este perechea (e, n), iar cheia privată este perechea (d, n)

➢ Algoritmul de semnare:

- Presupunem că un utilizator A are cheia publică (e, n) și cheia privată (d, n)
- Utilizatorul A semnează un mesaj M și i-l transmite utilizatorului B astfel:

1. codifică mesajul clar M sub forma unui număr cuprins între 0 și $n-1$
2. calculează semnătura S a mesajului M folosind relația $S = M^d \pmod n$
3. trimite perechea (M, S) utilizatorului B

➢ Algoritmul de verificare:

- Utilizatorul B recepționează perechea (M, S) și verifică autenticitatea mesajului M astfel:

1. obține cheia publică (e, n) a utilizatorului A
2. calculează $M' = S^e \pmod n$
3. verifică faptul că $M' = M$

➢ Exemplu:

1. Fie $p = 5$ şi $q = 11$
2. Se calculează produsul $n = p * q = 55$
3. Se calculează indicatorul lui Euler $\Phi(55) = 4 * 10 = 40$
4. Se selectează un număr natural $1 < e < 40$ astfel încât:

$$cmmdc(40, e) = 1 \Rightarrow e = 7$$

5. Se determină numărul natural d astfel încât $7 * d \equiv 1 \pmod{40} \Rightarrow d = 23$
6. Cheia publică este perechea $(7{,}55)$, iar cheia privată este perechea $(23{,}55)$
7. Mesajul $M = 17$ are semnătura $S = 17^{23} \pmod{55} = 18$
8. Se calculează $M' = 18^{7} \pmod{55} = 17 \Rightarrow M' = M \Rightarrow$ mesajul M este autentic

➢ Algoritmul de generare a cheilor:

1. Se selectează un număr natural prim p și un generator g al grupului $\mathbb{Z}_p^*$

2. Se selectează un număr $x \in \mathbb{Z}_{p-1}^*$ și se calculează $y = g^x (\mathrm{mod}\, p)$, deci $x = \log_g y$

3. Cheia publică este tripletul (p, g, y), iar cheia privată este numărul x

➢ Algoritmul de semnare:

- Presupunem că un utilizator A are cheia publică (p, g, y) și cheia privată x
- Utilizatorul A generează o semnătură S a mesajului M astfel:

1. alege un număr aleatoriu $r \in \mathbb{Z}_{p-1}^*$ astfel încât $cmmdc(r, p-1) = 1$
2. calculează $a = g^r \pmod p$
3. calculează $b = (M - xa)r^{-1} \pmod{p-1}$
4. dacă $b = 0$ se reia de la pasul 1
5. semnătura mesajului M este $S = (a, b)$

- Utilizatorul A trimite utilizatorului B tripletul (M, a, b)

➢ Algoritmul de verificare:

- Utilizatorul B recepționează tripletul (M, a, b)
- Utilizatorul B obține cheia publică (p, g, y) a utilizatorului A
- Utilizatorul B verifică faptul că:
  - $1 \leq a < p$ și $1 \leq b < p - 1$
  - $y^a a^b (\mathrm{mod}\, p) = g^M (\mathrm{mod}\, p)$

➢ Exemplu:

- Considerăm $p = 11$ şi generatorul $g = 2$ al grupului $\mathbb{Z}_{11}^*$
- Alegem $x = 5 \in \mathbb{Z}_{11}^*$ și calculăm $y = 2^5 (\mathrm{mod}\ 11) = 10$
- Cheia publică este tripletul $(11, 2, 10)$, iar cheia privată este numărul 5
- Considerăm mesajul $M = 3$
- Alegem numărul aleatoriu $r = 7 \in \mathbb{Z}_{10}^*, cmmdc(7,10) = 1$
- Calculăm $a = 2^7 (\mathrm{mod}\ 11) = 7$
- Calculăm $b = (3 - 5 \cdot 7) \cdot 7^{-1} (\mathrm{mod}\ 10) = 8 \cdot 3\ (\mathrm{mod}\ 10) = 4$
- Semnătura mesajului $M = 3$ este $S = (7,4)$
- Testăm validitatea semnăturii $S = (7,4)$ pentru mesajul $M = 3$ verificând dacă:
  - $1 \leq 7 < 11$ şi $1 \leq 4 < 10$
  - $10^7 \cdot 7^4 (\mathrm{mod}\ 11) = 2^3 (\mathrm{mod}\ 11) \Leftrightarrow 8 = 8 \Rightarrow$ mesajul $M = 3$ este autentic

- **ECDSA = Elliptic Curve Digital Signature Algorithm**

- **Algoritmul de generare a cheilor:**

1. Se selectează un număr natural prim p mare și o curbă eliptică E peste $\mathbb{Z}_p$
2. Se selectează un punct $A \in E, A \neq \mathcal{O}$ având ordinul un număr prim q mare, i.e. $q \cdot A = \mathcal{O}$
3. Se selectează un număr $m \in \mathbb{Z}_q^*$ și se determină punctul $B = m \cdot A$
4. Cheia publică este formată din (p, E, A, q, B)
5. Cheia privată este numărul m

➢ Algoritmul de semnare:

• Presupunem că un utilizator A are cheia privată x

• Utilizatorul A generează o semnătură S a mesajului M, reprezentat folosind cel mult numărul de biți pe care este considerat q, astfel:

1. alege un număr aleatoriu $k \in \mathbb{Z}_q^*$ (*cheie efemeră*)

2. semnătura asociată mesajului M și cheii private x este o pereche (r, s), calculată astfel:
   - se calculează $k \cdot A = (u, v)$
   - se calculează $r = u \pmod q$
   - se calculează $s = k^{-1}(M + m \cdot r)(\mathrm{mod}\, q)$

3. dacă $r = 0$ sau $s = 0$, atunci se reia pasul 1

4. semnătura mesajului M este $S = (r, s)$

➢ Algoritmul de verificare:

- Utilizatorul B recepționează tripletul (M, r, s)
- Utilizatorul B obține cheia publică (p, E, A, q, B) a utilizatorului A
- Utilizatorul B verifică faptul că punctul A și componentele r și s ale semnăturii sunt valide:
  - $A \in E$
  - $A \neq \mathcal{O}$
  - $q \cdot A = \mathcal{O}$
  - $1 \leq r, s \leq q - 1$
- Utilizatorul B verifică validitatea semnăturii, astfel:
  - calculează $i = s^{-1} \cdot M \pmod{q}$ și $j = s^{-1} \cdot r \pmod{q}$
  - calculează $(u', v') = i \cdot A + j \cdot B$
  - semnătura (r, s) este validă dacă $u' \pmod{q} = r$

➢ Corectitudinea algoritmului:

$$(u', v') = i \cdot A + j \cdot B = i \cdot A + j \cdot \underbrace{m \cdot A}_{B} = (i + j \cdot m) \cdot A = \left(\underbrace{s^{-1} \cdot M}_{i} + \underbrace{s^{-1} \cdot r}_{j} \cdot m \right) \cdot A =$$

$$= s^{-1} \cdot \left(\underbrace{M + r \cdot m}_{s \cdot k} \right) \cdot A = s^{-1} \cdot s \cdot k \cdot A = k \cdot A = (u, v) \Longrightarrow u' = u \Longrightarrow u' \,(\mathrm{mod}\, q) = r$$

➢ Exemplu:

- Considerăm curba eliptică $E: y^2 = x^3 + x + 5$ peste $\mathbb{Z}_{19} \Longrightarrow p = 19$.
- Curba E are 15 puncte, iar punctul $A_1(0,9)$ este generator:

$A_1 = 1 \cdot A_1 = (0,9)$ $\quad$ $A_6 = 12 \cdot A_1 = (3,15)$ $\quad$ $A_{11} = 8 \cdot A_1 = (12,4)$

$A_2 = 14 \cdot A_1 = (0,10)$ $\quad$ $A_7 = 4 \cdot A_1 = (4,4)$ $\quad$ $A_{12} = 7 \cdot A_1 = (12,15)$

$A_3 = 13 \cdot A_1 = (1,8)$ $\quad$ $A_8 = 11 \cdot A_1 = (4,15)$ $\quad$ $A_{13} = 10 \cdot A_1 = (13,7)$

$A_4 = 2 \cdot A_1 = (1,11)$ $\quad$ $A_9 = 6 \cdot A_1 = (11,6)$ $\quad$ $A_{14} = 5 \cdot A_1 = (13,12)$

$A_5 = 3 \cdot A_1 = (3,4)$ $\quad$ $A_{10} = 9 \cdot A_1 = (11,13)$ $\quad$ $\mathcal{O} = 15 \cdot A_1$

- Alegem $A = A_5 = 3 \cdot A_1$, deci $5 \cdot A = 5 \cdot A_5 = 15 \cdot A_1 = \mathcal{O} \Longrightarrow q = 5$
- Numărul $q = 5$ se reprezintă binar folosind 3 biți, deci mesajul M trebuie să fie codificat pe cel mult 3 biți!
- Considerăm mesajul $M = 6$
- Alegem $m = 3 \in \mathbb{Z}_5^*$ și calculăm punctul $B = m \cdot A = 9 \cdot A_1 = A_{10} = (11, 13)$
- Cheia publică este formată din $(p = 19, E, A = A_5, q = 5, B = A_{10})$
- Cheia privată este $m = 3$
- Alegem cheia efemeră $k = 2 \in \mathbb{Z}_5^*$
- Calculăm $k \cdot A = 2 \cdot A = 6 \cdot A_1 = A_9 = (11{,}6) \Longrightarrow (u, v) = (11, 6)$
- Calculăm $r = u \pmod q = 11 \pmod 5 = 1$
- Calculăm $s = k^{-1}(M + m \cdot r) \pmod q = 2^{-1}(6 + 3 \cdot 1) \pmod 5 = 2$
- Semnătura asociată mesajului $M = 6$ este perechea $(r, s) = (1, 2)$

- Verificăm faptul că punctul A și perechea (r, s) sunt valide:
  - $A \in E, A \neq \mathcal{O}$ și $q \cdot A = \mathcal{O}$
  - $1 \leq r, s \leq q - 1 = 4$
- Verificăm validitatea semnăturii $(r = 1, s = 2)$ pentru mesajul $M = 6$:
  - calculăm $i = s^{-1} \cdot M \pmod{q} = 2^{-1} \cdot 6 \pmod{5} = 3 \cdot 6 \pmod{5} = 3$
  - calculăm $j = s^{-1} \cdot r \pmod{q} = 2^{-1} \cdot 1 \pmod{5} = 3 \cdot 1 \pmod{5} = 3$
  - calculăm $(u', v') = i \cdot A + j \cdot B = 3 \cdot A + 3 \cdot B = 6 \cdot A_1 = A_9 = (11, 6)$
  - semnătura $(r = 1, s = 2)$ este validă deoarece $11 \pmod{5} = 1$