CRIPTOGRAFIE CU CHEIE PUBLICĂ

Conf.univ.dr. Radu Boriga

Conf.univ.dr. Ana Cristina Dăscălescu

SISTEME DE CRIPTARE ASIMETRICE (CU CHEIE PUBLICĂ)

- Ideea inovatoare de a utiliza o **cheie publică** şi o **cheie privată** a fost propusă de către cercetătorii **Whitfield Diffie** şi **Martin Hellman** în anul 1976 în cadrul unui protocol care permite crearea unei chei secrete comune folosind două chei private.

- **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!

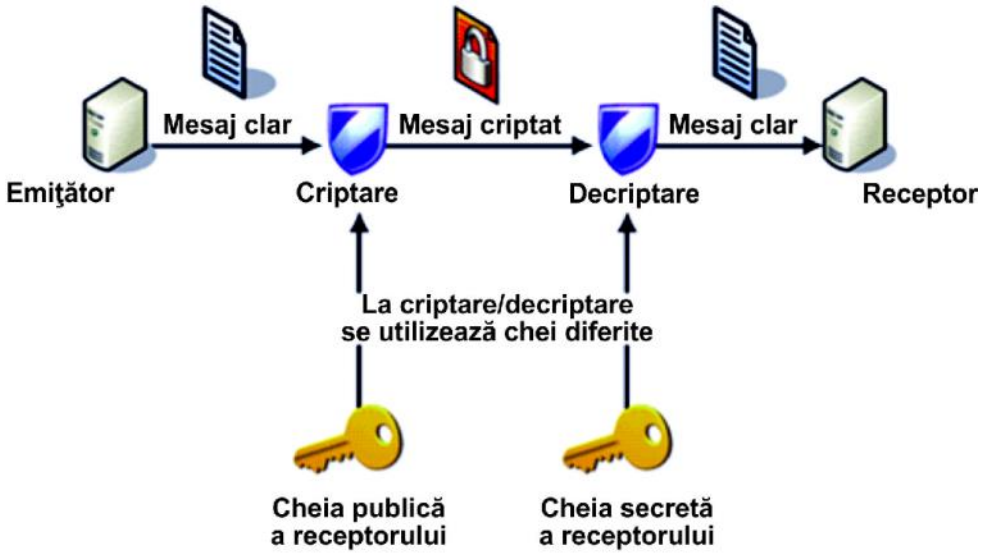
- Confidenţialitatea datelor într-o schemă de criptare asimetrică este asigurată de faptul că este imposibil de obţinut din punct de vedere computaţional cheia secretă utilizată pentru decriptarea datelor din cheia publică utilizată pentru criptarea datelor.

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.

PROTOCOLUL DIFFIE-HELLMAN (1976)

- **Protocolul Diffie-Hellman** este utilizat pentru a crea o cheie secretă partajată pe baza a două chei private, folosind un canal nesigur de comunicație.

- Securitatea protocolului se bazează pe dificultatea rezolvării **problemei logaritmului discret** într-un grup multiplicativ $\mathbb{Z}_p$, unde p este un număr prim cu cel puțin 1024 de biți!

- **Protocolul Diffie-Hellman:**
  - Alice și Bob aleg un număr prim p și un generator g al grupului multiplicativ $\mathbb{Z}_p$ (ambele valori p și g pot fi publice!)
  - Alice alege o cheie privată $a \in \mathbb{N}^*$ și îi trimite lui Bob numărul $A \equiv g^a \pmod p$
  - Bob alege o cheie privată $b \in \mathbb{N}^*$ și îi trimite lui Alice numărul $B \equiv g^b \pmod p$
  - Alice calculează $S \equiv B^a \pmod p \equiv g^{ab} \pmod p$
  - Bob calculează $S \equiv A^b \pmod p \equiv g^{ab} \pmod p$
  - Alice și Bob cunosc amândoi cheia secretă partajată S!

- Se poate observa faptul că nici Alice și nici Bob nu pot afla cheile private a și b cunoscând numerele A și B, deoarece acest lucru ar fi echivalent cu rezolvarea problemei logaritmului discret în grupul multiplicativ $\mathbb{Z}_p$ ales!

- Alice și Bob pot utiliza un canal nesigur de comunicație pentru a-și transmite unul altuia numerele A și B, deoarece, din același motiv ca mai sus, nici un atacator nu ar putea afla cheile private a și b!

- **Exemplu:**
  - Alice și Bob aleg $p = 11$ și generatorul $g = 6$ al grupului multiplicativ $\mathbb{Z}_{11}$
  - Alice alege cheia privată $a = 2$ și îi trimite lui Bob numărul $A \equiv 6^2 (\mathrm{mod}\ 11) = 3$
  - Bob alege cheia privată $b = 7$ și îi trimite lui Alice numărul $B \equiv 6^7 (\mathrm{mod}\ 11) = 8$
  - Alice calculează $S \equiv 8^2 (\mathrm{mod}\ 11) = 9$
  - Bob calculează $S \equiv 3^7 (\mathrm{mod}\ 11) = 9$
  - Alice și Bob cunosc amândoi cheia secretă partajată $S = 9$!

➢ Algoritmul de generare a cheilor:

1. Se generează un vector supercrescător de numere naturale nenule $w = (w_1, w_2, \dots, w_n)$, i.e. având proprietatea:

$$w_j > \sum_{i=1}^{j-1} w_i, \qquad \forall j \geq 2$$

2. Se selectează un număr natural q astfel încât $q > w_1 + w_2 + \cdots + w_n$

3. Se selectează un număr natural $1 \leq r < q$ astfel încât q și r să fie coprime, i.e. $cmmdc(q, r) = 1$

4. Se calculează vectorul $k = (k_1, k_2, \dots, k_n)$ folosind relația $k_i = rw_i (\mathrm{mod}\, q)$

5. Cheia publică este vectorul k, iar cheia privată este tripletul (w, q, r)

➢ Algoritmul de criptare:

- Presupunem că un utilizator A are cheia publică k și cheia privată (w, q, r)

- Un utilizator B criptează mesajul clar în format binar $M = m_1 m_2 \dots m_n$ $(m_i \in \{0,1\})$ în mesajul criptat C astfel:

$$C = \sum_{i=1}^{n} m_i * k_i$$

➢ Algoritmul de decriptare:

- Utilizatorul A recepționează un mesaj criptat C și obține mesajul inițial M astfel:

1. Calculează inversul modular s al lui r, i.e. determină numărul natural s cu proprietatea $s * r (\mathrm{mod}\ q) = 1$

2. Calculează $C' = s * C (\mathrm{mod}\ q)$

3. Determină mesajul inițial $M = m_1 m_2 \ldots m_n$ rezolvând problema:

$$C' = \sum_{i=1}^{n} m_i * w_i$$

➢ Exemplu:

1. Fie $w = (2, 7, 11, 21, 42, 89, 180, 354) \Rightarrow w_1 + w_2 + \cdots + w_8 = 706$
2. Alegem $q = 881 > 706$
3. Alegem $r = 588$ deoarece este coprim cu $q = 881$
4. Calculăm vectorul $k = (k_1, k_2, \dots, k_8)$ folosind relația $k_i = 588 * w_i (\mathrm{mod}\ 881)$:

$$k = (295, 592, 301, 14, 28, 353, 120, 236)$$

5. Cheia publică este vectorul k, iar cheia privată este tripletul $(w, 881, 588)$
6. Mesajului $M =$ "NU" îi corespund, conform codurilor ASCII, mesajele binare $M_1 = 01001110$ și $M_2 = 01010101$
7. Mesajul binar $M_1 = 01001110$ se criptează, folosind vectorul k, în mesajul $C_1 = 1093$, astfel:

$$C_1 = 0 * 295 + 1 * 592 + 0 * 301 + 0 * 14 + 1 * 28 + 1 * 353 + 1 * 120 + 0 * 236 = 1093$$

8. Mesajul binar $M_2 = 01010101$ se criptează, folosind vectorul k, în mesajul $C_2 = 1195$, astfel:

$$C_2 = 0 * 295 + 1 * 592 + 0 * 301 + 1 * 14 + 0 * 28 + 1 * 353 + 0 * 120 + 1 * 236 = 1195$$

9. Pentru decriptare, se calculează mai întâi inversul modulo $q = 881$ al lui $r = 588$, obținându-se $s = 442$

10. Pentru mesajul criptat $C_1 = 1093$ se calculează $C_1' = 1093 * 442 \pmod{881} = 318$ și se decriptează mesajul $C_1' = 318$, folosind vectorul w, astfel:

w	C_1'	Bit
354	318	**0**
180	$318 - 180 = 138$	**1**
89	$138 - 89 = 49$	**1**
42	$49 - 42 = 7$	**1**
21	7	**0**
11	7	**0**
7	$7 - 7 = 0$	**1**
2	0	**0**

$$\Rightarrow D_1 = 01001110_{(2)} = 78 = 'N'$$

11. Pentru mesajul criptat $C_2 = 1195$ se calculează $C_2' = 1195 * 442 \pmod{881} = 471$ și se decriptează mesajul $C_2' = 471$, folosind vectorul w, astfel:

w	C_2'	Bit
354	$471 - 354 = 117$	**1**
180	117	**0**
89	$117 - 89 = 28$	**1**
42	28	**0**
21	$28 - 21 = 7$	**1**
11	7	**0**
7	$7 - 7 = 0$	**1**
2	0	**0**

$\Rightarrow D_2 = 01010101_{(2)} = 85 = 'U'$

➢ 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 criptare:

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

1. obține cheia publică (e, n) a utilizatorului A
2. codifică mesajul clar M sub forma unui număr cuprins între 0 și $n - 1$
3. determină mesajul criptat C folosind relația $C = M^e \pmod n$
4. trimite textul criptat C utilizatorului A

➢ Algoritmul de decriptare:

- Utilizatorul A recepționează un mesaj criptat C și obține mesajul inițial M astfel:

1. folosește cheia sa privată (d, n)

2. determină mesajul inițial M folosind relația $M = C^d \pmod{n}$

➢ 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 $M = 17$ se criptează în $C = 17^7 \pmod{55} = 410338673 \pmod{55} = 8$
8. Mesajul criptat $C = 8$ se decriptează în $M = 8^{23} (mod\ 55) = 17$

➢ 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 $x \in \mathbb{Z}_p^*$ și se calculează $y = g^x \pmod p$, deci $x = \log_g y$
3. Cheia publică este tripletul (p, g, y), iar cheia privată este numărul x

➢ Algoritmul de criptare:

- Presupunem că un utilizator A are cheia publică (p, g, y) și cheia privată x
- Un utilizator B criptează un mesaj M pentru utilizatorul A astfel:
  - alege un număr aleatoriu $r \in \mathbb{Z}_{p-1}^*$ (*cheie efemeră*)
  - criptează mesajul clar M, reprezentat printr-un număr natural, prin perechea:

$$C = \left(\underbrace{g^r \pmod p}_{a}, \underbrace{M * y^r \pmod p}_{b} \right)$$

➢ Algoritmul de decriptare:

- Utilizatorul A decriptează un mesaj criptat $C = (a, b)$ astfel:

$$D = b * a^{-x} (\mathrm{mod}\ p)$$

➢ Corectitudinea algoritmului:

- Fie $C = (a, b)$ un mesaj criptat, deci $C = \left(\underbrace{g^r (\mathrm{mod}\ p)}_{a}, \underbrace{M * y^r (\mathrm{mod}\ p)}_{b} \right)$

- Mesajul decriptat D este:

$$D = b * a^{-x} (\mathrm{mod}\ p) = (M * y^r) * (g^r)^{-x}\ (\mathrm{mod}\ p) =$$

$$= M * (g^x)^r * g^{-rx} (\mathrm{mod}\ p) = M * g^{xr} * g^{-xr} (\mathrm{mod}\ p) = M$$

➢ Exemplu:

1. Considerăm $p = 11$ şi generatorul $g = 2$ al grupului $\mathbb{Z}_{11}^*$
2. Alegem $x = 5 \in \mathbb{Z}_{11}^*$ și calculăm $y = 2^5 (\mathrm{mod}\ 11) = 10$
3. Cheia publică este tripletul $(11, 2, 10)$, iar cheia privată este numărul 5
4. Mesajul $M = "DA"$ poate fi reprezentat prin perechea $(4, 1)$
5. Alegem numărul aleator $r_1 = 5 \in \mathbb{Z}_{10}^*$ și criptăm numărul $n_1 = 4$ prin perechea $C_1 = (2^5 (\mathrm{mod}\ 11), 4 * 10^5 (\mathrm{mod}\ 11)) = (10,7)$
6. Alegem numărul aleator $r_2 = 8 \in \mathbb{Z}_{10}^*$ și criptăm numărul $n_2 = 1$ prin perechea $C_2 = (2^8 (\mathrm{mod}\ 11), 1 * 10^8 (\mathrm{mod}\ 11)) = (9,1)$
7. Perechea $C_1 = (10,7)$ se decriptează în $D_1 = 7 * 10^{-5} (\mathrm{mod}\ 11) = 4$
8. Perechea $C_2 = (9,1)$ se decriptează în $D_2 = 1 * 9^{-5} (\mathrm{mod}\ 11) = 1$

Online calculator: Modular Multiplicative Inverse (planetcalc.com)