Seminarul 5 - 27 martie 2024

→ Exercițiile restante din seminarul 4 → Ex #4, Ex #5, Ex #6.

RSA clasic

RSA

I Generarea cheilor

- Bob alege $p \neq q$ prime; calculează $N = pq$ și $\varphi(N) = (p-1)(q-1)$
- Bob alege $1 < e < \varphi(N)$ cu $\gcd(e, \varphi(N)) = 1$
- Bob calculează, folosind algoritmul extins al lui Euclid, $0 < d < \varphi(N)$ a.î. $ed \equiv 1 \pmod{\varphi(N)}$

↳ invers modular $\Leftrightarrow d \equiv e^{-1} \pmod{\varphi(N)}$

Se obține cheia publică (N, e) și cheia privată (N, d).

II Criptarea

Fie $\mathcal{P} = \{m \in \mathbb{N} : 1 < m < N\}$

- Alice calculează $c = m^e \pmod N$

III Decriptarea

- Bob decriptează prin $m = c^d \pmod N$

Ex #1 Se consideră modulul RSA $N = 85$. Alice folosește cheia publică $e = 3$ și vrea să trimită mesajul $m = 80$ către Bob. Găsiți:

a) mesajul criptat

b) cheia secretă

c) arătați cum Bob decriptează mesajul de la Alice

Folosiți varianta clasică de RSA.

Deci

- Criptarea mesajului

$$\left.\begin{array}{l} N = 85 \\ m = 80 \\ e = 3 \end{array}\right\} \Rightarrow c = m^e \pmod N \Leftrightarrow c = 80^3 \pmod{85} = (-5)^3 \pmod{85}$$

$$c = -125 \pmod{85}$$

$$c = 45 \pmod{85}.$$

• Cheia secretă

Știm că $ed \equiv 1 \pmod{\varphi(N)}$. Calculăm, deci, $\varphi(N)$.

$\varphi(85) = \varphi(5 \cdot 17) = \varphi(5)\varphi(17) = (5-1)(17-1) = 4 \cdot 16 = 64$

Acum, cum $e = 5$, $3 \cdot d \equiv 1 \pmod{64} \Rightarrow d = 3^{-1} \pmod{64}$

Deci trebuie să găsim $3^{-1} \bmod 64$. Aplicăm algoritmul extins al lui Euclid.

$$64 = 3 \cdot 21 + 1$$

Deci $1 = 64 - 3 \cdot 21 = 64 + 3 \cdot (-21) \pmod{64}$

$1 = 3 \cdot (-21) \pmod{64}$

$1 = 3 \cdot 43 \pmod{64}$

adică $43 = 3^{-1} \pmod{64}$.

Prin urmare, cheia secretă $d = 43$.

• Decriptarea

Pentru decriptare, Bob trebuie să calculeze $45^{43} \pmod{85}$. Acesta aplică algoritmul de exponențiere rapidă

43	2
4	21	2
=3	20	10	2
2	=1	10	5	2
1		=0	4	2	2
			1	2	1
				0	

$\Rightarrow 43 = 101011_{(2)}$

$43 = 2^5 + 2^3 + 2 + 1$

$43 = 32 + 8 + 2 + 1$

Calculăm

- $45^{43} = 45^{32} \cdot 45^8 \cdot 45^2 \cdot 45 \pmod{85}$
- $45^2 = 70 \pmod{85} = (-15) \pmod{85}$
- $45^4 = 70 \cdot 70 = 55 \pmod{85}$
- $45^8 = 55 \cdot 55 = 50 \pmod{85}$
- $45^{16} = 50 \cdot 50 = 35 \pmod{85}$
- $45^{32} = 35 \cdot 35 = 35 \pmod{85}$

Deci $45^{43} = 35 \cdot 50 \cdot 70 \cdot 45 \pmod{85} = 80 \pmod{85}$.

□

Ex#2 Același mesaj m a fost criptat folosind RSA și trimis către A și B (doi utilizatori). A are cheia publică (1591, 17), iar B (1591, 5). Oscar interceptează textele cifrate $c_1 = 849$ și $c_2 = 22$. Cum poate Oscar, în condiții reale, determina textul simplu m? Găsiți-l.

Deci
m

A are cheia publică $(n, e_A) = (1591, 17)$
B are cheia publică $(n, e_B) = (1591, 5)$

Mesajul criptat cu aceste chei ne dă

$$\begin{cases} c_1 = m^{e_A} \pmod n \\ c_2 = m^{e_B} \pmod n \end{cases} \Leftrightarrow \begin{cases} m^{17} = 849 \pmod{1591} \\ m^5 = 22 \pmod{1591} \end{cases}$$

Cum $\gcd(e_A, e_B) = \gcd(17, 5) = 1 \Rightarrow \exists \alpha_1, \alpha_2 \in \mathbb{Z}$ a.î. $17\alpha_1 + 5\alpha_2 = 1$.
Folosim algoritmul lui Euclid pentru a afla α_1 și α_2.

$$17 = 5 \cdot 3 + 2 \Rightarrow 2 = 17 - 5 \cdot 3$$
$$5 = 2 \cdot 2 + 1 \Rightarrow 1 = 5 - 2 \cdot 2$$
$$2 = 1 \cdot 2 + 0$$

Deci $1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (17 - 5 \cdot 3)$
$1 = 7 \cdot 5 + (-2) \cdot 17$
$1 = (-2) \cdot 17 + 7 \cdot 5$

Adică $\alpha_1 = -2$ și $\alpha_2 = 7$.
Avem următorul calcul

$$m = m^1 = m^{(-2)\cdot 17 + 7 \cdot 5} = (m^{17})^{-2} (m^5)^7 = 849^{-2} \cdot 22^7 \pmod{1591}$$

Pentru a găsi 849^{-1} aplicăm algoritmul extins al lui Euclid.
Construim următorul tabel:

$$\begin{cases} t_j = t_{j-2} - q_{j-1} t_{j-1} & t_0 = 0, t_1 = 1 \\ r_{k-2} = q_{k-1} r_{k-1} + r_k \end{cases}$$

OBS r_k și q_k sunt resturile și câturile din Alg. lui Euclid

k	r_k	q_k	t_k
0	1591	–	0
1	849	1	1
2	742	1	-1
3	107	6	2
4	100	1	-13
5	7	14	15
6	2	3	-223
7	1	2	(684)

Așadar $849^{-1} \pmod{1591} = 684$.

Calculăm

$$a = 849^{-2} \cdot 22^7 = (849^{-1})^2 \cdot 22^7 = 684^2 \cdot 22^7 \pmod{1591}$$

$$a = 102 \cdot 816 = 500 \pmod{1591}$$

Încă concluzie, textul simplu este $a = 500$ (pentru că $1 < a < n$).

□

Ex #3 Fie $N = 85 = 5 \cdot 17$, $\varphi(N) = \varphi(85) = 4 \cdot 16 = 64$. Alegem $e = 5$. Calculați $d = e^{-1} \pmod{\varphi(N)}$.

Deci

Aplicăm algoritmul extins al lui Euclid

$$64 = 5 \cdot 12 + 4$$
$$5 = 4 \cdot 1 + 1$$
$$4 = 1 \cdot 4 + 0$$

k	r_k	q_k	t_k
0	64	–	0
1	5	12	1
2	4	1	-12
3	1	4	(13)

$$1 = 5 - 4 \cdot 1 = 5 - 1(64 - 5 \cdot 12)$$
$$1 = 13 \cdot 5 - 64 \pmod{64}$$
$$13 \cdot 5 = 1 \pmod{64}$$

$$\Rightarrow \boxed{d = 13}$$

□

Ex #4 În ipotezele problemei anterioare considerăm mesajul $m = 10$. Criptați-l și realizați decriptarea.

Deci m

- **Criptarea**

$c = m^e \pmod N \Leftrightarrow c = 10^5 \pmod{85}$

Exponențiere rapidă $10^5 = 10^4 \cdot 10 \pmod{85}$

$10^2 = 100 = 15 \pmod{85}$

$10^4 = 15 \cdot 15 = 55 \pmod{85}$

$10^5 = 10^4 \cdot 10 = 55 \cdot 10 = 40 \pmod{85}$

Deci $\boxed{c = 40}$

- **Decriptarea**

Avem $m = c^d \pmod N$, deci de calculat

$m = 40^{29}$

Exponențiere rapidă

$29 = 1 + 28 = 1 + 2^2 + 2^3 + 2^4 = 1 + 4 + 8 + 16$

$40^2 = 70 \pmod{85}$

$40^4 = 40 \cdot 70 = 55 \pmod{85}$

$40^8 = 55 \cdot 55 = 50 \pmod{85}$

$40^{16} = 50 \cdot 70 = 35 \pmod{85}$

Deci $m = 40^{29} = 40 \cdot 40^4 \cdot 40^8 \cdot 40^{16} = 40 \cdot 55 \cdot 50 \cdot 35 \pmod{85}$

$m = 10 \pmod{85}$

$\boxed{m = 10}$

□

- **Def** Spunem că un număr este **liber de pătrate** dacă niciun pătrat diferit de 1 îl divide. În descompunerea în factori primi a unui număr liber de pătrate, toate numerele prime au exponentul 1.

- **Cmmdc:** $\text{lcm}(a,b) = \dfrac{ab}{\gcd(a,b)}$

• Fie n un număr liber de pătrate și $n = p_1 p_2 \dots p_k$ descompunerea sa în factori primi. Definim

$$\lambda(n) = \text{lcm}(p_1 - 1, p_2 - 1, \dots, p_k - 1)$$

• Generalizare unica Th a lui Fermat

Fie N liber de pătrate și $e = a\lambda(N) + 1$. Atunci pentru toți $x \in \mathbb{Z}$

$$x^e = x \mod N$$

RSA modificat

În algoritmul clasic se înlocuiește $\varphi(n)$ cu $\lambda(n)$.

Ex #5 Aplicați RSA reformulat

$N = 119 = 7 \cdot 17$
$e = 5$
$m = 11$

a) Calculați $\lambda(N)$
b) Aflați cheia de decriptare d
c) Calculați m^e
d) Efectuați decriptarea

Deci

• Calculăm $\lambda(m) = \text{lcm}(7-1, 17-1) = \text{lcm}(6, 16) = \frac{6 \cdot 16}{2} = 6 \cdot 8 = 48$

• Cheia de decriptare

$$ed \equiv 1 \pmod{\lambda(m)} \Leftrightarrow d = e^{-1} \pmod{\lambda(m)} \Rightarrow$$
$$\Rightarrow d = 5^{-1} \pmod{48}$$

Euclid extins:

$48 = 5 \cdot 9 + 3$
$5 = 3 \cdot 1 + 2$
$3 = 2 \cdot 1 + 1$
$2 = 1 \cdot 2 + 0$

k	r_k	q_k	t_k
0	48	–	0
1	5	9	1
2	3	1	-9
3	2	1	10
4	1	2	-19

$\Rightarrow d = -19 = 29 \mod 48 \Rightarrow$

$\Rightarrow \boxed{d = 29}$

- Criptare

$$c = m^e \pmod n \iff c = 11^5 \pmod{119}$$

Exponentiere rapidă:

$11^5 = 11^4 \cdot 11 \pmod{119}$

$11^2 = 2 \pmod{119}$

$11^4 = 4 \pmod{119}$

$11^5 = 4 \cdot 11 = 44 \pmod{119}$

Deci $\boxed{c = 44}$

- Decriptare

$$m = c^d \pmod n \iff m = 44^{29} \bmod 119$$

$29 = 1 + 4 + 8 + 16$

$44^2 = 32 \pmod{119}$

$44^4 = 72 \pmod{119}$

$44^8 = 67 \pmod{119}$

$44^{16} = 86 \pmod{119}$

Așadar $m = 44^{29} \bmod 119$

$m = 44 \cdot 72 \cdot 67 \cdot 86 = 11 \pmod{119}$.

□

OBS Folosirea lui $\lambda(n)$ în loc de $\varphi(n)$ ne poate da o cheie privată de dimensiuni mai mici.

ElGamal

- Criptosistemul ElGamal se bazează pe
  - → problema logaritmului discret
  - → Protocolul Diffie-Hellman

ElGamal

- Alice îi trimite mesajul lui Bob, $m \in \{0, 1, \dots, p-1\}$

I Generarea cheilor

- Alice generează aleator un număr prim p
- Alice generează aleator o rădăcină primitivă $x \bmod p$

- Se alege aleator $a \in \mathbb{Z}$ cu $1 < a \leq p-2$
- Calculează $x^a \pmod p$
- Obține cheia publică (p, x, x^a) și cheia privată a

II Criptarea mesajului
- Bob preia cheia publică
- Alege un număr $b < p-1$, natural, aleator
- Calculează $x^b \pmod p$ și $mx^{ab} \pmod p$
- Obține mesajul $c = (x^b, mx^{ab})$ pe care îl trimite

III Decriptarea
- Alice folosește cheia privată și calculează

$$(x^b)^{-a} = (x^b)^{p-1-a} \pmod p$$

Little Fermat: $x^{p-1} \equiv 1 \pmod p$

$x^{-a} = x^{-a} \cdot 1 = x^{-a} \cdot x^{p-1} = x^{p-1-a} \pmod p$

- Calculează

$$(x^b)^{-a} mx^{ab} = mx^{ab-ab} = m \pmod p$$

! Dezavantaj ElGamal
↳ textul criptat își dublează dimensiunea în raport cu textul inițial

Ex #6 Alice și Bob folosesc ElGamal aditiv modulo 100 cu generatorul $g = 31$. Alice alege cheia secretă $k = 17$. Calculează cheia publică și o transmite lui Bob. Bob alege cheia $y = 11$. El folosește cheia publică și codează mesajul $m = 72$. Alice își folosește cheia și găsește mesajul inițial. Faceți toate calculele.

Deci
Lucrăm în $(\mathbb{Z}_{11}, +) =: G$.
Numărul $g = 31$ este generator pentru G pentru că $\gcd(31, 100) = 1$. Pentru că suntem în cadrul aditiv, cheia publică este dată de $h = gk \pmod w$, ie $h = 31 \cdot 17 \pmod{100}$

$h = 27 \pmod{100}$ (Alice)

Bob calculează
$(c_1, c_2) = (gy, m + hy) = (31 \cdot 11, 27 \cdot 11 + 72) = (41, 97 + 72)$
$(c_1, c_2) = (41, 69)$

Alice primește (c_1, c_2). Pentru a afla m, ea calculează
$m = c_2 - k c_1 = ky + m - k g y = g k y + m - k g y = m$ ok
$m = 69 - 17 \cdot 41 = 69 - 97 = 72 \pmod{100}$

□

Ex #7 În ipotezele problemei anterioare, Oscar intercepteză mesajul $(41, 69)$ și vrea să afle cheia secretă k. Ce trebuie să facă pentru asta?

Dem
m

Oscar cunoaște cheia publică $h = 27 \pmod{100}$
$h = g^k \pmod{100} \Rightarrow k = g^{-1} h \pmod{100}$
Să observăm că și g este public. Așadar Oscar trebuie doar să calculeze inversul modular al lui g. Aplicăm Euclid

$100 = 31 \cdot 3 + 7$
$31 = 7 \cdot 4 + 3$
$7 = 3 \cdot 2 + 1$
$3 = 1 \cdot 3 + 0$

k	r_k	q_k	t_k
0	100	-	0
1	31	3	1
2	7	4	-3
3	3	2	13
4	1	3	-29

$\Rightarrow g^{-1} = -29 = 71 \pmod{100}$

și găsește că
$k = g^{-1} h \pmod{100}$
$k = 71 \cdot 27 \pmod{100}$
$k = 17 \pmod{100}$.

□

Concluzie : Siguranță 0.

Ex #8 Alice și Bob folosesc ElGamal multiplicativ

- Calculele modulo 11
- Generator $g = 2$
- Alice alege cheia secretă $k = 9$
- Bob alege cheia $y = 7$
- Bob codează mesajul $m = 8$

Faceți toate calculele.

Deci
Alice calculează cheia publică $h = g^k \pmod{11}$, ie

$$h = 2^9 \pmod{11}$$

Exponențiere rapidă

$2^2 = 4 \pmod{11}$

$2^4 = 16 = 5 \pmod{11}$

$2^8 = 25 = 3 \pmod{11}$

Deci $h = 2^9 = 2^{1+8} = 2 \cdot 2^8 = 2 \cdot 3 = 6 \pmod{11}$

Alice face public h și g.

Bob calculează

- $c_1 = g^y \pmod{11} \Leftrightarrow c_1 = 2^7 = 2^{1+2+4} = 2 \cdot 4 \cdot 5 = 40 = 33 + 7 = 7 \ (11)$

$\boxed{c_1 = 7}$

- $c_2 = m h^y \pmod{11} \Leftrightarrow c_2 = 8 \cdot 6^7 \pmod{11}$

$6^7 = 6^{1+2+4} \pmod{11}$

$6^2 = 36 = 33 + 3 = 3 \pmod{11}$

$6^4 = 9 \pmod{11}$

$6^7 = 6 \cdot 3 \cdot 9 = 18 \cdot 9 = (11+7) \cdot 9 = 63 = 55 + 8 = 8 \pmod{11}$

$c_2 = 8 \cdot 8 = 64 = 55 + 9 = 9 \pmod{11}$

$\boxed{c_2 = 9}$

Alice trebuie să decripteze $(c_1, c_2) = (7, 9)$ pentru a obține m.

$$m = c_2 (c_1^k)^{-1} = m h^y (g^{-y})^k = m (g^k)^y (g^{-y})^k = m \quad \text{ok}$$

$m = 9 \cdot (7^9)^{-1} \pmod{11}$

Calculează

$7^9 = 7^{1+8} = 7 \cdot 7^8 \pmod{11}$

$7^2 = 49 = 44 + 5 = 5 \pmod{11}$

$7^4 = 25 = 22 + 3 = 3 \pmod{11}$

$7^8 = 9 \pmod{11}$

Deci $7^9 = 7 \cdot 9 = 63 = 8 \pmod{11}$

Deci $m = 9 \cdot 8^{-1} \pmod{11}$.

Calculăm $8^{-1} \pmod{11}$ cu Euclid.

$11 = 8 \cdot 1 + 3$
$8 = 3 \cdot 2 + 2$
$3 = 2 \cdot 1 + 1$
$2 = 1 \cdot 2 + 0$

k	r_k	q_k	t_k
0	11	–	0
1	8	1	1
2	3	2	-1
3	2	1	3
4	1	2	-4

Deci $8^{-1} \equiv -4 \equiv 7 \pmod{11}$

Revenim și găsim

$$a_{10} = 9 \cdot 7 = 63 \equiv 8 \pmod{11}$$

Așadar $\boxed{a_{10} = 8}$ ok.

□

Concluzie → Calcule mai complicat de efectuat
⇓
siguranță mai mare.

Mica teorema a lui Fermat

Fie p un număr prim și $a \in \mathbb{N}$ prim cu p. Atunci

$$a^{p-1} \equiv 1 \pmod{p}$$

Logaritm discret

Fie G un grup ciclic de ordin $n \in \mathbb{N}$ și α un generator al lui G. Fie acum elementul $\beta \in G$. Numim **logaritmul discret** al lui β în baza α ($\log_\alpha \beta$), numărul unic întreg $e \leq \#(G-1)$ astfel ca $\alpha^e = \beta$.

Problema logaritmului discret

Considerăm $G = \mathbb{F}_p^*$ grupul multiplicativ cu elemente nenule în $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ cu p prim impar. Fie α generator al lui $\mathbb{F}_p^*$ și un element $\beta \in \mathbb{F}_p^*$. Se cere să se găsească unicul întreg nenul $e \leq p-2$ astfel încât

$$\alpha^e \equiv \beta \pmod{p}.$$

Rădăcină primitivă mod n

Se numește **rădăcină primitivă modulo** n, numărul $a \in \mathbb{Z}$ cu $\gcd(a, n) = 1$, dacă satisface

$$a^{\varphi(n)} = 1 \pmod{n}$$
$$a^{\alpha} \neq 1 \pmod{n}$$

pentru orice $\alpha \in \mathbb{Z}$ cu $\alpha \in (0, \varphi(n))$.

OBS $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \Rightarrow \varphi(n) = (p_1 - 1) p_1^{\alpha_1 - 1} \cdots (p_k - 1) p_k^{\alpha_k - 1}$