Seminar 7 - 10 Aprilie 2024

→ Exercițiile rămase din seminarul 6 → Ex #5, Ex #6, Ex #7, Ex #8

Ex #1 Găsiți o factorizare pentru $N = 77$ știind că $(e, d) = (43, 7)$.

Algoritm

Fie $ed - 1 = 2^s k$, k impar, $s \in \mathbb{N}$

P1) Alegem la întâmplare $a \in \{1, 2, \dots, N-1\}$

P2) Calculăm $\gcd(a, N)$.

P3) Dacă $\gcd(a, N) = 1$, atunci ~~calculăm~~ pentru $t = s-1, s-2, \dots$ calculăm $g = \gcd(a^{2^t k} - 1 \pmod N, N)$ până când $g > 1$ sau $t = 0$.

P4) Dacă $g > 1$, avem că $g = p$ sau $g = q$. STOP

Altfel, reia algoritmul cu alt a (return PAS 1).

Deci

Calculăm $ed - 1 = 43 \cdot 7 - 1 = 301 - 1 = 300$

$= 2^2 \cdot 5^2 \cdot 3 =$

$= 2^2 \cdot 75 \Rightarrow \begin{cases} s = 2 \\ k = 75 \end{cases}$

1) Alegem la întâmplare $a \in \{1, 2, \dots, 76\}$

Fie $a = 2$.

2) Calculăm (folosind algoritmul lui Euclid) $\gcd(2, 77) = 1$.

3) • $t = s - 1 \Leftrightarrow t = 2 - 1 \Leftrightarrow t = 1$

$2^{2 \cdot 75} - 1 = 4^{75} - 1 \overset{\text{exponențiere rapidă}}{=} 1 - 1 = 0 \pmod{77} \Rightarrow g = 1$

• $t = s - 2 \Leftrightarrow t = 2 - 2 \Leftrightarrow t = 0$

$2^{75} - 1 = 43 - 1 = 43 \pmod{77}$

Exponențiere rapidă: $75 = 64 + 8 + 2 + 1$

$2^2 = 4 \pmod{77}$

$2^4 = 16 \pmod{77}$

$2^8 = 25 \pmod{77}$

$2^{16} = 9 \pmod{77}$

$2^{32} = 4 \pmod{77}$

$2^{64} = 16 \pmod{77}$

Deci $2^{77} = 16 \cdot 25 \cdot 4 \cdot 2 = 43 \pmod{77}$

Avem acum

$g = \gcd(42, 77) = 7 > 1$

Algoritmul lui Euclid:

$77 = 42 \cdot 1 + 35$
$42 = 35 \cdot 1 + 7$ $\Rightarrow \gcd(42, 77) = 7$
$35 = 7 \cdot 5 + 0$

4) $g = 7 > 1$, deci $p = 7$ și $q = N : 7 \Rightarrow q = 11$. Așador

$N = pq = 7 \cdot 11.$

□

EX #2 – Examen 2022-2023 –

RSA. Un mesaj este criptat folosind algoritmul RSA cu $N = 33$ și cheia publică $e = 13$. Mesajul criptat este $c = 20$. Aflați mesajul original.

Deci
m

Știm că $c = m^e \pmod N$

Observăm că $33 = 3 \cdot 11$. Așador putem calcula $\varphi(N) = \varphi(33) = \varphi(3)\varphi(11)$, ie $\varphi(N) = 2 \cdot 10 = 20$.

Știind $\varphi(N)$ putem afla d astfel încât

$ed \equiv 1 \pmod{\varphi(N)}$

Aplicăm algoritmul lui Euclid pentru $\varphi(N) = 20$ și $e = 13$ și avem

$20 = 13 \cdot 1 + 7$
$13 = 7 \cdot 1 + 6$
$7 = 6 \cdot 1 + 1$
$6 = 1 \cdot 6 + 0$

deci $1 = 7 - 6 = 7 - (13 - 7) =$
$= 7 \cdot 2 - 13 = (20 - 13) \cdot 2 - 13 =$
$= 20 \cdot 2 - 13 \cdot 3$

Modulo $\varphi(N)$ găsim că $-13 \cdot 3 = 1 \pmod{\varphi(N)}$, ie
$13 \cdot 17 = 1 \pmod{20}$

Așadar am găsit cheia secretă $d = 17$.

Acum putem afla $m = c^d \pmod N$,

$m = 20^{17} \pmod{33}$

Aplicăm algoritmul de exponențiere rapidă,

Observăm că $17 = 1 + 16$. Calculăm

$20^1 = 20 \pmod{33}$
$20^2 = 4 \pmod{33}$
$20^4 = 16 \pmod{33}$
$20^8 = 25 \pmod{33}$
$20^{16} = 31 \pmod{33}$

Deci $w = 20^{17} = 20 \cdot 20^{16} = 20 \cdot 31 = 620 \pmod{33}$, adică
$w = 26 \pmod{33}$.

□

Ex #3 ElGamal aditiv. Se dă modulul $N = 1000$ cu generatorul $g = 143$. Cheia publică este $h = 3$ și mesajul criptat este $(c_1, c_2) = (2, 100)$. Aflați mesajul inițial w.

Dem
w

Știm $N = 1000$
$g = 143$
$h = 3$
$(c_1, c_2) = (2, 100)$.

Vrem w

Lucrăm peste $(\mathbb{Z}_{1000}, +)$ așador operațiile clasice din ElGamal se vor transforma astfel

$$\begin{cases} a^b \mapsto ab \\ a^{-1} \mapsto -a \\ ab \mapsto a+b \end{cases}$$

Astfel, cheia secretă se găsește ușor știind că $h = gk \bmod N$, ie $k = g^{-1}h \bmod N$.

Să observăm că g este inversabil ca generator pentru că $\gcd(143, 1000) = 1$, deci există $143^{-1} \bmod 1000$.

Aplicăm algoritmul lui Euclid și avem

$1000 = 143 \cdot 6 + 142$
$143 = 142 \cdot 1 + 1$
$142 = 1 \cdot 142 + 0$

deci $1 = 143 - 142 = 143 - (1000 - 143 \cdot 6) =$
$= 143 \cdot 7 - 1000$

Modulo $N=1000$ avem $143 \cdot 7 = 1 \pmod{1000}$, ie
$143^{-1} = 7 \pmod{1000}$

Calculăm, acum $k_s = g^{-1}h \pmod{1000}$
$k_s = 7 \cdot 3 \pmod{1000}$
$k_s = 21 \pmod{1000}$

Putem afla, acum, mesajul $m = c_2 - k_s c_1 \pmod{1000}$
$m = 100 - 21 \cdot 2 = 100 - 42 \pmod{1000} \iff$
$m = 58 \pmod{1000}$

□

Ex#4 ElGamal multiplicativ. Se dă modulul $p=29$ în grupul generat de $g=2$. Cheia publică este $h=19$ iar mesajul criptat este $(c_1, c_2) = (7, 21)$. Aflați mesajul m.

Dem
m

Lucrăm în $(\mathbb{Z}_{29}^*, \cdot)$
Știm că cheia publică h este dată de $h = g^k \bmod p$, unde k este cheia privată (de care avem nevoie). Cum lucrăm cu numere mici, putem afla k prin forță brută. Astfel, calculăm

$2^1 = 2 \pmod{29}$
$2^2 = 4 \pmod{29}$
$2^3 = 8 \pmod{29}$
$2^4 = 16 \pmod{29}$
$2^5 = 3 \pmod{29}$
$2^6 = 6 \pmod{29}$
$2^7 = 12 \pmod{29}$
$2^8 = 24 \pmod{29}$
$2^9 = 19 \pmod{29}$

Așador am găsit că $k = 9$.
Acum vrem să aflăm $m = c_2 (c_1^k)^{-1}$, ie
$m = 21 \cdot (7^9)^{-1} \pmod{29}$

Aplicăm algoritmul de exponențiere rapidă observând că $9 = 1+8$. Așador

$7^1 = 7 \pmod{29}$
$7^2 = 20 \pmod{29}$
$7^4 = 23 \pmod{29}$
$7^8 = 7 \pmod{29}$

Deci $7^9 = 7 \cdot 7^8 = 7 \cdot 7 = 7^2 = 20 \pmod{29}$

4/10

Acum aplicăm algoritmul lui Euclid pentru a afla $20^{-1} \pmod{29}$

$$29 = 20 \cdot 1 + 9$$
$$20 = 9 \cdot 2 + 2$$
$$9 = 2 \cdot 4 + 1$$
$$2 = 1 \cdot 2 + 0$$

de unde $1 = 9 - 2 \cdot 4 = 9 - (20 - 9 \cdot 2) \cdot 4 =$
$= 9 \cdot 9 - 20 \cdot 4 = (29 - 20) \cdot 9 - 20 \cdot 4 =$
$= 29 \cdot 9 - 20 \cdot 13$

Modulo 29 avem $-20 \cdot 13 = 1 \pmod{29}$, ie
$20 \cdot 16 = 1 \pmod{29}$, ie
$20^{-1} = 16 \pmod{29}$

Așadar $x = 21 \cdot 16 = 17 \pmod{29}$.

□

EX#5 Shamir Secret Sharing. Fie $P \in \mathbb{Z}_{29}[X]$ un polinom de grad 2. Considerăm perechile $(\alpha, P(\alpha))$ unde $\alpha \in \mathbb{Z}_{29} \setminus \{0\}$ și $P(\alpha) \in \mathbb{Z}_{29}$. Dacă avem trei astfel de perechi $(2,11), (4,27), (8,25)$ deduceți elementul secret $0 = P(0) \in \mathbb{Z}_{29}$.

Problema Avem n persoane. Fiecare submulțime de t persoane își poate reconstrui elementul secret, dar fiecare submulțime de $t+1$ persoane poate și primește acces.

↳ vezi exemplul cu chei și banca nucleară

Metoda lui Shamir

1) Se alege un corp $\mathbb{F}_q$ cu $q > n$
2) Elementul secret transmis este un element $a \in \mathbb{F}_q$ ales aleator. Se aleg t elemente aleatoare, cu neapărat diferite, $f_1, \dots, f_t \in \mathbb{F}_q$ și se consideră polinomul

$$f(X) = a + f_1 X + f_2 X^2 + \dots + f_t X^t \in \mathbb{F}_q[X]$$

3) Fiecare persoană primește o cheiță unică $x_i \in \mathbb{F}_q$. Persoana îi primește perechea $s_i = (x_i, f(x_i))$.

Teoremă Dată construcția de mai sus, fiecare submulțime de $t+1$ persoane poate recunoaște elementul secret $a = f(0)$, pe când fiecare submulțime de t persoane nu poate.

Demonstrație

Considerăm polinomul $P(x) = a + \alpha x + \beta x^2 \in \mathbb{Z}_{29}[x]$. Vrem să aflăm a, α și β. Așadar, considerăm sistemul

$$(S)\begin{cases} a + 2\alpha + 4\beta = 11 \\ a + 4\alpha + 16\beta = 27 \\ a + 8\alpha + 64\beta = 25 \end{cases} \Leftrightarrow \begin{cases} a + 2\alpha + 4\beta = 11 \\ a + 4\alpha + 16\beta = 27 \\ a + 8\alpha + 6\beta = 25 \end{cases}$$

$$\left[\begin{array}{ccc|c} 1 & 2 & 4 & 11 \\ 1 & 4 & 16 & 27 \\ 1 & 8 & 6 & 25 \end{array}\right] \xrightarrow[L_3 - L_1]{L_2 - L_1} \left[\begin{array}{ccc|c} 1 & 2 & 4 & 11 \\ 0 & 2 & 12 & 16 \\ 0 & 6 & 2 & 14 \end{array}\right] \xrightarrow[\frac{1}{2}L_3]{\frac{1}{2}L_2} \left[\begin{array}{ccc|c} 1 & 2 & 4 & 11 \\ 0 & 1 & 6 & 8 \\ 0 & 3 & 1 & 7 \end{array}\right] \xrightarrow{L_3 - 3L_2}$$

$$\rightarrow \left[\begin{array}{ccc|c} 1 & 2 & 4 & 11 \\ 0 & 1 & 6 & 8 \\ 0 & 0 & 12 & 12 \end{array}\right] \rightarrow \left[\begin{array}{ccc|c} 1 & 2 & 4 & 11 \\ 0 & 1 & 6 & 8 \\ 0 & 0 & 1 & 1 \end{array}\right] \xrightarrow[L_1 - 4L_3]{L_2 - 6L_3} \left[\begin{array}{ccc|c} 1 & 2 & 0 & 7 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 1 \end{array}\right] \xrightarrow{L_1 - 2L_2}$$

$$\rightarrow \left[\begin{array}{ccc|c} 1 & 0 & 0 & 3 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 1 \end{array}\right]$$

Prin urmare am găsit că $\begin{cases} a = 3 \\ \alpha = 2 \\ \beta = 1 \end{cases}$

OBS: Primul pas era să verificăm dacă sistemul (S) are soluții. Pentru asta trebuia să calculăm determinantul

$$\Delta = \begin{vmatrix} 1 & 2 & 4 \\ 1 & 4 & 16 \\ 1 & 8 & 64 \end{vmatrix} = (1-2)(2-4)(4-1) = 1 \cdot 2 \cdot 3 = 6 \neq 0$$

Cum $\gcd(6, 29) = 1$, deducem că sistemul (S) are soluții.

□

6/10

Ex #6 Shamir secret sharing in the field $\mathbb{Z}_{41}$. Se evaluează un polinom necunoscut de grad doi $f \in \mathbb{Z}_{41}[X]$. Trei zeități au perechile $(x, f(x)) \in \mathbb{Z}_{41}^2$ care sunt $(1,10), (2,26), (3,14)$. Găsiți cheia secretă $f(0)$.

Deci

Considerăm polinomul $f(x) = a + bx + cx^2$. Sistemul

$$\begin{cases} a + b + c = 10 \\ a + 2b + 4c = 26 \\ a + 3b + 9c = 14 \end{cases}$$

Rezolvăm sistemul folosind calculele modulo 41

$$\left[\begin{array}{ccc|c} 1 & 1 & 1 & 10 \\ 1 & 2 & 4 & 26 \\ 1 & 3 & 9 & 14 \end{array}\right] \xrightarrow[L_3 - L_1]{L_2 - L_1} \left[\begin{array}{ccc|c} 1 & 1 & 1 & 10 \\ 0 & 1 & 3 & 16 \\ 0 & 2 & 8 & 4 \end{array}\right] \rightarrow \left[\begin{array}{ccc|c} 1 & 1 & 1 & 10 \\ 0 & 1 & 3 & 16 \\ 0 & 1 & 4 & 2 \end{array}\right] \xrightarrow{L_3 - L_2}$$

$$\rightarrow \left[\begin{array}{ccc|c} 1 & 1 & 1 & 10 \\ 0 & 1 & 3 & 16 \\ 0 & 0 & 1 & 27 \end{array}\right] \xrightarrow[L_1 - L_3]{L_2 - 3L_3} \left[\begin{array}{ccc|c} 1 & 1 & 0 & 24 \\ 0 & 1 & 0 & 17 \\ 0 & 0 & 1 & 27 \end{array}\right] \xrightarrow{L_1 - L_2} \left[\begin{array}{ccc|c} 1 & 0 & 0 & 7 \\ 0 & 1 & 0 & 17 \\ 0 & 0 & 1 & 27 \end{array}\right]$$

Așadar $\begin{cases} a = 7 \\ b = 17 \\ c = 27 \end{cases}$

Deci elementul secret este $a = f(0) = 7$.

□

Ex #7 Decideți dacă 8 este pătrat modulo 23.

Deci

Var 1. Ne vom folosi de simbolul lui Legendre. Dacă $\left(\frac{8}{23}\right) = 1$, atunci 8 este pătrat modulo 23.

Criteriul lui Euler $\Rightarrow$ [p prim impar și $\gcd(a,p) = 1$ atunci $a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right) \bmod p$

Evident $\left.\begin{array}{l} \cdot\ 23 \text{ prim impar} \\ \cdot\ \gcd(2^3, 23) = 1 \end{array}\right\} \Rightarrow 8^{\frac{23-1}{2}} = \left(\frac{8}{23}\right) \bmod 23$

7/10

$8^{\frac{23-1}{2}} = 8^{11} = 8^{1+2+8} \mod 23$

- $8^2 = 64 = -5 \mod 23$
- $8^4 = 25 = 2 \mod 23$
- $8^8 = 4 \mod 23$

Deci $8^{11} = 8 \cdot (-5) \cdot 4 = 8 \cdot (-20) = 8 \cdot 3 = 24 = 1 \mod 23$, adică $\left(\frac{8}{23}\right) = 1$, deci 8 este pătrat modulo 23.

Var 2 Folosim ~~[illegible]~~ faptul că $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ și avem

$$\left(\frac{8}{23}\right) = \left(\frac{2^3}{23}\right) = \left(\frac{2}{23}\right)^3 = \left(\frac{2}{23}\right) \cdot \left(\frac{2}{23}\right)^2 = \left(\frac{2}{23}\right) = (-1)^{\frac{23^2-1}{8}} = (-1)^{\frac{528}{8}} = (-1)^{66} = 1$$

□

Ex #8 Găsiți o valoare pentru expresia $\sqrt[7]{23} \mod 77$.

Deci
mod
Să observăm că $23 \in \mathbb{Z}_{77}^*$, $\gcd(23, 77) = 1$.
Știm că $\#\mathbb{Z}_{77}^* = \varphi(77) = \varphi(7)\varphi(11) = 6 \cdot 10 = 60$.
Calculăm

$$\sqrt[7]{23} \mod 77 = 23^{1/7} \mod 77 = 23^{(7^{-1} \mod \varphi(77))} \mod 77 =$$
$$= 23^{(7^{-1} \mod 60)} \mod 77.$$

Folosind algoritmul lui Euclid, calculăm $7^{-1} \mod 60$.

$$\left.\begin{aligned} 60 &= 7 \cdot 8 + 4 \\ 7 &= 4 \cdot 1 + 3 \\ 4 &= 3 \cdot 1 + 1 \\ 3 &= 1 \cdot 3 + 0 \end{aligned}\right\} \Rightarrow$$

$$\Rightarrow 1 = 4 - 3 = 4 - (7 - 4) = 4 \cdot 2 - 7 =$$
$$= (60 - 7 \cdot 8) \cdot 2 - 7 = 60 \cdot 2 - 7 \cdot 17 \pmod{60}$$

$$\Rightarrow -7 \cdot 17 = 1 \pmod{60}$$
$$7 \cdot 43 = 1 \pmod{60}$$
$$43 = 7^{-1} \pmod{60}$$

Deci $\sqrt[7]{23} \mod 77 = 23^{43} \mod 77$.

Observăm că $43 = 1 + 2 + 8 + 32$. Aplicăm exponențiere rapidă 8/10

Și avem $23^1 = 23 \pmod{77}$

$23^2 = -10 \pmod{77}$

$23^4 = 100 = 23 \pmod{77}$

$23^8 = -10 \pmod{77}$

$23^{16} = 23 \pmod{77}$

$23^{32} = -10 \pmod{77}$

Așadar $23^{43} = 23 \cdot 23^2 \cdot 23^8 \cdot 23^{32} =$

$= 23 \cdot (-10) \cdot (-10) \cdot (-10) =$

$= 23 \cdot 23 \cdot (-10) =$

$= (-10) \cdot (-10) =$

$= 23 \pmod{77}$

În concluzie $\sqrt[7]{23} \bmod 77 = 23 \bmod 77$.

□

Ex #9 RSA. Un mesaj este criptat cu RSA modulo 91, cheia publică $e = 5$, mesajul criptat $c = 3$. Aflați m.

Deci

Observăm că $91 = 7 \cdot 13$. Așadar $\varphi(91) = \varphi(7)\varphi(13) = 6 \cdot 12 = 72$.

Știm că $ed = 1 \pmod{\varphi(n)}$, deci $d = e^{-1} \pmod{\varphi(n)}$. La noi $d = 5^{-1} \pmod{72}$

Euclid: $72 = 5 \cdot 14 + 2$

$5 = 2 \cdot 2 + 1$

$2 = 1 \cdot 2 + 0$

$\Rightarrow 1 = 5 - 2 \cdot 2 = 5 - (72 - 5 \cdot 14) \cdot 2 = 5 \cdot 29 - 72 \cdot 2 \pmod{72}$

$1 = 5 \cdot 29 \pmod{72}$

$5^{-1} = 29 \pmod{72} \Rightarrow \boxed{d = 29}$

Știm că $m = c^d \pmod{n}$, deci $m = 3^{29} \pmod{91}$.

Avem că $29 = 1 + 4 + 8 + 16$. Calculăm

- $3^1 = 3 \pmod{91}$
- $3^2 = 9 \pmod{91}$
- $3^4 = -10 \pmod{91}$
- $3^8 = 9 \pmod{91}$
- $3^{16} = -10 \pmod{91}$

Agador $3^{29} = 3 \cdot 3^4 \cdot 3^8 \cdot 3^{16} =$

$= 3 \cdot (-10) \cdot 9 \cdot (-10) =$

$= 3 \cdot 9 \cdot 9 =$

$= 3 \cdot (-10) =$

$= -30 =$

$= 61 \pmod{91}.$

Deci $\boxed{m = 61}$

□