Recuperare Protocoale criptografice

- Sala 202
- Stoilow
- 20.05.2025, 8-10

} Examen

Ex #1 Arătați că polinomul x^3+x^2+1 este ireduct. peste $\mathbb{F}_2$. Fie ω o rădăcină a polinomului.
Calculați elementul $(\omega^2+\omega+1)^{-1}$ în $\mathbb{F}_8=\mathbb{F}_2[\omega]$

Dem

Fie $f(x)=x^3+x^2+1$. Observăm că f nu are zerouri peste $\mathbb{F}_2$ deoarece

$$f(0)=0+0+1 \overset{2}{=} 1 \quad \text{și}$$
$$f(1)=1+1+1 \overset{2}{=} 1$$

Dacă ar fi fost reductibil, ar fi găsit un fact. de deg $=1$ și un factor de deg $=2$.

Dacă ω este rădăcină a lui f, regula de calcul din $\mathbb{F}_8=\mathbb{F}_2[\omega]$ este $\omega^3=\omega^2+1$, iar elementele din $\mathbb{F}_8$ sunt de forma $a+b\omega+c\omega^2$ cu $a,b,c\in\mathbb{F}_2$. Căutăm un astfel de element care să satisfacă

$$(\omega^2+\omega+1)(a+b\omega+c\omega^2)=1$$

Calculăm

$c\omega^4 + (b+c)\omega^3 + (a+b+c)\omega^2 + (a+b)\omega + a = 1$ (*)

Stim că $\omega^3 = \omega^2 + 1$, deci

$$\omega^4 = \omega^3 + \omega$$
$$= \omega^2 + 1 + \omega$$

Din (*), avem:

$$c(\omega^2+1+\omega) + (b+c)(\omega^2+1) + (a+b+c)\omega^2 + (a+b)\omega + a = 1$$

$$(c+b+c+a+b+c)\omega^2 + (c+a+b)\omega + (c+b+c+a) = 1 \pmod 2$$

Așadar

$$(a+c)\omega^2 + (a+b+c)\omega + (a+b) = 1 + 0\cdot\omega + 0\cdot\omega^2 \pmod 2$$

$$\Rightarrow \begin{cases} a+b = 1 & (1) \\ a+b+c = 0 & (2) \\ a+c = 0 & (3) \end{cases} \pmod 2$$

(3) $\Rightarrow a = c$

(2) $\Rightarrow 2a + b = 0 \Rightarrow \boxed{b = 0}$

(1) $\Rightarrow a + 0 = 1 \Rightarrow \boxed{a = 1} \Rightarrow \boxed{c = 1}$

Prin urmare, $(a, b, c) = (1, 0, 1)$, deci

$$(\omega^2 + \omega + 1)^{-1} = 1 + \omega^2$$

Verificare:

$$(1+\omega+\omega^2)(1+\omega^2) = 1+\omega^2+\omega+\omega^3+\omega^2+\omega^4$$
$$= 1+\omega+\omega^2+1+\omega^2+1+\omega$$
$$= 1. \quad \square$$

EX #2 Shamir Secret Sharing. Fie $P \in \mathbb{Z}_{19}[X]$ un pol. de $\deg = 2$. Se consideră următoarele perechi $(\alpha, P(\alpha))$ unde $\alpha \in \mathbb{Z}_{19}^*$ și $P(\alpha) \in \mathbb{Z}_{19}$: $(10,16)$, $(11,0)$ și $(12,5)$. Deduceți secretul partajat $s = P(0) \in \mathbb{Z}_{19}$.

Demo

Considerăm $P(X) = s + aX + bX^2 \in \mathbb{Z}_{19}[X]$.

atunci avem

$$\begin{cases} s + 10a + 100b \overset{19}{=} 16 \\ s + 11a + 121b \overset{19}{=} 0 \\ s + 12a + 144b \overset{19}{=} 5 \end{cases} \iff$$

$$\begin{cases} s + 10a + 5b = 16 \\ s + 11a + 4b = 0 \\ s + 12a + 11b = 5 \end{cases}$$

$$\left[\begin{array}{ccc|c} 1 & 10 & 5 & 16 \\ 1 & 11 & 7 & 0 \\ 1 & 12 & 11 & 5 \end{array}\right] \xrightarrow[L_3 - L_1]{L_2 - L_1} \left[\begin{array}{ccc|c} 1 & 10 & 5 & 16 \\ 0 & 1 & 2 & 3 \\ 0 & 2 & 6 & 8 \end{array}\right] \xrightarrow{\frac{1}{2}L_3}$$

$$\left[\begin{array}{ccc|c} 1 & 10 & 5 & 16 \\ 0 & 1 & 2 & 3 \\ 0 & 1 & 3 & 4 \end{array}\right] \xrightarrow{L_3 - L_2} \left[\begin{array}{ccc:c} 1 & 10 & 5 & 16 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 1 \end{array}\right] \xrightarrow[L_1 - 5L_3]{L_2 - 2L_3}$$

$$\left[\begin{array}{ccc:c} 1 & 10 & 0 & 11 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{array}\right] \xrightarrow{L_1 - 10L_2} \left[\begin{array}{c:c} I_3 & \begin{matrix}1\\1\\1\end{matrix} \end{array}\right]$$

$$\Rightarrow \begin{cases} a = 1 \\ a = 1 \\ b = 1 \end{cases}$$

□

RSA. O persoană criptează mesajul m mod 85. folosind cheia publică $e = 9$ și obține $c = 10$. Decriptați mesajul folosind funcții

a) $\varphi(n)$

b) $\lambda(n)$

Dem

[a] Știm $n = 85 = 5 \cdot 17$

$ed = 1 \mod \varphi(n)$ (*)

$\varphi(n) = (p-1)(q-1) = (5-1)(17-1) = 4 \cdot 16$

$\Rightarrow \varphi(85) = 64$

Din (*) $\Rightarrow d = 9^{-1} \mod 64$.

Calc. $9^{-1} \bmod 64$ folosind Euclid extins.

$$64 = 9 \cdot 7 + 1 \Rightarrow 1 = 64 - 9 \cdot 7 \pmod{64}$$

$$\Rightarrow 1 = -9 \cdot 7 \pmod{64}$$

$$\Rightarrow 1 = 9 \cdot 57 \pmod{64}.$$

Deci $d = 57 \pmod{64}$.

Calculăm $a_w = c^d \pmod{a_w}$, ie

$$a_w = 10^{57} \pmod{85}$$

folosind alg. de exponentiere rapidă.

$$57 = 1 + 56$$

$$57 = 32 + 16 + 8 + 1$$

Avem

$$\left.\begin{aligned} 10^2 &= 15 \\ 10^4 &= 55 \\ 10^8 &= 50 \\ 10^{16} &= 35 \\ 10^{32} &= 35 \end{aligned}\right\} \Rightarrow a_w = 10^{57} = 35 \cdot 35 \cdot 50 \cdot 10$$

$$= 75.$$

$$\Rightarrow \boxed{w = 75}$$

□

b) $\lambda(n)$

Știm $a_w = 85 = 5 \cdot 17$

$$ed = 1 \pmod{\lambda(n)}$$

$$\lambda(n) = \text{lcm}(5-1, 17-1) = \text{lcm}(4, 16) = 16$$

Calculăm $d = 9^{-1} \pmod{16}$ cu Euclid extins.

$$\begin{aligned} 16 &= 9 \cdot 1 + 7 \\ 9 &= 7 \cdot 1 + 2 \\ 7 &= 2 \cdot 3 + 1 \end{aligned} \Rightarrow 1 = 7 - 2 \cdot 3$$

$$= 7 - (9-7) \cdot 3$$

$$= 7 \cdot 4 - 9 \cdot 3$$

$$= (16-9) \cdot 4 - 9 \cdot 3$$

$\Rightarrow 1 = 16 \cdot 4 - 9 \cdot 7 \pmod{16} \Rightarrow 1 = -9 \cdot 7 \pmod{16}$

$\Rightarrow d = -7 = 9 \pmod{16} \Rightarrow \boxed{d = 9}$

Descriptiva: $a_n = c^d \pmod{n}$

$\Rightarrow a_n = 10^9 \pmod{85}$

Exponențiere rapidă: $9 = 8 + 1$

$10^2 = 15$

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

$10^8 = 50$

Așadar $a_n = 50 \cdot 10 = 75 \Rightarrow \boxed{n = 75}$.

□

Algoritm de aflare a logaritmului discret

Baby Step - Giant Step

OBS • Brute force → 14 pași calc. mod 19.

VREM x a.î. $\boxed{2^x = 6 \pmod{19}}$

Algoritm

știm y, g și x. Vreau $g^x = y \pmod p$

x se n. logaritmul discret a lui y

$$x = \log_g y \pmod p$$

Folosim faptul că fiecare $x < p$ se poate scrie

$$x = \lceil \sqrt{p} \rceil x_1 + x_2, \text{ unde } 0 \le x_1, x_2 \le \lfloor \sqrt{p} \rfloor$$

$\lceil 3{,}14 \rceil = 4 \quad \lfloor 3{,}14 \rfloor = 3$

Avem

$$y = g^x = g^{\lceil \sqrt{p} \rceil x_1 + x_2} = \left(g^{\lceil \sqrt{p} \rceil}\right)^{x_1} \cdot g^{x_2}$$

$$\Leftrightarrow \quad y \cdot \left(g^{-1}\right)^{x_2} = \left(g^{\lceil \sqrt{p} \rceil}\right)^{x_1}$$

Calculăm $g^{-1} \bmod p =: z$ și $g^{\lceil \sqrt{p} \rceil} \pmod p = \omega$

Scriem resturile

$$L_1 = \{(x_1, \omega^{x_1}) \mid x_1 = 0, 1, \dots, \lfloor \sqrt{p} \rfloor\}$$

$$L_2 = \{(x_2, yz^{x_2}) \mid x_2 = 0, 1, \dots, \lfloor \sqrt{p} \rfloor\}$$

Se caută o coliziune de tipul $(x_1, \delta) \in L_1$ și $(x_2, \delta) \in L_2$. Atunci $x = \lceil \sqrt{p} \rceil x_1 + x_2$ este log-disc-căutat.

$\boxed{2^x \equiv 6 \pmod{19}}$ $\quad p = 19 \quad y = 6$
$g = 2$

OBS: $\sqrt{19} \approx 4{,}35$

$\lceil \sqrt{19} \rceil = 5$ iar $\lfloor \sqrt{19} \rfloor = 4$

Căutăm $x < p$ cu $x = 5x_1 + x_2$, unde

$$0 \leq x_1, x_2 \leq 4$$

Calculăm $g^{-1} \bmod p = 2^{-1} \pmod{19}$ (Euclid)

$\Rightarrow \dots \Rightarrow 2^{-1} \equiv 10 \pmod{19} \Rightarrow \boxed{z = 10}$

Calculăm $g^{\lceil \sqrt{p} \rceil} \bmod p = 2^5 \bmod 19$ (exp. rapidă)

$\Rightarrow \dots \Rightarrow 2^5 \equiv 13 \pmod{19} \Rightarrow \boxed{\omega = 13}$

Construim listele

x_1

$L_1 = \{(0,1); (1,13); (2,17), (3,12), (4,4)\}$

x_2

$L_2 = \{(0,6); (1,3); (2,11); (3,17); (4,17)\}$

$\omega^0 = 13^0 = 1$

$\omega^1 = 13^1 = 13$

$\omega^2 = 13^2 = 17$

$\omega^3 = 13^3 = 12$

$\omega^4 = 13^4 = 4$

$yz^0 = 6 \cdot 10^0 = 6$

$yz^1 = 6 \cdot 10^1 = 3$

$yz^2 = 6 \cdot 10^2 = 11$

$yz^3 = 6 \cdot 10^3 = 15$

$yz^4 = 6 \cdot 10^4 = 17$

Găsim coliziunea $\cdot (x_1, 8) = (2, 17) \in L_1$

$\cdot (x_2, 8) = (4, 17) \in L_2$

și calculăm $x = 5 \cdot x_1 + x_2 \pmod{19}$

$x = 5 \cdot 2 + 4 = 14 \pmod{19}$.

□

nicoleta.dumitru@my.fmi.unibuc.ro