19.01.2024

SSI lab. 14

S. Legendre:

$a \in \mathbb{Z}_p$, a = rest pătratic

dacă $\exists\, b \in \mathbb{Z}_p$: $b^2 \equiv a \pmod p$

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & a = \text{rest pătr. mod } p \\ -1, & a \neq \text{— " —} \\ 0, & a \equiv 0 \pmod p \end{cases}$$

$\mathbb{Z}_{11}$:

a	0	± 1	± 2	± 3	± 4	± 5
$a^2 \bmod 11$	0	1	4	9	5	3

$\mathbb{Z}_{11}$ = resturile pătratice $\{1, 3, 4, 5, 9\}$

$2, 6, 7, 8$ NU SUNT resturi pătratice

Proprietăți:

1. $\left(\frac{ab}{p}\right) = \frac{a}{p} \cdot \frac{b}{p}$
2. $\frac{a}{p} = a^{\frac{p-1}{2}} \bmod p$
3. $\frac{2}{p} = (-1)^{\frac{p^2-1}{8}}$
4. $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot \left(\frac{q}{p}\right)$ cu p, q prime impare distincte.

S. Jacobi:

$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$

$$\frac{a}{n} = \frac{a}{p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}} = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdot \ldots \cdot \left(\frac{a}{p_k}\right)^{\alpha_k}$$

exemplu: $\left(\frac{74}{131}\right) = \left(\frac{2}{131}\right) \cdot \underbrace{\left(\frac{37}{131}\right)}_{\text{folosim proprietatea}} =$

$= (-1)^{\frac{131^2-1}{8}} \cdot \left(\frac{131}{37}\right) \cdot (-1)^{\frac{131-1}{2} \cdot \frac{37-1}{2}} =$

reducere modulară

$= (-1)^{\frac{130 \cdot 132}{8}} \cdot \left(\frac{20}{37}\right) \cdot (-1)^{\frac{130}{2} \cdot \frac{36}{2}} =$

$= (-1)^{65 \cdot 33} \cdot \left(\frac{20}{37}\right) \cdot \cancel{(-1)^{65 \cdot 18}} =$

$= (-1) \left(\frac{2}{37}\right)^2 \cdot \frac{5}{37} =$

$= (-1) \frac{2}{5} \cdot (-1) \cdot (-1)^{\frac{5^2-1}{3}} =$

$= 1$

$\Rightarrow$ 74 este rest pătratic modulo 131

cât este?

$(\pm 27)^2 \equiv 74 \pmod{131}$

Cheie

$(N=77,\ e=13)$ - cheie publică RSA

cheia publică de la RSA o folosim la criptare

$d = ?$

$N = 7 \cdot 11,\ p = 7,\ q = 11$

$\varphi(N) = (p-1)(q-1) = 6 \cdot 10 = 60$

$e = 13$, $\gcd(13, 60) = 1$

$d = 13^{-1} \pmod{60}$

Alg. lui Euclid extins (:))

$\alpha \cdot 60 + \beta \cdot 13 = \gcd(60, 13) = 1$

q_{i-1}	r_i	s_i	t_i
-	60	1	0
-	13	0	1
4	8	1	-4
⋮			

$5 \cdot 60 + (-23) \cdot 13 = 1$

mod 60 ; $-23 \cdot 13 \equiv 1 \pmod{60}$

$13^{-1} \equiv -23 \equiv 37 \pmod{60}$

$\Rightarrow$ Cheia privată este: $(N = 77,\ d = 37)$

LFSR ! trecerea de la LFSR la diagonală / exemple în carte

generați primii 10 biți

$\boxed{\text{El Gamal}}$ Bob → Alice

bagat pe DLP (problema logaritmului discret) / RSA e bagat pe mult. factorizării

Bob → Alice

① Gen. cheile | Alice face asta

- $G = \langle g \rangle$ → grupul G e generat de g
  ord $\cancel{g} = q$ prim
- se alege random ($x \underset{\$}{\in} \{1, \ldots, q-1\}$ ~~start. cu~~ ~~h~~
- $h := g^x \in G$

Public key (pt. criptare) $= (G, \cancel{q}\, h, q)$
Private key (pt decript) $= x$
↳ DOAR LA ALICE

$x = \log_g h$

CRIPTARE (BOBIȚĂ)
② $m \in G \longleftrightarrow M$ = mesaj

- $k \underset{\$}{\in} \{1, \ldots, q-1\}$ cheie efemeră
- $s := h^k \in G$
- $c_1 := g^k \in G$
- $c_2 = m \cdot s \in G$

Bob trimite (c_1, c_2)

③ DECRIPTARE (Alice)

- $c_1^{\,x} = s \in G$
- $c_2 \cdot s^{-1} = \boxed{m}$

Reutilizarea lui k:

$\cancel{c_1 = c_1'}$ (c_1, c_2) = primul ciphertext

c_1', c_2' = al 2 lea

$c_1 = c_1' = g^k \Rightarrow s = s'$

$c_2 = m \cdot s$

$c_2' = m' \cdot s' = m' \cdot s'$

Dacă adversarul află $m \Rightarrow s' = c_2^{-1} \cdot m$

$\Rightarrow c_2' \cdot s^{-1} = m'$ $\Rightarrow$ NU refolosim k