Examen de Protocoale Criptografice - Reexaminare 3 iunie 2021

May 16, 2022

1 Problemă Elgamal aditiv

S-au ales $n = 63$ și $g = 16$.

(a)

S-au ales $x = 5$ și $y = 7$. Bob va cripta $m = 9$.

1. Cheia publică a lui Alice este $h = x \cdot g = 5 \cdot 16 \equiv 17 \pmod{n = 63}$.
2. Bob calculează $c_1 = y \cdot g = 7 \cdot 16 \equiv 49 \pmod{n = 63}$ și $c_2 = y \cdot h + m = 7 \cdot 17 + 9 \equiv 2 \pmod{n = 63}$.
3. Bob trimite mesajul criptat $(c_1, c_2) = (49, 2)$ lui Alice.
4. Alice decriptează mesajul $m = (x \cdot c_1)^{-1} + c_2 = (5 \cdot 49)^{-1} + 2 \equiv 56^{-1} + 2 \equiv 7 + 2 \equiv 9 \pmod{n = 63}$.

Obs. $56^{-1} \bmod 63 = 63 - 56 = 7$ (inversul aditiv).

(b)

1. Eva calculează $g^{-1} \bmod n = 16^{-1} \bmod 63 = 63 - 16 = 47$ (inversul aditiv).
2. Apoi calculează cheia privată a lui Alice: $h + x \cdot g^{-1} \equiv 0 \pmod{n} \Leftrightarrow 17 + x \cdot 47 \equiv 0 \pmod{n} \Leftrightarrow x \cdot 47 \equiv 46 \pmod{n} \Leftrightarrow x \equiv 46 \cdot 59 \pmod{n} \Leftrightarrow x \equiv 5 \pmod{n}$.

Obs. Inversul multiplicativ al lui 47 mod 63 = 59 este calculat astfel:

$$63 = 1 \cdot 47 + 16$$
$$47 = 2 \cdot 16 + 15$$
$$16 = 1 \cdot 15 + 1$$
$$1 = 16 - 15 = 16 - (47 - 2 \cdot 16) = 3 \cdot 16 - 47 = 3 \cdot (63 - 47) - 47 = -4 \cdot 47 = 59 \cdot 47 = 1 \pmod{n = 63}$$

2 Problemă Elgamal multiplicativ

Avem $p = 19$, $g = 2$, $h = 9$. Vom decripta $(c_1, c_2) = (10, 11)$ folosind $m = (c_1^x)^{-1} c_2$.

Oservăm că $2 \cdot 10 \bmod 19 = 1$, deci $z = g^{-1} \bmod n = 10$. Aplicăm **Baby Step - Gigant Step** pentru a calcula $log_g h = x$.

1. $ceil(\sqrt{p}) = 5$, $floor(\sqrt{p}) = 4$, deci $k = g^{ceil(\sqrt{p})} = 2^5 = 32 \equiv 13 \pmod{p}$.
2. $L_1 = \{(x_1, k^{x_1}) \mid x_1 \in \overline{0, floor(\sqrt{p})}\} = \{(0,1), (1,13), (2,17), (3,12), (4,4)\}$
3. $L_2 = \{(x_2, hz^{x_2}) \mid x_2 \in \overline{0, floor(\sqrt{p})}\} = \{(0,9), (1,14), (2,7), (3,13), (4,16)\}$
4. $x = x_1 \cdot floor(\sqrt{p}) + x_2 = 8$

Atunci $c_1^x \bmod n = 10^8 \bmod 19 = 17$. $(c_1^x)^{-1} = 9$. $m = 9 \cdot 11 \bmod 19 = 4$.

3 Problemă RSA

$N = 91 = 7 \cdot 13$. $\lambda(N) = \text{lcm}(\lambda(7), \lambda(13)) = \text{lcm}(\phi(7), \phi(13)) = \text{lcm}(6, 12) = 12$.

$d = e^{-1} \bmod \lambda(N)$. $e = 5$, deci $d = 5$.

$m = c^d \bmod \lambda(N) = 5^5 \bmod 12 = 5$.

4 Problemă Goldwasser-Micali

$N = 77 = 7 \cdot 11$. $(23, 53, 36, 41) \bmod 7 = (2, 4, 1, 6) = (3^2, 2^2, 1^2, 6) \bmod 7$. Atunci mesajul este $(0, 0, 0, 1)$.

5 Problemă Shamir Secret Sharing

Avem $P(X) = aX^2 + bX + c$ și $(1, 11), (2, 13), (3, 16)$ perechi $(x, P(x))$.

$$\begin{aligned} a + b + c &= 11 \\ 4a + 2b + c &= 13 \\ 9a + 3b + c &= 16 \end{aligned}$$

Deci $a = b = c = 10$ și $P(X) = 10(X^2 + X + 1)$. $P(0) = 0$

6 Problemă Secure Multiparty Computation over $\mathbb{Z}$