13 mai 2019

IC - SEMINARUL NR 3

Criptosistemul GOLDWASSER - MICALI

- p prim, $a \in \mathbb{Z}$ reziduu pătratic mod p dacă $\exists x \in \mathbb{Z}_p^*$ a.î. $a \equiv x^2 \bmod p$

$(a,p)=1$

Simbolul Legendre a lui $a \bmod p$: $\left(\frac{a}{p}\right) \overset{def}{=} \begin{cases} 1, & \text{dacă } a \text{ reziduu pătratic mod } p \\ -1, & \text{altfel} \end{cases}$

Criteriul lui Euler: $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$, unde p prim, impar
$(a,p)=1$

$\left(\frac{a}{p}\right) = \left(\frac{a \bmod p}{p}\right)$; $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$; $\left(\frac{a^k}{p}\right) = \left(\frac{a}{p}\right)^k = \left(\frac{a}{p}\right)^{k \bmod 2}$

Fie $n = p \cdot q$, p, q prime distincte

$(a,n)=1$

Simbolul Jacobi $\left(\frac{a}{n}\right) \overset{def}{=} \left(\frac{a}{p}\right)\left(\frac{a}{q}\right)$

Prop 1: $a \in \mathbb{Z}$, $(a,n)=1$

a reziduu pătratic mod $n \Leftrightarrow$ a reziduu pătratic mod p și
— " — q

deci $\exists a$, $\left(\frac{a}{n}\right) = 1$, dar a NU este reziduu pătratic mod n $\left(\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1\right)$

- cheia publică: $n = p \cdot q$, $y \in \mathbb{Z}_n^*$ $\left(\frac{y}{p}\right) = \left(\frac{y}{q}\right) = -1$ (y este un elem. cu simb Jacobi $= 1$, dar y nu e reziduu pătratic)

cheia privată: p, q prime, impare, distincte

Criptare: $m \in \{0,1\}$, $enc(m) = y^m \cdot \alpha^2 \bmod n$, $\alpha \in \mathbb{Z}_n^*$ generat aleatoriu

Decriptare: $dec(c) = \begin{cases} 0, & \text{dacă } \left(\frac{c}{p}\right) = 1 \\ 1, & \text{altfel} \end{cases}$

Obs: $\forall c$ criptotext G-M, $\left(\frac{c}{n}\right) = 1$

Exerciții

(4p) 1. Dem. că $\forall c$ criptotext GM, $\left(\frac{c}{p}\right)=1 \Leftrightarrow c=enc(0)$

(2p) 2. Fie $p=3, q=7, n=21, y=20$

GM cheia publică: $n=21, y=20$

cheia privată: $p=3, q=7$

Decriptați $c=5$.

(2p) 3. Dem că $\forall m_1, m_2 \in \{0,1\}$, $dec(enc(m_1) \cdot enc(m_2)) = m_1 \oplus m_2$

$\uparrow$
înmulțire mod n

(2p) 4. Prezentați un algoritm eficient care, având la intrare cheia publică și un criptotext c, să construiască un alt criptotext c' a.î. $dec(c)=dec(c')$

Rezolvare

1. „$\Rightarrow$"

$\left(\frac{c}{p}\right)=1 \Rightarrow dec(c)=0$

$\Rightarrow enc(0)=c$

„$\Leftarrow$"

$enc(0)=c \Leftrightarrow c=y^0 \alpha^2 \bmod n$

$\Leftrightarrow c=\alpha^2 \bmod n$

$\Rightarrow c$ reziduu pătratic mod n $\Rightarrow$

$\Rightarrow c$ reziduu pătratic mod p $\Leftrightarrow \left(\frac{c}{p}\right)=1$

2. $dec(\overset{c}{5})=?$

$\left(\frac{c}{p}\right) \equiv c^{\frac{p-1}{2}} \bmod p \Leftrightarrow \left(\frac{c}{p}\right) \equiv 5^{\frac{3-1}{2}} \bmod 3 \Leftrightarrow \left(\frac{c}{p}\right) \equiv 5^1 \bmod 3 \equiv 2 \bmod 3$

$\Rightarrow \underline{dec(c)=1}$

3. $enc(m_1) \cdot enc(m_2) = y^{m_1} \alpha_1^2 \bmod n \cdot y^{m_2} \alpha_2^2 \bmod n = y^{m_1+m_2} \alpha_1^2 \alpha_2^2 \bmod n =$

$$= y^{m_1+m_2} (\alpha_1 \alpha_2)^2 \bmod n$$

$dec(enc(m_1) \cdot enc(m_2)) = dec\left(y^{m_1+m_2} (\alpha_1\alpha_2)^2 \bmod n\right)$

$$\left(\frac{y^{m_1+m_2} (\alpha_1\alpha_2)^2 \bmod n}{p}\right) = \left(\frac{y^{m_1+m_2} \bmod n}{p}\right) \cdot \left(\frac{(\alpha_1\alpha_2)^2 \bmod n}{p}\right) =$$

$$= \left(\frac{y^{m_1+m_2} \bmod n}{p}\right) \cdot 1 = \left(\frac{y}{p}\right)^{m_1+m_2} = \left(\frac{y}{p}\right)^{m_1+m_2 \bmod 2} = \left(\frac{y}{p}\right)^{m_1 \oplus m_2} = \begin{cases} 1, & m_1 \oplus m_2 = 0 \\ -1, & m_1 \oplus m_2 = 1 \end{cases}$$

$$\Rightarrow dec(enc(m_1) \cdot enc(m_2)) = \begin{cases} 0, & \text{dacă } m_1 \oplus m_2 = 0 \\ 1, & \text{dacă } m_1 \oplus m_2 = 1 \end{cases}$$

$$\Rightarrow dec(enc(m_1) \cdot enc(m_2)) = m_1 \oplus m_2$$

4. Input: n, y

c

Output: $c' \neq c$ a.î. $dec(c') = dec(c)$

$c' = c^3 \bmod n \Rightarrow \left(\frac{c'}{p}\right) = \left(\frac{c^3 \bmod n}{p}\right) = \left(\frac{c}{p}\right)^3 = \left(\frac{c}{p}\right)$

$2k+1, k \in \mathbb{Z}^*$

$$\Rightarrow \underline{dec(c') = dec(c)}$$