Criptosistemul El Gamal

6 mar 2019

Seminarul nr 2

- criptosistem cu chei publice
- cheia publică - p, q nr. prime a.î. $q \mid (p-1)$

  ~ 1024 biți, 160 biți

  - $\alpha \in \mathbb{Z}_p^*$ el de ordin q, $\alpha^q \equiv 1 \bmod p \wedge \forall 1 \le q' < q$, $\alpha^{q'} \not\equiv 1 \bmod p$
  - $\beta = \alpha^a \bmod p$

- cheia privată $a \in \mathbb{Z}_q^*$

$x \in \mathbb{Z}_p^*$ $\quad enc(x) = (\gamma, \delta)$, $\begin{cases} \gamma = \alpha^k \bmod p \\ \delta = x \cdot \beta^k \bmod p \end{cases}$ $k \in \mathbb{Z}_q^*$ aleator

$$dec((\gamma, \delta)) = \delta \cdot (\gamma^{-1})^a \bmod p$$

Exerciții

(5p) 1. Dem. că $dec(enc(x)) = x$, $\forall x \in \mathbb{Z}_p^*$

(3p) 2. Dem. că dacă la criptarea a 2 mesaje dif x_1 și x_2 se folosește același k, atunci având aceleași (γ_1, δ_1) și (γ_2, δ_2) și unul din plaintexte (x_1), se poate determina ușor al doilea plaintext (x_2). (fără a avea cheia privată)

(2p) 3. Dem. că criptarea El Gamal e maleabilă

Având un criptotext $(\gamma, \delta) \xleftarrow{enc} x$

$\downarrow$? pot să modific ușor

$(\gamma', \delta') \xrightarrow{dec} \varepsilon x$ $\quad \varepsilon$ arbitrar ales

Rezolvare

1. $dec(enc(x)) = dec((\gamma, \delta))$, unde $\gamma = \alpha^k \bmod p$, $\delta = x \cdot \beta^k \bmod p$

$\Leftrightarrow dec(enc(x)) = dec((\gamma, \delta)) = \delta \cdot (\gamma^{-1})^a \bmod p =$

$= (x \cdot \underbrace{\beta^k}_{\bmod p}) \cdot [(\alpha^k \bmod p)^{-1}]^a \bmod p = x \cdot \beta^k \cdot [(\alpha^k \bmod p)^{-1}]^a \bmod p =$

$= x \cdot (\alpha^a \bmod p)^k \cdot [(\alpha^k \bmod p)^{-1}]^a \bmod p =$

$= x \cdot (\alpha^k \bmod p)^a \cdot [(\alpha^k \bmod p)^{-1}]^a \bmod p =$

$= x \cdot [\underbrace{(\alpha^k \bmod p)(\alpha^k \bmod p)^{-1}}_{1 \bmod p}]^a \bmod p =$

$= x \cdot 1^a \bmod p = x$ (deoarece $x \in \mathbb{Z}_p^*$)

2. $enc(x_1) = (\gamma_1, \delta_1)$ unde $\gamma_1 = \alpha^k \bmod p$, $\delta_1 = x_1 \cdot \beta^k \bmod p$

$enc(x_2) = (\gamma_2, \delta_2)$ unde $\gamma_2 = \alpha^k \bmod p = \gamma_1$, $\delta_2 = x_2 \cdot \beta^k \bmod p$

(γ_1, δ_1)
(γ_2, δ_2)
x_1

$x_2 = ?$

$x_1 = dec((\gamma_1, \delta_1)) = \delta_1 \cdot (\gamma_1^{-1})^a \bmod p \Leftrightarrow (x_1 \cdot \beta^k \bmod p) \cdot (\gamma_1^{-1})^a \bmod p = x_1$

$\Leftrightarrow x_1 \cdot \beta^k \cdot (\gamma_1^{-1})^a \bmod p = x_1 = x_1 \bmod p$

$\Rightarrow \beta^k \cdot (\gamma_1^{-1})^a \bmod p = 1$ $(*)$

$dec((\gamma_2, \delta_2)) = \delta_2 \cdot (\gamma_2^{-1})^a \bmod p \overset{\gamma_2 = \gamma_1}{=} \delta_2 \cdot (\gamma_1^{-1})^a \bmod p =$

$= (x_2 \cdot \beta^k \bmod p) \cdot (\gamma_1^{-1})^a \bmod p = x_2 \cdot \underbrace{\beta^k (\gamma_1^{-1})^a}_{1 \bmod p} \bmod p \overset{(*)}{=} x_2 \bmod p$

$= x_2$

2

$\delta_2 = x_2 \cdot \beta^k \bmod p$

$\delta_1 = x_1 \cdot \beta^k \bmod p \Leftrightarrow \beta^k \bmod p = \delta_1 \cdot x_1^{-1} \bmod p$

$\delta_2 = x_2 \cdot \beta^k \bmod p \Leftrightarrow \delta_2 = x_2 \cdot \delta_1 \cdot x_1^{-1} \bmod p$

$\Leftrightarrow \underline{x_2 = \delta_2 \cdot x_1 \cdot \delta_1^{-1} \bmod p}$

3. $\delta \cdot (\gamma^{-1})^a = x$

$\delta' = \delta \cdot \beta \bmod p$

$\gamma' = \gamma \cdot \alpha \bmod p$

$\delta' \cdot (\gamma'^{-1})^a \bmod p = \delta \cdot \beta \bmod p \cdot \left((\gamma \cdot \alpha \bmod p)^{-1}\right)^a \bmod p$

$= \delta \cdot \beta \cdot (\gamma^{-1} \bmod p \cdot \alpha^{-1} \bmod p)^a \bmod p =$

$= \delta \cdot \beta \cdot (\gamma^{-1})^a \cdot (\alpha^{-1})^a \bmod p =$

$= \delta \cdot (\gamma^{-1})^a \cdot \alpha^a \cdot \alpha^{-a} \bmod p = \delta \cdot (\gamma^{-1})^a \bmod p = x$

$\delta' = \varepsilon^{a+1} \delta \bmod p$

$\gamma' = \varepsilon \gamma \bmod p$

$\delta' \cdot (\gamma'^{-1})^a \bmod p = \varepsilon^{a+1} \delta \cdot \left((\varepsilon \gamma)^{-1}\right)^a \bmod p =$

$= \varepsilon^{a+1} \delta \cdot \varepsilon^{-a} \cdot (\gamma^{-1})^a \bmod p = \delta \cdot (\gamma^{-1})^a \cdot \varepsilon^a \cdot \varepsilon^{-a} \cdot \varepsilon \bmod p$

$= \varepsilon \cdot \delta \cdot (\gamma^{-1})^a \bmod p = \varepsilon x$

$\delta' = \varepsilon \delta \bmod p$ $\qquad \delta' (\gamma'^{-1})^a \bmod p = \varepsilon \delta (\gamma^{-1})^a \bmod p$

$\gamma' = \gamma$ $\qquad = \varepsilon x$