Esercizio (El Gamal firme incaute), per la lezione di martedì 21 maggio 2019

El Gamal firma in conta

Supponiamo che A. sia titolare di un critto-sistema di El Gamal con

$(p, g, \beta) \longrightarrow$ chiave pubblica

$a \longrightarrow$ chiave privata

(Come al solito p è primo, g è una radice primitiva mod p e $\beta \equiv g^a \pmod p$).

A. non deve firmare due messaggi in chiaro M_1 ed M_2 con lo stesso valore del parametro k (che è a scelta): infatti in questo caso il crittosistema può essere violato (cioè Oscar, che spia, può calcolare la chiave segreta a.

Vediamo come. Sappiamo che la firma di un messaggio in chiaro M è data dalla coppia $\Sigma = (\gamma, \delta)$ con

$$1) \begin{cases} \gamma \equiv g^k \pmod p \\ \delta \equiv (M - a\gamma)k^{-1} \pmod{p-1} \end{cases}$$

dove $k \cdot k^{-1} \equiv 1 \pmod{p-1}$).

Se A. firma due messaggi in chiaro M_1 ed M_2 con lo stesso k si hanno le due terne

$$2)\begin{cases}(M_1, \Sigma_1) = (M_1, (\gamma, \delta_1)) \\ (M_2, \Sigma_2) = (M_2, (\gamma, \delta_2))\end{cases}$$

dove $\gamma \equiv g^k \pmod p$ è lo stesso per tutte e due i messaggi, mentre

$$3)\begin{cases}\delta_1 \equiv (M_1 - a\gamma)k^{-1} \pmod{p-1} \\ \delta_2 \equiv (M_2 - a\gamma)k^{-1} \pmod{p-1}\end{cases}$$

Se Oscar intercetta le due terne in 2), da 3) ricava

$$4)\begin{cases}k\delta_1 + a\gamma \equiv M_1 \pmod{p-1} \\ k\delta_2 + a\gamma \equiv M_2 \pmod{p-1}\end{cases}$$

e, sottraendo membro a membro,

$$5)\quad k(\delta_1 - \delta_2) \equiv M_1 - M_2 \pmod{p-1}$$

La 5) è una congruenza di primo grado nell'incognita k (gli altri numeri sono noti ad Oscar), e quindi Oscar la risolve rapidamente (algoritmo euclideo ed identità di Bézout). La 5) può avere più soluzioni, infatti, come sappiamo, ne ha

$$6) \quad d = (\delta_1 - \delta_2, p-1)$$

(In questo caso è certo che $d \mid (M_1 - M_2)$, infatti la 5) ha soluzione).

Se ci sono effettivamente più soluzioni, Oscar può scegliere il valore corretto di k controllando la congruenza

$$7) \quad \gamma \equiv g^k \pmod{p}$$

(infatti g e p fanno parte della chiave pubblica di A.).

Una volta trovato k, dalla prima delle congruenze 4) (ad esempio), Oscar ricava

$$8) \quad a\gamma \equiv M_1 - k\delta_1 \pmod{p-1}$$

La 8) è una congruenza di primo grado nell'incognita γ: anche questa congruenza può avere più soluzioni, ma per trovare il valore corretto di a Oscar basta che controlli la congruenza

$$9) \quad \beta \equiv g^a \pmod{p}$$

infatti β, g e p sono pubblici.

Vediamo un esempio.

Osservazione

Ovviamente A. deve tenere segreto il valore del parametro k che sceglie per firmare un messaggio in chiaro, altrimenti dalle 8) Oscar calcola a.

Esempio di firme in conto.

A. è titolare di un crittosistema di El Gamal con

$$(p, g, \beta) = (53, 2, 45) \longrightarrow \text{chiave pubblica}$$

$$a = 29 \longrightarrow \text{chiave privata}$$

($p = 53$ è primo e $2^{29} \equiv 45 \pmod{53}$).

A. firma i due messaggi in chiaro

$$M_1 = 11$$
$$M_2 = 7$$

usando lo stesso $k = 9$ come parametro.

Come prima cosa A. calcola

$$10)\quad \gamma \equiv 2^9 \pmod{53}$$

Si ha $2 \equiv 2 (53)$, $2^2 \equiv 4$, $2^4 \equiv 16$, $2^8 \equiv (16)^2 = 256 \equiv 44 \equiv -9 (53)$

e infine $2^9 \equiv -18 \equiv 35 \pmod{53}$. Abbiamo quindi

11) $\gamma \equiv 2^9 \equiv 35 \pmod{53}$

Calcoliamo ora $k^{-1} \pmod{p-1}$, per noi

12) $9 \cdot k^{-1} \equiv 1 \pmod{52}$

Si ha

$$\begin{aligned} 52 &= 9 \cdot 5 + 7 \\ 9 &= 7 \cdot 1 + 2 \\ 7 &= 2 \cdot 3 + 1 \\ 2 &= 1 \cdot 2 + 0 \end{aligned} \quad \Longrightarrow \quad \begin{aligned} 1 &= 7 - 2 \cdot 3 = 7 - (9-7) \cdot 3 = \\ &= 4 \cdot 7 - 3 \cdot 9 = \\ &= 4(52 - 9 \cdot 5) - 3 \cdot 9 = \\ &= 4 \cdot 52 - 9 \cdot 23 \end{aligned}$$

e quindi $k^{-1} \equiv -23 \equiv 29 \pmod{52}$. Abbiamo quindi

13) $k^{-1} = 29$

Firmiamo ora $M_1 = 11$. Si ha

$$\delta_1 \equiv (M_1 - a\gamma)k^{-1} \pmod{p-1}$$

per noi (lavorando mod 52)

14) $\delta_1 \equiv (11 - 29 \cdot 35)29 \equiv (11 - 29(-17))29 \equiv$

$\equiv (11 + 493) \cdot 29 \equiv (11 + 25) \cdot 29 \equiv$

$\equiv (36)(29) \equiv (-16)(-23) \equiv 368 \equiv 4 \pmod{52}$

Abbiamo quindi

15) $(M_1, \Sigma_1) = (M_1, (\gamma, \delta_1)) = (11, (35, 4))$

Firmiamo ora M_2. Si ha

$$\delta_2 \equiv (M_2 - a\gamma)k^{-1} \pmod{p-1}$$

per noi (lavorando mod 52),

16) $\delta_2 \equiv (7 - 29 \cdot 35)29 \equiv (7-(29)(-17))\,29 \equiv$

$\equiv (7+493)\cdot 29 \equiv (7+25)(29) \equiv$

$\equiv (32)(29) \equiv (-20)(-23) \equiv 460 \equiv$

$\equiv 44 \pmod{52}$

Quindi abbiamo

17) $(M_2, \Sigma_2) = (M_2, (\gamma, \delta_2)) = (7, (35, 44))$

Per noi la firma in conto è quindi

18) $M_1 = 11 \longrightarrow (M_1, (\gamma, \delta_1)) = (11, (35, 4))$

$M_2 = 7 \longrightarrow (M_2, (\gamma, \delta_2)) = (7, (35, 44))$

(vedi le pagine successive per la soluzione)

Per noi la forma in conto è

$M_1 = 11 \qquad (M_1,(\gamma,\delta_1)) \equiv (11,(35,4))$
$M_2 = 7 \qquad (M_2,(\gamma,\delta_2)) \equiv (7,(35,44))$

Quindi

$$k(\delta_1-\delta_2) \equiv M_1 - M_2 \pmod{p-1}$$

per noi è

$$k(4-44) \equiv 11-7 \pmod{52}$$

cioè $(-40)k \equiv 4 \pmod{52}$ che equivale a

$$12 \cdot k \equiv 4 \pmod{52}$$

Siccome $(12,52) = 4$ si ha che

$$12k \equiv 4 \pmod{52} \iff 3k \equiv 1 \pmod{13}$$

$$13 = 3 \cdot 4 + 1 \Rightarrow k \equiv -4 \equiv -4+13 \equiv 9 \pmod{13}$$

Quindi $k_0 = 9 = x_0$

e $x_0, x_0+\frac{m}{d}, x_0+2\frac{m}{d}, \ldots x_0+(d-1)\frac{m}{d}$

(per noi $m=52$, $d=4$ $\quad \frac{m}{d} = \frac{52}{4} = 13$

e quindi si ha

$9, \ 9+13, \ 9+2\cdot 13, \ 9+3\cdot 13$

$9, \ 22, \ 35, \ 48$ sono le sol. di (*)

Quale sia il valore buono di k si capisce che

$g^k \equiv r \pmod{p}$, per noi

$2^k \equiv 35 \pmod{53}$

cioè $k = 9$, come deve essere

Dunque $k = 9$. Dobbiamo poi risolvere la

$a\, r \equiv (\Pi_2 - k\, \sigma_2) \pmod{(p-1)}$, per noi

$a \cdot 35 \equiv (7 - 9 \cdot 44) \pmod{52}$
$\equiv (7 - 9(-8)) \pmod{52}$
$\equiv (7 + 72) \pmod{52}$
$\equiv (7 + 20) \pmod{52}$
$\equiv 27 \pmod{52}$

Risolviamo la

$35\, a_1 \equiv 1 \ (52)$

Si ha $52 = 35 \cdot 1 + 17$
$35 = 17 \cdot 2 + 1 \Rightarrow 1 = 35 - 17 \cdot 2$
$= 35 - (52 - 35) \cdot 2$
$= 3 \cdot 35 - 2 \cdot 52$

$\boxed{a_1 \equiv 3 \ (52)}$

Quindi $(a_1 \cdot 27) = 3 \cdot 27 \equiv 81 \equiv 29 \pmod{52}$
è il valore cercato

Infatti $\boxed{a = 29}$
come è giusto!