# Lezione di Crittografia di martedì 2 aprile 2019

(Scaricatela e portatela in aula F8)

# Crittosistema di El Gamal (1985)

A. si vuol dotare di un crittosistema di El Gamal. Procede nel modo seguente.

- Sceglie un primo grande $p$, una radice primitiva $g \bmod p$ ed una chiave segreta $a$, con $1 < a < p-1$ e calcola $g^a \equiv \beta \pmod p$.

A questo punto il crittosistema di A. è così stabilito:

i) la terna $(p, g, \beta)$ è la chiave pubblica

ii) l'esponente $a$ è la chiave privata.

## Procedimento di cifratura

B. vuol cifrare il messaggio $M$ per A. (il messaggio $M$ è un numero, $1 < M < p$).

- B. sceglie un numero $k$ con $1 < k < p-1$ e calcola

$$1) \quad \gamma \equiv g^k \pmod p$$

Calcola poi

$$2) \quad \delta \equiv M \beta^k \pmod p$$

Invia il cifrato, costituito dalla coppia

$(\gamma, \delta) = C$ ad A.

## Decifrazione

A. riceve il cifrato $C = (\gamma, \delta)$ e, disponendo della sua chiave privata a, calcola

$$3) \quad \gamma^a \equiv (g^k)^a \equiv g^{ak} \pmod{p}$$

e ne calcola poi l'inverso moltiplicativo mod $p$, indichiamolo con $(g^{ak})^{-1}$, cioè

$$4) \quad (g^{ak})(g^{ak})^{-1} \equiv 1 \pmod{p}$$

(algoritmo euclideo ed identità di Bézout).
Moltiplica poi $\delta$ per $(g^{ak})^{-1}$, ritrovando il messaggio M, infatti

$$5) \quad \delta (g^{ak})^{-1} \equiv (M \cdot \beta^k)(g^{ak})^{-1} \equiv$$
$$\equiv M (g^{ak})(g^{ak})^{-1} \equiv M \cdot 1 \equiv$$
$$\equiv M \pmod{p}$$

Alternativamente A. può calcolare semplicemente

6) $\gamma \cdot \gamma^{p-1-a} \cdot \delta \equiv (g^k)^{(p-1-a)} \cdot M \cdot \beta^k \equiv$

$\equiv (g^k)^{(p-1-a)} \cdot M \cdot g^{ak} \equiv$

$\equiv g^{k(p-1)-ka+ka} \cdot M \equiv$

$\equiv (g^{p-1})^k \cdot M \equiv 1^k \cdot M \equiv$

$\equiv M \pmod p$.

poiché $g^{p-1} \equiv 1 \pmod p$, per il piccolo teorema di Fermat.

Osservazione 1

Nel crittosistema di El Gamal, il messaggio M porta una "maschera" (cioè viene moltiplicato per $\beta^k$). A., titolare del crittosistema, riesce a togliere la maschera ad M, utilizzando la sua chiave privata a e l'informazione $\gamma \equiv g^k \pmod p$, che viene inviata da B.

Osservazione 2

La sicurezza del crittosistema di El Gamal si basa sul problema del logaritmo discreto, o meglio, sul problema di Diffie-Hellman. Supponiamo infatti che Oscar (O.) stia

spiando la comunicazione tra B. ed A.
Il nostro O. conosce $\beta \equiv g^a \pmod p$, poiché fa parte della chiave pubblica, e anche $\gamma \equiv g^k \pmod p$. Per decifrare il messaggio deve però calcolare $g^{ak} \pmod p$, cioè deve risolvere il problema di Diffie-Hellman.

Esempio 1

L'esempio che segue ha un valore didattico, illustrativo del crittosistema di El Gamal. Tutti i calcoli si possono eseguire facilmente a mano, anche senza calcolatrice.

- Scegliamo il primo $p = 23$ e cerchiamo una radice primitiva $g \bmod 23$. Dato che $\varphi(p) = \varphi(23) = 22$, $g$ deve avere ordine 22. Gli ordini possibili degli elementi del sistema ridotto di resti mod 23 sono quindi i divisori di 22, cioè $\delta = 1, 2, 11, 22$. Proviamo con 2, 3, 4, ma queste elementi hanno ordine 11. Invece $g = 5$ è quello che cerchiamo, infatti $5^{11} \equiv 160 \equiv -1 \pmod{23}$, perciò $g = 5$ è radice primitiva mod 23 (verificate, con facili calcoli, queste affermazioni!). Dobbiamo poi scegliere la chiave privata $a$, con $1 < a < p-1$, per noi $1 < a < 22$. Scegliamo

$a = 7$ e calcoliamo $\beta = g^a \equiv 5^7 \equiv 17 \pmod{23}$.
A questo punto il crittosistema di ElGamal è costruito, con

$(p, g, \beta) = (23, 5, 17)$, come chiave pubblica

$a = 7$, come chiave privata.

Supponiamo che B. ci voglia cifrare il messaggio $M = 10$. B. procede nel modo seguente:

i) sceglie un numero $k$ con $1 < k < p-1$, per noi $1 < k < 22$ e calcola $\gamma \equiv g^k \bmod p$. Supponiamo che B scelga $k = 4$, ottenendo $\gamma \equiv 5^4 \equiv 4 \pmod{23}$.

Perciò

$$\boxed{\gamma = 4}$$

ii) Poi B. calcola $\delta \equiv M \cdot \beta^k \pmod p$, per noi $\delta \equiv (10)(17^4) \pmod{23}$. Dato che $17^4 \equiv 8 \pmod{23}$ si ha $\delta \equiv (10)(8) \equiv 80 \equiv 11 \pmod{23}$.

Perciò

$$\boxed{\delta = 11}$$

A questo punto B. ci manda il cifrato

$$C = (\gamma, \delta) = (4, 11)$$

Noi lo decifriamo con la nostra chiave segreta $a = 7$, calcolando $M \equiv (\gamma^{p-1-a} \cdot \delta) \pmod p$, perciò

$\left(\left(4^{23-1-7}\right).(11)\right) \bmod 23$, Dato che

$4^{23-1-7} = 4^{15} \equiv 3 \pmod{23}$, ne segue che

$$M \equiv (3.11) \equiv 33 \equiv 10 \pmod{23}$$

ed abbiamo decifrato C.

Alternativamente avremo potuto calcolare prima

$$r^a \equiv 4^7 \equiv 8 \pmod{23}$$

per poi trovarne l'inverso mod 23, cioè risolvere la congruenza $8x \equiv 1 \pmod{23}$, che fornisce $x \equiv 3 \pmod{23}$. Quindi, come prima,

$$M \equiv 3.11 \equiv 33 \equiv 10 \pmod{23}.$$

---

## Firma di El Gamal

Nel 1985 El Gamal presentò anche una firma digitale molto interessante, di cui ora parliamo.

Supponiamo che A. sia titolare di un crittosistema di El Gamal con

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

$a$, come chiave privata

Se A. vuole inviare un messaggio in chiaro (7)
M a B., firmandolo, procede nel modo se
guente.

- sceglie un numero $k$ con $1 < k < p-1$, tale che $(k, p-1) = 1$.
- calcola poi $k^{-1} \bmod p$, cioè $k \cdot k^{-1} \equiv 1 \pmod{(p-1)}$ ($k^{-1}$ è l'inverso moltiplicativo di $k$ mod $(p-1)$)

e

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

$$8) \quad \delta \equiv (M - a\gamma) k^{-1} \pmod{(p-1)}$$

La coppia $\Sigma = (\gamma, \delta)$ costituisce la firma del messaggio M. A. quindi invia a B. la terna $(M, (\gamma, \delta)) = (M, \Sigma)$.

B. riceve il messaggio firmato e verifica l'autenticità della firma, controllando che valga la congruenza

$$9) \quad \beta^\gamma \gamma^\delta \equiv g^M \pmod p$$

Se la 9) vale la firma è accettata come autentica, altrimenti è rifiutata.

Dimostriamo che, se la firma è autentica, la congruenza 9) deve valere.

Infatti, ricordando che $\beta \equiv g^a \pmod p$ e $\gamma \equiv g^k \pmod p$, a sinistra di 9) troviamo

10) $\beta^\gamma \gamma^\delta \equiv (g^a)^\gamma (g^k)^\delta = g^{a\gamma + k\delta} \pmod p$

e dalla 8) segue

11) $k\delta + a\gamma \equiv M \pmod{(p-1)}$

Quindi la congruenza 9) è in questo caso verificata, infatti la 11) equivale a

12) $k\delta + a\gamma = M + h(p-1)$, $h \geq 1$

e quindi, da 10) e 12) segue

13) $\beta^\gamma \gamma^\delta \equiv g^{M+h(p-1)} \equiv g^M \cdot (g^{p-1})^h \equiv$

$\equiv g^M \cdot 1 \equiv g^M \pmod p$

dato che, per il piccolo teorema di Fermat, si ha $g^{p-1} \equiv 1 \pmod p$.

- Osserviamo che la firma $\Sigma = (\gamma, \delta)$ dipende sia dal messaggio $M$ che dalla chiave privata $a$ (vedi la 8), definizione di $\delta$), oltre che dal parametro casuale $k$. Chi la riceve con il messaggio $M$, la può facilmente verificare, poiché $(p, g, \beta)$ è la chiave pubblica

di A., $r$, $s$ ed M sono inviati direttamente. Inoltre B. (il destinatario) non può modificare il messaggio M: infatti, non conoscendo né a (chiave privata di A.) né k, non sarebbe poi in grado di firmarlo.

---

Esempio 2 (didattico, illustrativo di firma di El Gamal)

Supponiamo che A. sia titolare del cripto-sistema di El Gamal precedentemente illustrato nell'esempio 1, cioè con

$(p, g, \beta) = (23, 5, 17)$, come chiave pubblica

$a = 7$, come chiave privata

Supponiamo che A. voglia firmare il messaggio $M = 11$. A. deve scegliere un parametro k, con $1 < k < p-1$, tale che $(k, p-1) = 1$, per poi calcolare $k^{-1} \pmod{(p-1)}$. Supponiamo che scelga $k = 3$ (scelta ammessa, poiché $(3, 22) = 1$) e poi risolva la congruenza $k \cdot k^{-1} \equiv 1 \pmod{p-1}$ per noi

$$14) \quad 3 \cdot k^{-1} \equiv 1 \pmod{22}$$

Dato che $22 = 3 \cdot 7 + 1$ si ha $3(-7) \equiv 1 \pmod{22}$, quindi $k^{-1} \equiv -7 \equiv -7 + 22 \equiv 15 \pmod{22}$

Calcola poi $\gamma \equiv g^k \pmod p$, per noi

15) $\gamma \equiv 5^3 \equiv 10 \pmod{23}$

e infine $\delta \equiv (M - a\gamma)k^{-1} \pmod{(p-1)}$, per noi

16) $\delta \equiv (11 - 7.10)(15) \pmod{22}$

$\equiv (-59)(-7) \pmod{22}$

$\equiv (7)(-7) \pmod{22}$

$\equiv (-49) \equiv 17 \pmod{22}$

A questo punto A. invia a B. la terna $(M, (\gamma, \delta)) = (M, \Sigma)$, dove M è il messaggio in chiaro, e $\Sigma = (\gamma, \delta)$ è la firma del messaggio, dicendo sono A., messaggio firmato.

B. verifica la firma controllando la validità della congruenza

$$\beta^\gamma \cdot \gamma^\delta \equiv g^M \pmod p$$

per noi

17) $17^{10} \cdot 10^{17} \equiv 5^{11} \pmod{23}$

Verifichiamo la 17).

Poiché $(10)_2 = 1010$ calcoliamo

$17 \equiv 17 \pmod{23}$

$\rightarrow 17^2 \equiv 289 \equiv -10 \ (23)$

$17^4 \equiv 100 \equiv 8 \ (23)$

$\rightarrow 17^8 \equiv 64 \equiv -5 \ (23)$

e quindi

$(17)^{10} \equiv (-10)(-5) = 50 \equiv 4 \pmod{23}$

Inoltre $(17)_2 = (10001)$ e quindi

$\rightarrow 10^1 \equiv 1 \ (23)$

$10^2 \equiv 100 \equiv 8 \ (23)$

$10^4 \equiv 64 \equiv -5 \ (23)$

$10^8 \equiv 25 \equiv 2 \ (23)$

$\rightarrow 10^{16} \equiv 4 \ (23)$

da cui $(10)^{17} \equiv 10 \cdot 4 \equiv 40 \equiv$
$\equiv 17 \equiv -6 \ (\text{mod } 23)$

Perciò a sinistra di 17) abbiamo

18) $17^{10} \cdot 10^{17} \equiv (4)(-6) \equiv -24 \equiv -1 \ (\text{mod } 23)$

A destra di 17) abbiamo lo stesso risultato, essendo 5 radice primitiva mod 23 (infatti $11 = 2 \cdot (22)$). Comunque verifichiamolo:

si ha $(11)_2 = (1011)$ e quindi

$\rightarrow 5^1 \equiv 5 \ (23)$

$\rightarrow 5^2 \equiv 25 \equiv 2 \ (23)$

$5^4 \equiv 4 \ (23)$

$\rightarrow 5^8 \equiv 16 \equiv -7 \ (23)$

da cui $5^{11} \equiv (5 \cdot 2)(-7) \equiv -70 \equiv -1 \ (\text{mod } 23)$

Dunque la congruenza 17) è vera e B. accetta la firma di A. come firma autentica.