Questo fascicolo contiene un esempio di compito di Crittografia (Cristosistemi di Rabin e di Blum-Goldwasser). Scaricatelo, costituirà parte della lezione di domani, martedì 27 maggio 2019.

Il compito è un pò troppo lungo (ho voluto esemplificare tutto). Aspettatevi compiti un pò più brevi.

Esempio di compito di Crittografia (2018-2019)

Esercizio 1 (Rabin)

A. è titolare di un cryptosistema di Rabin con $p=23$, $q=31$. Dato che $n=p\cdot q=(23)(31)=713$ si ha

$n=713 \longrightarrow$ chiave pubblica

$p=23$, $q=31 \longrightarrow$ chiave privata

B. cifra per A. il messaggio $M=313$.

Si domanda

i) qual'è il cifrato C che A. riceve?

ii) mettetevi nei panni di A. e decifrate C. Fattorizzate $n=713$ in base ai possibili messaggi M che avete ottenuto.

Esercizio 2

A. è titolare di un cryptosistema di Blum-Goldwasser con $p=23$, $q=31$ e quindi $n=713$ è la chiave pubblica di A

B. cifra per A il messaggio $M=(1,1,0,1,0)$ scegliendo come seme $s_0=49$. Si domanda

i) qual'è il cifrato C che A. riceve?

ii) mettetevi nei panni di A. e decifrate C.

Facoltativo: dimostrate che $P(n)=n^5-n\equiv 0 \pmod{30}$ $\forall n$.

Svolgimento esercizio 1

- Rispondiamo ad i).
La risposta è ovvia, in quanto $C \equiv M^2 \pmod{n}$, per noi

$C \equiv (313)^2 \equiv 97969 \equiv 288 \pmod{713}$, e quindi

1) $\boxed{C = 288}$

- Rispondiamo ad ii)
Per decifrare C la titolare A. del crittosistema segue lo schema seguente:

- Calcola $ap + bq = 1$, per noi $a \cdot 23 + b \cdot 31 = 1$
Basta applicare l'algoritmo euclideo e poi leggerlo all'indietro:

$31 = 23 \cdot 1 + (8)$
$23 = 8 \cdot 2 + (7)$
$8 = 7 \cdot 1 + (1) \Longrightarrow 1 = 8 - 7 = 8 - (23 - 8 \cdot 2) =$
$7 = 1 \cdot 7 + 0$
$= 3 \cdot 8 - 23 =$
$= 3(31 - 23) - 23 =$
$= 3 \cdot 31 - 4 \cdot 23$

Per noi $\boxed{a = -4}$, $\boxed{b = 3}$.

(Notate che l'identità di Bézout $ap + bq = 1$ può essere precalcolata da A., infatti è la stessa per tutti i cifrati e dipende solo da p e q)

- Calcola $r \equiv C^{(p+1)/4} \pmod p$ e $s \equiv C^{(q+1)/4} \pmod q$,

per noi $r \equiv (288)^{(23+1)/4} \equiv (288)^6 \pmod{23}$ e

$s \equiv (288)^{(31+1)/4} \equiv (288)^8 \pmod{31}$.

Calcoliamo r: si ha

$$288 \equiv 12 \pmod{23}$$
$$288^2 \equiv (12)^2 \equiv 144 \equiv 6 \pmod{23}$$
$$288^4 \equiv 36 \equiv 13 \pmod{23}$$
$$288^6 \equiv (13).(6) \equiv 78 \equiv 9 \pmod{23}$$

Calcoliamo ora s: si ha

$$288 \equiv 9 \pmod{31}$$
$$288^2 \equiv 81 \equiv -12 \pmod{31}$$
$$288^4 \equiv 144 \equiv -11 \pmod{31}$$
$$288^8 \equiv (-11)^2 \equiv 121 \equiv 28 \pmod{31}$$

A. ha quindi ottenuto

$$\boxed{r = 9}, \quad \boxed{s = 28}$$

- A questo punto A. decifra C calcolando

$x \equiv aps + bqr \pmod n$ e $y = aps - bqr \pmod n$

Per noi $x \equiv -4.23.28 + 3.31.9 \pmod{713}$, cioè

$$x \equiv -4.644 + 93.9 \pmod{713}$$
$$\equiv (-4)(-69) + 93.9 \pmod{713}$$
$$\equiv 276 + 837 \equiv 1113 \equiv 400 \pmod{713}$$

Vediamo ora y: si ha

$$y = aps - bqr = -4.23.28 - 3.31.9 \pmod{713}$$
$$\equiv 276 - 837 \equiv -561 \pmod{713}$$
$$\equiv -561 + 713 \equiv 152 \pmod{713}$$

Le quattro radici quadrate di C sono, come sappiamo, $\pm x$ e $\pm y$, per noi $\pm 400 \pmod{713}$ e $\pm 152 \pmod{713}$, cioè

$$400, 313, 152, 561$$

Una di queste è proprio $M = 313$, il messaggio inviato.

Rispondiamo ora alla domanda sulla fattorizzazione di n.

Prendendo, ad esempio, $x = 400$ e $y = 152$, si ha

$$400^2 \equiv 152^2 \pmod{713}$$

da cui segue $(400 - 152)(400 + 152) \equiv 0 \pmod{713}$, cioè $(248)(552) \equiv 0 \pmod{713}$. Calcoliamo ora $(248, 713) = d_1$: si ha

$$713 = 248.2 + 217$$
$$248 = 217.1 + 31$$
$$217 = 31.7 + 0$$

e quindi $(248, 713) = d_1 = 31 = 9$

mentre per $d_2 = (552, 713)$ si ha

$$713 = 552.1 + 161$$
$$552 = 161.3 + 69$$
$$161 = 69.2 + 23$$
$$69 = 23.3 + 0$$

e quindi $d_2 = (552, 713) = 23 = p$.

Esercizio 2 (Blum – Goldwasser)

Dato che $p = 23$, $q = 31$, si $n = p \cdot q = (23)(31) = 713$ e primoli

$n = 713 \longrightarrow$ chiave pubblica di A.

$p = 23, q = 31 \longrightarrow$ chiave privata di A.

Rispondiamo ad i).

Dato che $s_0 = 49$, calcoliamo successivamente

$$s_1 \equiv s_0^2 \equiv (49)^2 \equiv 2401 \equiv 262 \pmod{713}$$

$$s_2 \equiv s_1^2 \equiv (262)^2 \equiv 68644 \equiv 196 \pmod{713}$$

(*) $$s_3 \equiv s_2^2 \equiv (196)^2 \equiv 38416 \equiv 627 \equiv -86 \pmod{713}$$

$$s_4 \equiv s_3^2 \equiv (-86)^2 \equiv 7396 \equiv 266 \pmod{713}$$

$$s_5 \equiv (266)^2 \equiv 70756 \equiv 169 \pmod{713}$$

Questa sequenza produce l'output

1) $z = (z_1, z_2, z_3, z_4, z_5) = (0, 0, 1, 0, 1)$

dato che

$$z_i \equiv s_i \pmod 2, \text{ per } 1 \leq i \leq 5$$

Siccome il messaggio M che B. vuole inviare ad A. è

2) $x = (1, 1, 0, 1, 0) = M$

dobbiamo calcolare $x_i + z_i \equiv y_i \pmod 2$.

Da 1) e 2) segue

3) $y = (y_1, y_2, y_3, y_4, y_5) = (1, 1, 1, 1, 1)$

Per calcolare il cifrato C dobbiamo aggiungere ad y l'informazione $S_6 \equiv S_5^2 \pmod{713}$. Siccome

4) $S_6 \equiv S_5^2 \equiv (169)^2 \equiv 28561 \equiv 41 \pmod{713}$

il cifrato C sarà la stringa

5) $\boxed{C = (1,1,1,1,1,41)}$

Questo risponde alla domanda i').

Rispondiamo ora alla domanda ii).

Per decifrare C la titolare A. segue lo schema seguente:

- Calcola $a_1 \equiv \left(\frac{p+1}{4}\right)^{e+1} \pmod{(p-1)}$ e $a_2 \equiv \left(\frac{q+1}{4}\right)^{e+1} \pmod{(q-1)}$

per noi $a_1 \equiv \left(\frac{23+1}{4}\right)^{5+1} \equiv 6^6 \pmod{22}$ e

$a_2 \equiv \left(\frac{31+1}{4}\right)^{5+1} \equiv 8^6 \pmod{30}$.

Si ha quindi

$6^1 \equiv 6 \pmod{22}$

$6^2 \equiv 36 \equiv 14 \pmod{22}$

$6^4 \equiv (14)^2 \equiv 196 \equiv -2 \pmod{22}$

$6^6 \equiv (14)(-2) \equiv -28 \equiv 16 \pmod{22}$

e

$8^1 \equiv 8 \pmod{30}$

$8^2 \equiv 64 \equiv 4 \pmod{30}$

$8^4 \equiv 16 \pmod{30}$

$8^6 \equiv 16 \cdot 4 = 64 \equiv 4 \pmod{30}$

A. ha quindi ottenuto

6) $\boxed{a_1 = 16}$, $\boxed{a_2 = 4}$

- Calcola poi $b_1 \equiv s_{e+1}^{a_1} \pmod p$ e $b_2 \equiv s_{e+1}^{a_2} \pmod q$, per noi, ricordando 4) e 6),

7) $$b_1 \equiv s_6^{a_1} \equiv (41)^{16} \pmod{23}$$
$$b_2 \equiv s_6^4 \equiv (41)^4 \pmod{31}$$

Si ha

$$41 \equiv -5 \pmod{23}$$
$$41^2 \equiv 25 \equiv 2 \pmod{23}$$
$$41^4 \equiv 4 \pmod{23}$$
$$41^8 \equiv 16 \equiv -7 \pmod{23}$$
$$41^{16} \equiv 49 \equiv 3 \pmod{23}$$

e

$$41 \equiv 10 \pmod{31}$$
$$41^2 \equiv 100 \equiv 7 \pmod{31}$$
$$41^4 \equiv 49 \equiv 18 \pmod{31}$$

Perciò A. ottiene

8) $\boxed{b_1 = 3}$, $\boxed{b_2 = 18}$

- A questo punto, la titolare A. deve utilizzare il teorema cinese del resto per calcolare s_0, poiché $s_0 \equiv b_1 \pmod p$, $s_0 \equiv b_2 \pmod q$: per noi

9) $$\begin{cases} s_0 \equiv 3 \pmod{23} \\ s_0 \equiv 18 \pmod{31} \end{cases}$$

La soluzione di 9) è $s_0 = 49$ e quindi A. ha trovato il seme s_0: deve perciò calcolare successivamente s_1, s_2, s_3, s_4, s_5 (vedi formula (*) a pag. 4) da cui ottiene l'output $z = (0, 0, 1, 0, 1)$.
Se chiamiamo C^* il cifrato C escluso $s_6 = 41$, si ha $C^* = (1, 1, 1, 1, 1)$: il messaggio M si ottiene calcolando

$$(z + C^*) \pmod 2$$

cioè

$$z = (0, 0, 1, 0, 1)$$
$$C^* = (1, 1, 1, 1, 1)$$
$$M = (0+1, 0+1, 1+1, 0+1, 1+1)$$
$$= (1, 1, 0, 1, 0).$$

che è il messaggio effettivamente inviato da Bob.