

Lezione di CRITOGRAFIA

lunedì 9 novembre, 11:15

RSA



RSA

- CREAZIONE della chiave

DEST

- sceglie p e q , primi, molto grandi

$$n = p \times q \quad \text{dove avere almeno 2048 cifre binarie}$$

$$3072 \quad " \quad "$$

temp
polinomiale via Miller-Rabin

- calcola

$$n = p \times q$$

$$\phi(n) = (p-1) \times (q-1)$$

tempo polinomiale

- sceglie $e < \phi(n)$: $\text{MCD}(e, \phi(n)) = 1$

tempo
polin.

- calcola $d = e^{-1} \bmod \phi(n)$ $(\exists !)$ \uparrow

tempo polin.
via Ext. Eud.

- Rende pubblico

$$k[\text{pub}] = \langle e, n \rangle$$

- mantiene private

$$k[\text{priv}] = \langle d \rangle$$

MESSAGGIO

sequenza binaria, trattata come un intero



$$m < n$$

Se $m \geq n$, m si divide in blocchi di $b = \lceil \log_2 n \rceil$ bit, a testi indipendentemente.

PRATICA : si fissa un limite concreto per le dimensioni dei blocchi

$$m + 2^b < n$$

CIFRATURA

$$c = G(m, k(\text{pub})) = m^e \mod n$$

$m < n$

$c < n$

tempo
polinomiale

(quadrature
successive)

DECIFRAZIONE

$$m = D(c, k(\text{priv})) = c^d \mod n$$

ESEMPIO

$$p=5 \quad q=11$$

$$n=55$$

$$\phi(n) = (p-1)(q-1) = 40$$

$$e=7 \quad \text{e} \odot (7, 40) = 1 \quad \checkmark$$

$$d = 7^{-1} \mod 40$$

$$EE(7, 40) \rightarrow \langle 1, -17 \rangle$$

$$EE(40, 7) \rightarrow \langle 1, 3, -2 - 3 \cdot \lfloor 40/7 \rfloor \rangle = \langle 1, 3, -17 \rangle$$

$$EE(7, 5) \rightarrow \langle 1, -2, 1 - (-2) \cdot \lfloor 7/5 \rfloor \rangle = \langle 1, -2, +3 \rangle$$

$$EE(5, 2) \rightarrow \langle 1, 1, 0 - \lfloor 5/2 \rfloor \cdot 1 \rangle = \langle 1, 1, -2 \rangle$$

$$EE(2, 1) \rightarrow \langle 1, 0, 1 - \lfloor 2/1 \rfloor \cdot 0 \rangle = \langle 1, 0, 1 \rangle$$

$$EE(1, 0) \rightarrow \langle 1, 1, 0 \rangle$$

$$d = -17 \bmod 40 = 23 \bmod 40 = 23$$

$$k(\text{pub}) = \langle 7, 55 \rangle$$

$$k(\text{priv}) = \langle 23 \rangle$$

$$m < 55$$

$$c = m^7 \bmod 55$$

~~$$m = c^{23} \bmod 55$$~~

CORRETTEZZA

$$\mathbb{D}(G(m, k[\text{pub}]), k[\text{priv}]) = m$$

$$c^d \bmod n = (m^e \bmod n)^d \bmod n = m^{ed} \bmod n = m$$

TEOREMA

$$\forall m < n \quad m^{ed} \bmod n = m$$

DIM

→ (1) $p < q$ non dividono m

$\Rightarrow m \text{ e } n \text{ sono CO-PRIMI} \quad \text{MCD}(m, n) = 1$

(1) • $m^{\phi(n)} \equiv 1 \pmod{n}$ (Th. Eulero)

(2) • $e \cdot d \equiv 1 \pmod{\phi(n)}$
 $e \cdot d = 1 + r \phi(n) \quad r \in \mathbb{N}$ (def di Inverso)

$$m^{\text{col}} \bmod n = m^{1+r\phi(n)} \bmod n = m \underbrace{(m^{\phi(n)})^r}_{1} \bmod n$$

(2)

$$\stackrel{(1)}{=} m \cdot 1^r \bmod n = m \bmod n = \begin{matrix} m \\ \downarrow \\ m < n \end{matrix}$$

→ (2) $m \in n$ non sono coprimi

$$p \mid m \in q \nmid m$$

$$p \mid m \quad m \equiv 0 \pmod p$$

$$\forall r \in \mathbb{N} \quad m^r \equiv 0 \pmod p$$

$$\Rightarrow \forall r \in \mathbb{N} \quad m^r - m \equiv 0 \pmod p$$

$r = \text{e.d}$

$$m^{\text{ed}} - m \equiv 0 \pmod p$$

$$q \nmid m \Rightarrow \text{gcd}(q, m) = 1 \quad \text{sono coprimi} \quad \Rightarrow$$

$$m^{\phi(q)} \equiv 1 \pmod{q}$$

$$\begin{aligned} m^{ed} \pmod{q} &= m^{1 + r\phi(n)} \pmod{q} = m \cdot m^{r(p-1)(q-1)} \pmod{q} = \\ &= m \left(m^{(q-1)} \right)^{r(p-1)} \pmod{q} = m \left(m^{\phi(q)} \right)^{r(p-1)} \pmod{q} \\ &= m (1)^{r(p-1)} \pmod{q} = m \pmod{q} \end{aligned}$$

$$m^{ed} \equiv m \pmod{q}$$

$$m^{ed} - m \equiv 0 \pmod{q}$$

$m^{cd} - m$ è divisibile per $p \in \{p \mid q\}$ \Rightarrow è divisibile
anche per $n = p \cdot q$

$$m^{cd} - m \equiv 0 \pmod{n}$$

$$m^{cd} \equiv m \pmod{n}$$

$$m^{cd} \pmod{n} = m \pmod{n} = m$$

\downarrow

$m < n$



(3) $p \in \{p \mid q\}$ ~~dividono m~~ NON SI VERIFICA
perché $m < n$



CALCOLO di $\phi(n)$ da n e fattorizzazione di n
sono problemi computazionalmente equivalenti

(caso si trasforma nell'altro in tempo polinomiale)

tutti - $n \Rightarrow$ calcolo di $\phi(n)$

$$n = p \cdot q \quad \longrightarrow \quad \phi(n) = (p-1) \cdot (q-1) \quad \checkmark$$

$n \in \phi(n) \Rightarrow$ trov $p \in q$ in tempo polinomiale

$$\phi(n) = (p-1)(q-1) = pq - (p+q) + 1 = n - (p+q) + 1$$

$$\Rightarrow x_1 = p+q = n - \phi(n) + 1 \quad \left. \begin{array}{l} p = \frac{x_1+x_2}{2} \\ q = \frac{x_1-x_2}{2} \end{array} \right\}$$

$$(p-q)^2 = (p+q)^2 - 4n = x_1^2 - 4n$$

$$x_2 = p-q = \sqrt{x_1^2 - 4n}$$

ATTACCHI (scelta di e)

$$e \neq \frac{\phi(n) + 2}{2}$$

$$2 \mid (p-1) \quad 2 \mid (q-1)$$

$$\Rightarrow m^e \bmod n = m \quad (\text{Now VA BENE})$$

$m \in \mathbb{Z}_{\text{co-primi}}$

$$e \neq \frac{\phi(n) + k}{k}$$

$$\forall k \in \mathbb{Z} \quad k \mid (p-1) \quad \text{e} \quad k \mid (q-1)$$

~~sk~~

Attacco con c troppo piccolo

- supponiamo che ci siano e utenti, che hanno scelto lo stesso valore (piccolo) di c .
- gli e utenti riceveranno lo stesso messaggio m

$$\left. \begin{array}{l} C_1 = m^e \pmod{n_1} \\ C_2 = m^e \pmod{n_2} \\ \vdots \\ C_e = m^e \pmod{n_e} \end{array} \right\} \quad \forall i \quad 1 \leq i \leq e$$

$m < n_i$

$$\underbrace{m \cdot m \cdots m}_{c \text{ volte}} < n_1 n_2 \cdots n_e = n$$

IPOTESI: n_1, n_2, \dots, n_e coprimi fra loro

$$\downarrow \\ m^e < n$$

per il teorema cinese del resto:

\exists e si può facilmente calcolare un unico m' t.c.

$$m' < n = n_1 * n_2 * \cdots * n_e$$

$$m' \equiv m^e \pmod{n}$$

$$m' \pmod{n} = m^e \pmod{n}$$

$$m' = m^e \Rightarrow m = \sqrt[e]{m'}$$

$$m' < n$$

$$m^e < n$$

ATTACCO con lo stesso valore di n

$$\langle e_1, n \rangle$$

$$\langle e_3, n \rangle$$

$$\text{mcd}(e_1, e_2) = 1$$

$$\exists r, s \in \mathbb{Z} \text{ t.c.}$$

$$e_1 r + e_2 s = 1 \Rightarrow \text{mcd}(e_1, e_2)$$

(si trova con l'algoritmo di Euclide Esteso)

$$ax + by = \text{mcd}(a, b)$$

$$r < 0, \quad s > 0$$

Eve intercetta

$$C_1 = m^{e_1} \bmod n$$

$$C_2 = m^{e_2} \bmod n$$

$$m = m^1 = m^{re_1 + se_2} = \underbrace{(m^{e_1 \bmod n})^r}_{c_1} \cdot \underbrace{(m^{e_2 \bmod n})^s}_{c_2} \bmod n$$

$$= (c_1^r \cdot c_2^s) \bmod n = ((c_1^{-1})^{-r} \cdot c_2^s) \bmod n$$

c_1 : calcolo inverso di $c_1 \bmod n$

ipotesi

$$c_1^{-1} \bmod n$$

$$\text{HCD}(c_1, n) = 1$$

$$(c_1^{-1})^{-r} \in c_2^s \text{ con } \text{alg. quadr. successiva}$$

$$\Rightarrow m = (c_1^{-1})^{-r} \cdot (c_2)^s \bmod n$$