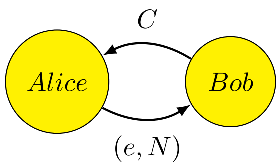
Crittografia asimmetrica: RSA

Prof. Salvatore D'Asta

20 febbraio 2021

Indice

1 Algoritmo RSA



Alice vuole consentire a Bob di inviarle un messaggio m segreto.

1. - Sceglie due numeri primi p e q e calcola $N = p \times q$.
   - Calcola $\varphi(N) = (p-1) \times (q-1)$.
   - Trova $0 < e < N$ in modo che $MCD(e, \varphi(N)) = 1$ (cioè siano coprimi). La coppia (e, N) costituisce la chiave pubblica e viene inviata a Bob.
   - Alice poi crea la sua chiave privata $(\mathbf{d}, \mathbf{N})$ trovando d tale che $\boxed{e \times d \equiv 1 \mod \varphi(N)}$.
2. Bob ricevuto (e, N) calcola:

$$m^e \mod N = C$$

e lo invia a Alice. Quest'ultima per decifrare il messaggio eseguirà:

$$C^d \mod N = m$$

1.1 Perchè RSA funziona?

Sappiamo che: $\boxed{C = m^e \mod N} \Rightarrow C^d \mod N = m^{e \times d} \mod N$
inoltre

$$\boxed{e \times d \equiv 1 \mod \varphi(N)}$$

che equivale a:

$$e \times d \mod \varphi(N) = 1$$

allora posso scrivere:

$$e \times d = k \times (\varphi(N)) + 1 = k(p-1)(q-1) + 1$$

e quindi:

$$m^{e \times d} \mod N = m^{k(p-1)(q-1)+1} \mod N = m^{k(p-1)(q-1)} \times m \mod N$$

Se dimostriamo che $\boxed{m^{k(p-1)(q-1)} \mod N = 1}$ otteniamo la tesi.

Poiché

$$m^{k(p-1)(q-1)} \mod q = [m^{q-1}]^{k(p-1)} \mod q$$

e per il *piccolo Teorema di Fermat*:

$$\boxed{m^{q-1} \equiv 1 \mod q}$$

si ha allora:

$$(m^{(q-1)})^{k(\mathbf{p-1})} \mod q = 1^{k(p-1)} \mod q = 1$$

analogamente:

$$m^{k(p-1)(q-1)} \mod p = [m^{p-1}]^{k(q-1)} \mod p = 1^{k(q-1)} \mod p = 1$$

Dai due risultati:

$$m^{k(p-1)(\mathbf{q-1})} \mod q = 1$$
$$m^{k(q-1)(\mathbf{p-1})} \mod p = 1$$

Che possiamo scrivere come:

$$\begin{cases} 1 \equiv a \mod q \\ 1 \equiv b \mod p \end{cases}$$

Indicando con $\boxed{a = m^{k(p-1)(\mathbf{q-1})}}$ e con $\boxed{b = m^{k(q-1)(\mathbf{p-1})}}$ Possiamo quindi applicare il *teorema cinese del resto* e scrivere:

$$m^{k(p-1)(q-1)} \mod (q \times p) = m^{k(p-1)(q-1)} \mod N = 1$$

$\boxed{\text{teorema cinese del resto.}}$

$$\begin{cases} x \equiv a \mod p \\ x \equiv b \mod q \end{cases}$$

Se
p e q sono coprimi
$\exists!$ la soluzione x modulo pq

1.2 Il teorema cinese del resto: una semplice applicazione

Supponiamo di dover contare un esercito di uomini sapendo solo che:

- disposti in 7 file rimangono 3 soldati nell'ultima riga;
- disposti in 8 file ne rimangono 5 nell'ultima riga;

. In pratica il problema consiste nel risolvere il seguente sistema:

$$\begin{cases} x \equiv 3 \mod 7 \\ x \equiv 5 \mod 8 \end{cases}$$

La prima equazione del sistema dice che $x = k * 7 + 3$ mentre per la seconda deve aversi $x = k * 8 + 5$ con $k \in \mathbb{Z} = \{\text{Insieme degli Interi}\}$
Facendo variare $k = 1, 2, \ldots$ dovrò cercare il primo valore comune alle 2 espressioni. Questo valore esisterà se i due moduli sono coprimi.

$$x = k * 7 + 3 \text{ dove k è: } 1, 2, \ldots \text{ darà } x = 10, 17, 24, 31, 38, \mathbf{45}, 52 \ldots$$

$$x = k * 8 + 5 \text{ dove k è: } 1, 2, \ldots \text{ darà } x = 15, 21, 29, 37, \mathbf{45}, 53, \ldots$$

La soluzione sarà dunque:

$$\boxed{\text{x=45}}$$

Questo significa che l'esercito sarà costituito da 45 soldati.