RSA (Crittografia Asimmetrica)

Prof. Salvatore D'Asta

20 febbraio 2021

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 $\phi(N) = (p-1) \times (q-1)$.
   - Trova $0 < e < N$ in modo che $MCD(e, \phi(N)) = 1$ (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 $\boxed{e \times d \equiv 1 \mod N}$.
2. Bob ricevuto (e, N) calcola:

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

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

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

Perchè RSA funziona?

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

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

che equivale a:

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

allora posso scrivere:

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

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

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

e per il Teorema piccolo Teorema di Fermat:

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

si ha allora:

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

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:

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

Applicando il *teorema cinese del resto* posso scrivere:

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