RSA (Crittografia Asimmetrica)

Prof. Salvatore D'Asta

14 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 $d \equiv e \mod N$ ossia $\boxed{e \times d \equiv 1 \mod N}$.
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

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

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:

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

Applicando il *teorema cinese del resto* posso scrivere:

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

equivale a dire che e $e \times d \equiv 1 \mod N$ e quindi che sono uno l'inverso dell'altro. Quindi calcolare $c^d \mod N$ equivale a calcolare $(m^e)^d \mod N = m^{e \times d}$ e poiché $e \times d \mod N = 1$ Allora sarà

$$m^1 \mod N = m$$

Sia p un numero primo molto grande. Si può dimostrare che $\exists g \in \mathbb{Z}_p$ generatore di $\mathbb{Z}_p$. Questo significa che $\forall h \in \mathbb{Z},\ \exists k \setminus g^h \mod p = k \in \mathbb{Z}_p$

Se g è un generatore di $\mathbb{Z}_p$ con p primo, allora:

$$g^1 \mod p; g^2 \mod p; g^3 \mod p \dots g^p \mod p$$

Sono distinti e compresi tra 1 e $p-1$.
Per un qualsiasi intero b ed un generatore g di N si può trovare un esponente unico i che

$$b \equiv g^i \mod N$$

dove $0 \leq i \leq (p-1)$

Logaritmo discreto

Si consideri il numero primo $p = 56509$ e sia 2 il generatore di $\mathbb{Z}_p$ calcolare il **logaritmo discreto** di $h = 38679$ equivale a trovare l'esponente x a cui bisogna elevare la base 2 per ottenerlo in $\mathbb{Z}_p$. In pratica equivale a risolvere la seguente equazione rispetto all'incognita x:

$$2^x \mod p = 38679$$