

# Crittografia asimmetrica: RSA

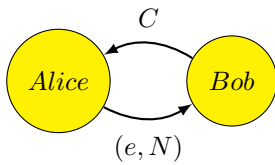
Prof. Salvatore D'Asta

19 febbraio 2021

## Indice

<b>1</b>	<b>Algoritmo RSA</b>	<b>2</b>
1.1	Perchè RSA funziona? . . . . .	2
1.2	Il teorema cinese del resto: una semplice applicazione . . . . .	3

# 1 Algoritmo RSA



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

- 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  $(d, N)$  trovando  $d$  tale che  $e \times d \equiv 1 \pmod{\varphi(N)}$ .
- Bob ricevuto  $(e, N)$  calcola:

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

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

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

## 1.1 Perché RSA funziona?

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

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

che equivale a:

$$e \times d \pmod{\varphi(N)} = 1$$

allora posso scrivere:

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

e quindi:

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

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

Poiché

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

e per il *piccolo Teorema di Fermat*:

$$m^{q-1} \equiv 1 \pmod q$$

si ha allora:

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

analogamente:

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

Dai due risultati:

$$[1cm]$$

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

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

Che possiamo scrivere come:

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

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

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

teorema cinese del resto.

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

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:

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

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  $k = 1, 2, \dots$  dovrò cercare il primo valore comune alle 2 espressioni.

Questo valore esisterà se i due moduli sono coprimi.

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

$$x = k * 8 + 5 \text{ dove } k \text{ è: } 1, 2, \dots \text{ darà } x = 13, 21, 29, 37, \mathbf{45}, 53, \dots$$

La soluzione sarà dunque:

$$\boxed{x=45}$$

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