

CRITTOGRAFIA A CHIAVE PUBBLICA - RSA (1)

RSA Rivest, Shamir, Adleman 1976

Alice

Sceglie p, q numeri primi
con $p \neq q$

Calcola $N = pq$ e

$$\varphi(N) = (p-1)(q-1)$$

Sceglie r con

$$(r, \varphi(N)) = 1$$

Trova (con l'algoritmo di
Euclide) s (e t) tali
che

$$1 = r \cdot s + \varphi(N) \cdot t$$

Rende pubblica la

coppia

$$(N, r)$$

mentre tiene segreto
l'intero

s

Bob

Vuole mandare

ad Alice un

messaggio b con

$$0 < b < N \text{ e } (b, N) = 1.$$

Alice

Riceve da Bob
il messaggio a .

Calcola

$$a^s \bmod N$$

e ritrova b .

Infatti

$$1 = r \cdot s + \varphi(N) \cdot t$$

così

$$b = b^1 = b^{rs + \varphi(N)t}$$

$$\equiv b^{rs} \cdot b^{\varphi(N)t}$$

$$\equiv (b^r)^s \cdot (b^{\varphi(N)})^t$$

$$\equiv a^s \cdot 1 = a^s \bmod N$$

perché, per il Teorema di

Eulero,

$$b^{\varphi(N)} \equiv 1 \bmod N$$

e dunque $b^{\varphi(N)t} \equiv 1 \bmod N$

Bob ②

Calcola

$$b^r \bmod N = a$$

e spedisce ad Alice

il messaggio a

Alice

③

Bob

Calcola

$$b^r \bmod N \text{ cioè}$$

calcola

$$5^7 \bmod 22 = 3$$

Spedisce 3 ad Alice

Riceve da Bob il

messaggio $3 = a$.

Calcola

$$a^s \bmod N \text{ cioè}$$

calcola

$$3^3 \bmod 22 = 5$$

e dunque ricostruisce

il messaggio originale

di Bob.

Osservazioni

1) Scoprire s è tanto difficile quanto fattorizzare

$$N = p \cdot q$$

2) E' possibile sapere se un dato numero è primo senza aver bisogno della sua fattorizzazione.

④ 3) Quello descritto è l'RSA ridotto all'osso.

Si possono fare molte altre considerazioni per renderlo più sicuro ed efficace.

4) L'esempio è particolarmente bene perché abbiamo fatto i conti senza calcolatrici o calcolatori.

ESERCIZIO

Supponete di ricevere messaggi crittati usando il metodo RSA. La coppia (N, e) che avete scelto (chiave pubblica) è $(65, 35)$ (dunque $p = 13$ e $q = 5$). Supponete di ricevere un messaggio. Chi vi scrive trasforma i propri messaggi, come prima cosa, in sequenze di numeri secondo la corrispondenza

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z
2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22

Inoltre, una volta trasformato il messaggio in sequenza di numeri, lo codifica usando l'RSA con la vostra chiave pubblica e ve lo spedisce. Voi riceverete il messaggio

33	6	57	11	22	23	33
----	---	----	----	----	----	----

Definizione.

5

Conviene risolvere l'esercizio facendo fare i conti a un computer. Scegliete voi come fare. Una possibilità è usare il software gratuito GAP (Groups, Algorithms, Programming) che potete scaricare all'indirizzo web

www.gap-system.org

Se usate gap alcune istruzioni utili sono

$p := 13$; pone la variabile p uguale a 13

$\text{Gcd}(a, b)$; calcola il massimo comune divisore (greatest common divisor) tra a e b

$\text{GcdRepresentation}(a, b)$; calcola una coppia di interi s, t con

$$(a, b) = as + bt \quad (\text{identità di Bezout})$$

Notate che 'GcdRepresentation' fornisce in uscita una stringa

$[s, t]$

Se pongo

$$g := \text{GcdRepresentation}(a, b);$$

allora

$g[1]$; mi dà l'intero s e

$g[2]$; mi dà l'intero t .