RSA

Leonardo Bizzoni

November 4, 2023

1 Creazione della chiave pubblica e privata

1. Si scelgono 2 numeri primi **grandi** p, q con $p \neq q$
2. Si calcola $N = p * q$
3. Si calcola la funzione di Eulero $\varphi(N) = \varphi(p * q) = \varphi(p) * \varphi(q) = (p-1)(q-1)$
4. Si sceglie un intero e(*negli appunti della prof viene usato* r) tale che:
   - $1 < e < \varphi(N)$
   - $(\varphi(N), e) = 1$ quindi $\exists d \mid d * e \equiv 1 \bmod \varphi(N)$

   La coppia (e, N) forma la **chiave pubblica**.

1. Si applica l'algoritmo di Euclide a $\varphi(N)$ e e trovando 2 interi d, t tali che $ed + \varphi(N)t = 1$ (*una volta trovato* d *ce ne possiamo fregare di* t)

   d è la **chiave privata**.

1.1 Info extra

e sta per *encryption* metre d sta per *decription*.
Per p, q "grandi" si intende $p, q \geq 2^{512}$.
Quando si parla di RSA-1024 vuol dire che $N = 2^{512} * 2^{512} = 2^{1024}$.

2 Cifratura di un messaggio

Data una chiave pubblica (N, e) ed un messaggio $0 < x < N$ (ovvero $x \in \mathbb{Z}_N = \{0, 1, \cdots, N-1)$ allora il messaggio criptato y sarà:

$$y = x^e \bmod N$$

3 Decifratura di un messaggio

Data una chiave privata d ed un messaggio cifrato $0 < y < N$ allora il messaggio in chiaro x sarà:

$$x = y^d \bmod N$$

4 Esercizi

$K_{pub} (N, e) = (143, 47)$

$p = 11 \qquad q = 13 \qquad y = 9$

$d = [47]^{-1}_{143} = [23]_{143}$

$\varphi(143) = \varphi(11) \cdot \varphi(13) = 10 \cdot 12 = 120$

$120 = 47 \cdot 2 + 26 \qquad 26 = a - 2b$

$47 = 26 + 21 \qquad 21 = 3b - a$

$26 = 21 + 5 \qquad 5 = 2a - 5b$

$21 = 5 \cdot 4 + 1 \qquad 1 = 3b - a - 4(2a - 5b)$

$5 = 1 \cdot 5 + 0 \qquad = 23b - 9a$

$x = y^D \bmod 143 = 9^{23} \bmod 143 = 3 \bmod 143$

$MCD(143, 9) = 1$

$143 = 9 \cdot 15 + 8$

$9 = 8 + 1$

$8 = 1 \cdot 8 + 0$

0		
1	1	$C_0 = 1$
2	0	$C_1 = 1^2 \cdot 9^1 = 9 \bmod 143$
5	1	$C_2 = 9^2 \cdot 9^0 = 81 \bmod 143$
11	1	$C_3 = 81^2 \cdot 9^1 = -10 \bmod 143 \ (= 133 \bmod 143)$
23	1	$C_4 = (-10)^2 \cdot 9^1 = 42 \bmod 143$
		$C_5 = 42^2 \cdot 9 = 3 \bmod 143$

$K_{pub} = (N, e) = (437, 233)$

$p = 19 \qquad q = 23 \qquad y = 3$

$\varphi(437) = 18 \cdot 22 = 396$

$d = [233]^{-1}_{437} = 17$

$396 = 233 + 163 \qquad 163 = a - b$

$233 = 163 + 70$

$163 = 70 \cdot 2 + 23$ $\quad 23 = 3a - 5b$

$70 = 23 \cdot 3 + 1$ $\quad 1 = 17b - 10a$

$X = y^d \bmod 437 = 3^{17} \bmod 437 = 108$

17	1
8	0
4	0
2	0
1	1
0	

$17 = 10001$

$C_0 = 1$

$C_1 = 1^2 \cdot 3^1 = 3 \bmod 437$

$C_2 = 3^2 \cdot 3^0 = 9 \bmod 437$

$C_3 = 9^2 \cdot 3^0 = 81 \bmod 437$

$C_4 = 81^2 \cdot 3^0 = 6 \bmod 437$

$C_5 = 6^2 \cdot 3^1 = 108 \bmod 437$

$36 \cdot 3 = 108$

$81 \cdot 81 = 6561$

$6561 : 437 = 15$ Rest $6561 - 15 \cdot 437 = 6561 - 6555 = 6$

$686 - 437 = 249$

$13 \cdot 437 = 5681$