

Crittografia in chiave pubblica

Fin dai tempi di Euclide si sà che i numeri primi sono infiniti e che sono distribuiti in maniera irregolare tra i numeri interi.

Negli anni 80 i grandi numeri primi sono stati usati per cifrare messaggi segreti con il metodo RSA (Rivest, shamir e Adleman - Massachusetts Institute of Technology).

Crittografia in chiave pubblica - Metodo RSA

Il metodo RSA (Rivest, shamir e Adleman - Massachusetts Institute of Technology) richiede:

- Numeri segreti: p, q numeri primi e N numero primo con $(p - 1)(q - 1)$
- Chiave pubblica: prodotto pq e un numero M tale che $MN - 1$ è multiplo di $(p - 1)(q - 1)$
- $x \leq pq$ messaggio da trasmettere = numero intero positivo
- y messaggio cifrato = resto di x^M diviso pq
- \tilde{y} messaggio decifrato = resto di y^N diviso pq

Crittografia in chiave pubblica - in pratica...e considerazioni

- si considera il messaggio
- lo si trasforma in cifre con un qualsiasi metodo (eventualmente lo si spezzetta)
- si scelgono p, q **molto grandi** in modo che sia impossibile fattorizzare pQ in un **tempo ragionevole**

Tanto più p e q sono grandi, quanto più lungo è il calcolo di y (messaggio cifrato) e il calcolo di \tilde{y} (messaggio decifrato).