CENNI MATEMATICI

Per poter trattare dell'algoritmo RSA sono necessari alcuni cenni matematici.

Innanzitutto bisogna dare una definizione di numero primo e di numero composto: quest'ultimo è fattorizzabile in numeri primi, mentre i numeri primi sono divisibili unicamente per 1 e per se stessi

Inoltre bisogna introdurre l'aritmetica modulare: un ramo della matematica che studia i resti delle divisioni, che vengono definiti moduli. Per esempio 10 modulo 3 è congruente a 1, in quanto il resto della divisione intera è 1

FUNZIONE DI EULERO

La funzione di Eulero è una particolare funzione, per calcolare la quale è necessario conoscere la scomposizione in fattori primi del numero. La funzione presenta tuttavia delle particolarità, infatti se il numero di cui si vuole calcolare PHI è primo, allora il risultato della funzione sarà semplicemente il numero sottratto di un'unità. Altra particolarità è che la funzione del prodotto è uguale al prodotto delle funzioni.

TEOREMI

Ruolo importante gioca anche il teorema di Femat: esso afferma che, considerati due numeri “a” e “p”, primi tra loro e di cui “p” è anche primo, a^(p-1)=1 mod p.

Inoltre generalizzando, se consideriamo n come intero positivo primo, allora possiamo asserire che a^(PHI(n)) = 1 mod n, in quanto PHI(n) è uguale a n-1.

INVERSO

In algebra l'inverso di un numero x è y tale che x\*y=1; lo stesso accade in aritmetica modulare con modulo n, quindi l'inverso di x sarà y tale che [ … ].

bisogna notare che questo è possibile solo se X ed N sono coprimi ed è calcolabile secondo la formula [ …. ]

GENERAZIONE DELLE CHIAVI

La generazione delle chiavi è un processo relativamente semplice. Inizialmente bisogna individuare due numeri primi molto grandi,di circa 300 cifre; in seguito è necessario calcolarne il prodotto n. Si procede quindi calcolando PHI(n), che grazie alle affermazioni fatte prima è la funzione di un prodotto, quindi calcolabile in quel modo e dato che p e q sono primi, calcolare PHI(n) è semplice. Successivamente si procede scegliendo un numero e, minore di PHI(n) e coprimo con esso. L'ultimo passaggio consiste nella generazione di un numero d, inverso di e modulo PHI(n). Le chiavi sono quindi le coppie (n,d) e (n,e).

CIFRATURA/DECIFRATURA

La cifratura e la decifratura sono operazioni facili ma complesse: è sufficiente eseguire degli elevamenti a potenza in modulo n per passare dal messaggio in chiaro al messaggio cifrato. Questo tipo di operazioni sono abbastanza complesse per il calcolatore: se la chiave aumenta in maniera notevole anche il numero di operazioni da eseguire cresce

CONCLUSIONI

La forza dell'algoritmo risiede nel fatto che per scoprire la chiave privata è necessario fattorizzare n. grazie agli algoritmi e gli strumenti attualmente a nostra disposizione, dato che n dovrebbe essere di circa 300 cifre, ciò è computazionalmente molto complesso, tale da essere praticamente impossibile, se le chiavi hanno sufficiente dimensione.