Crittografia Asimmetrica: il metodo RSA

Premessa: non si forniscono dimostrazioni alla validità del sistema, ma soltanto i passi per la codifica e la decodifica del messaggio.

Si tratta di un metodo a chiave pubblica. Il nome deriva dalle iniziali dei nomi dei ricercatori a cui è dovuto il metodo: Rivest, Shamir, Adlemann.
L'idea è la seguente: supponiamo che A voglia mandare un messaggio segreto a B. Il destinatario B consegna ad A una chiave pubblica (che può essere vista come un lucchetto che è stato dato ad A da B) con la quale A codifica il messaggio da mandare (si può pensare che A chiuda con il lucchetto il messaggio in una scatola che poi spedisce a B). Quando B riceve il messaggio, egli utilizza la chiave privata, che è posseduta soltanto da lui, per decifrare il messaggio (si può pensare che B apra il lucchetto della scatola contenente il messaggio arrivatogli da A con la chiave del lucchetto che solo B possiede). Benché sia possibile costruire la chiave privata da quella pubblica, il sistema per farlo è molto complicato e difficile da attuare (si può pensare che in linea di principio sia possibile costruire una chiave per aprire un lucchetto se si possiede il lucchetto, ma ciò non è sicuramente alla portata di tutti).

Vediamo come si costruiscono la chiave privata e quella pubblica:

Si prendono due numeri primi p e q. Detto *m* il prodotto $m=pq$, sia E un numero che sia primo con il prodotto $(p-1)(q-1)$. La coppia (m, E) è la *chiave pubblica* (con la quale il mittente codifica il messaggio).

Per determinare la *chiave privata* (con la quale il destinatario decodifica il messaggio) si trova un numero $D=[k(p-1)(q-1)+1]/E$ dove k va scelto in modo che D sia un numero intero. Ad esempio, se $p=2, q=5, E=3$ allora se $k=5$, si ha $D=7$, se $k=2, D=3$, se $k=185, D=247$, se $k=8, D=11$ etc... (ci sono infinite scelte per k che fanno essere D un numero intero!). La coppia (m, D) è la *chiave privata* (che B si è costruito scegliendo uno fra i possibili k).

Adesso A deve codificare il messaggio da spedire. Possiamo supporre, a titolo di esempio, che il messaggio sia un numero: esiste la possibilità, fra l'altro, di trasformare un messaggio di testo in una serie di numeri, ad esempio utilizzando il codice ASCII. Codifichiamo allora 4 2 1.
Ogni cifra c viene codificata con la formula $c^E \bmod m$.

Con l'esempio precedente $(p=2, q=5, E=3, m=10)$, il messaggio 4 2 1 diviene 4 8 1 (il fatto che la cifra 4 e la cifra 1 rimangano inalterate è casuale e dipende dalle scelte fatte per i parametri utilizzati).

Il mittente A a questo punto manda il messaggio 4 8 1 al destinatario B che procede a decifrarlo utilizzando la chiave privata. Ogni cifra c viene decodificata con la formula $c^D \bmod m$. Supponendo che la chiave privata scelta da B sia $(10,7)$ (che significa che B ha scelto il valore $k=5$ che fa essere $D=7$), il messaggio 4 8 1 diviene 4 2 1.

Come premesso, non si fornisce la dimostrazione del fatto che con l'operazione di decodifica ritorni il messaggio iniziale spedito da A.

E' da tener presente che quando i numeri primi sono molto grossi (e quindi non è il caso dell'esempio qui utilizzato) è praticamente impossibile che dalla chiave pubblica si riesca a trovare la chiave privata. E' sempre bene non tenere traccia dei numeri primi scelti per rendere ancora più difficile la possibilità di scoprire la chiave privata.