LICEO SCIENTIFICO "PLINIO SENIORE"
LICEO MATEMATICO - CLASSE PRIMA

ALGORITMO DI CIFRATURA RSA

1. Introduzione

L'algoritmo di cifratura asimmetrica RSA si basa sull'uso di due chiavi distinte generate in modo che sia impossibile ricavarne una dall'altra. Le due chiavi, dette **chiave pubblica** e **chiave privata**, servono rispettivamente per cifrare e per decifrare il messaggio.
Così facendo si viene a creare una sorta di "elenco telefonico" a disposizione di tutti gli utenti, che raggruppa tutte le chiavi dirette, mentre quelle inverse saranno tenute segrete dagli utenti che le hanno create e da questi utilizzate solo quando ricevono un messaggio cifrato con la rispettiva chiave pubblica dell'"elenco" da parte di un certo mittente, ottenendo in questo modo i presupposti necessari alla sicurezza del sistema. Quindi una persona che voglia comunicare con un'altra persona in modo sicuro non deve far altro che cifrare il messaggio con la chiave pubblica del destinatario. Il ricevente, una volta ricevuto il messaggio, non dovrà fare altro che decifrarlo con la chiave segreta personale.
Chiunque utilizzi questo tipo di protocollo di comunicazione possiede quindi una **coppia di chiavi**, quella pubblica può essere tranquillamente distribuita e resa di pubblico dominio perché consente solo di cifrare il messaggio, mentre quella privata deve essere conosciuta solo da una persona.
Se la prima chiave viene usata per la cifratura, la seconda deve necessariamente essere utilizzata per la decifratura e viceversa. La questione fondamentale è che nonostante le due chiavi siano fra loro dipendenti, non sia possibile risalire dall'una all'altra, in modo che se anche si è a conoscenza di una delle due chiavi, non si possa risalire all'altra, garantendo in questo modo l'integrità della crittografia.

Facendo un esempio pratico, se **Alice** vuole spedire un messaggio a **Bob** e non vuole che altri all'infuori di **Bob** possano leggerlo, **Alice** cercherà sull'elenco la chiave pubblica di **Bob** e con quella potrà cifrare il messaggio. Essendo **Bob** l'unico a possedere la chiave inversa, sarà anche l'unico a poter decifrare il messaggio, che rimarrà così segreto per tutti gli altri, compresa **Alice**, che non disponendo della chiave inversa non sarà in grado di decifrare il messaggio da lei stessa creato. Ovviamente il successo di questo sistema si basa sull'assoluta necessità che **Bob** sia l'unico ad essere in possesso della chiave inversa. In caso contrario, avendo entrambe le chiavi, chiunque potrebbe decifrare agevolmente il messaggio.
Con questo metodo di cifratura è possibile anche garantire la provenienza di un messaggio. Riprendiamo l'esempio precedente: **Alice** questa volta, prima di cifrare il messaggio usando la chiave pubblica di **Bob**, lo cifrerà usando la propria chiave privata e solo in un secondo momento lo ri-crittograferà utilizzando la chiave pubblica di **Bob**. Quando **Bob** riceverà il messaggio e lo decifrerà usando la propria chiave privata, otterrà ancora un messaggio crittografato. Quel dato messaggio necessiterà poi della chiave pubblica di **Alice** per essere decifrato, garantendo in questo modo che il messaggio è stato spedito solo e soltanto da **Alice**, unica a possedere la chiave privata con la quale era stato crittografato il messaggio.
Più semplicemente, utilizzando questo metodo di cifratura, **Alice** può mandare messaggi a tutti, garantendo la provenienza. Infatti cifrando il messaggio con la propria chiave privata, chiunque sarà in grado di leggere il messaggio, decifrandolo con la sua chiave pubblica, assicurandosi in tal modo che il mittente sia proprio **Alice**.
La prima applicazione dell'RSA è stata sviluppata nel 1978 da ***Ronald Rivest, Adi Shamir*** e ***Leonard Adleman***, (RSA è l'iniziale dei nomi degli ideatori dell'Algoritmo).
Il metodo di cifratura risulta essere ancora oggi inviolato, l'efficacia di tale algoritmo non consiste nella segretezza del modo in cui è implementato (il procedimento è conosciuto) ma nella difficoltà di invertire l'algoritmo in tempi accettabili ovvero sull'elevata complessità computazionale della fattorizzazione in numeri primi.

Ad oggi, con la tecnologia attuale, per fattorizzare un numero a 500 cifre ci vorrebbe un tempo pari alla vita stimata dell'universo (10^{25} anni).
Per ottenere una discreta sicurezza è necessario utilizzare chiavi binarie di almeno 2048 bit. Quelle a 512 bit sono ricavabili in poche ore. Le chiavi a 1024 bit, ancora oggi largamente utilizzate, non sono più consigliabili.[2] La fattorizzazione di interi grandi, infatti, è progredita rapidamente mediante l'utilizzo di hardware dedicati, al punto che potrebbe essere possibile fattorizzare un intero di 1024 bit in un solo anno di tempo, al costo di un milione di dollari (un costo sostenibile per qualunque grande organizzazione, agenzia o intelligence).

2. Procedimento per la generazione della chiave pubblica e privata

- Chiave Pubblica, formata da 2 numeri **(n; e)**
- Chiave Privata, formata da 2 numeri (**n; d)**

1. Si scelgono due numeri primi **(p; q)** abbastanza grandi (maggiori di 300 cifre). Si calcola il loro prodotto chiamato anche modulo **n**=p·q (ovviamente la fattorizzazione è segreta) e si pone **z** =(p-1)·(q-1). (La funzione z coincide con la **funzione di Eulero** quando **n** è il prodotto di due numeri primi, tale funzione associa a un numero intero n il numero dei numeri interi co-primi con n e minori di n compreso l'uno. Se **n** è un numero primo z(n) =n-1).
2. Si sceglie poi un numero ***e*** chiamato esponente pubblico, coprimo con **z** e più piccolo di **z** stesso (**e** non deve necessariamente essere primo).
3. Si sceglie il numero ***d*** chiamato esponente privato tale che il suo prodotto con ***e*** sia congruo a 1 mod(z), cioè $\mathbf{d \cdot e \equiv 1 \mod(z)}$

La chiave pubblica è **(n; e)** mentre quella privata è (**n; d)**

La forza dell'algoritmo è che per calcolare **d** ed **e** non basta conoscere **n** ma si deve conoscere anche **z** e fattorizzarlo in fattori primi richiede molto tempo.

3. Cifratura del messaggio

Un messaggio **M** viene cifrato attraverso l'operazione $\mathbf{M^e \pmod n}$ trasformandolo nel messaggio cifrato **c**. Una volta trasmesso **c** viene decifrato con $\mathbf{c^d \equiv M \pmod n}$. Il procedimento funziona solo se la chiave pubblica **e** e quella privata **d** sono legate dalla relazione $d \cdot e \equiv 1 \ (mod\ z)$. Quindi quando un messaggio viene cifrato con una chiave può essere decifrato solo con l'altra e viceversa.

La forza di questo algoritmo si basa però sull'assunzione che calcolare la radice e-esima di *c* mod (n) con n numero composto sia un problema non trattabile computazionalmente.

Esempio di applicazione:
Determinazione Chiave Pubblica:
p = 3, **q** = 11 $\Rightarrow$ **n** = 3·11 = 33 $\Rightarrow$ **z** = 2·10 = 20
Si prende **e**=7 dato che deve essere co-primo di 20 e minore di 20 stesso.
Sia **d**=3 infatti d·e=21 e $21 \equiv 1 \pmod{20}$

Quindi abbiamo la chiave privata (33; 3) e la chiave pubblica (33;7) e il fatto che **d** sia uguale a **p** è casuale.

Cifratura e decifratura

Prendiamo ora in considerazione il messaggio M=15; e cifriamolo per ottenere il messaggio cifrato **c**; ovviamente possiamo usare i 33 e 7, ma non 3 che fa parte della chiave privata.

$c = M^e \pmod n$ quindi nel nostro esempio **$c = 15^7 \equiv 27 \pmod{33}$.**

Infatti $15^2 \equiv 27 \pmod{33}$ da cui $15^3 = 15 \cdot 15^2 \equiv 15 \cdot 27 = 5 \cdot 81 \equiv 5 \cdot 15 = 75 \equiv 9 \pmod{33}$

$15^6 = (15^3)^2 \equiv 9^2 = 81 \equiv 15 \pmod{33}$ e $15^7 = 15 \cdot 15^6 \equiv 15 \cdot 15 = 15^2 \equiv 27 \pmod{33}$

ALTRO METODO

$15^2 \equiv 27 \pmod{33}$ *e* $81 \equiv 15 \pmod{33}$ da cui $15^6 \equiv 27^3 \pmod{33} = 3^4 \cdot 3^4 \cdot 3 \equiv 15^2 \cdot 3 \pmod{33} \equiv 27 \cdot 3 = 81 \equiv 27 \pmod{33}$

Per la decifratura bisogna usare la chiave privata nella formula **$c^d \equiv M \pmod n$**. Quindi **$27^3 \equiv 15 \pmod{33}$.**

Infatti $27^3 = 27 \cdot 27^2 \equiv 27 \cdot (-6)^2 = 27 \cdot 36 \equiv 27 \cdot 3 = 81 \equiv 15 \pmod{33}$

Ecco dunque il messaggio decodificato.

4. Esercizi Proposti

1. Calcola la chiave pubblica (n,e) e privata (n,d) dati p=7, q=13, e=11.
2. Calcola la chiave pubblica (n,e) e privata (n,d) dati p=7, q=17, e=5.
3. Date la seguente chiave pubblica (35;5) e volendo trasmettere il messaggio m=2, cifrare e m utilizzando RSA .
4. Date la seguente chiave pubblica (33;3) e volendo trasmettere il messaggio m=2, cifrare e m utilizzando RSA .