TECNICHE DI CRITTOGRAFIA PER L'INTERNET SECURITY

SISTEMI E RETI
Prof. Verga - Prof.ssa Dalbesio
A.S. 2023/24

L'ALGORITMO DI CRITTOGRAFIA RSA

L'**RSA** è un **algoritmo a chiave asimmetrica** che deve il suo nome alle iniziali dei matematici che lo crearono nel 1977: Ronald Rivest, Adi Shamir e Leonard Adleman.

Gli algoritmi asimmetrici hanno il loro punto di forza nella difficoltà a scoprire la chiave privata, anche conoscendo quella pubblica.

L'ALGORITMO DI CRITTOGRAFIA RSA

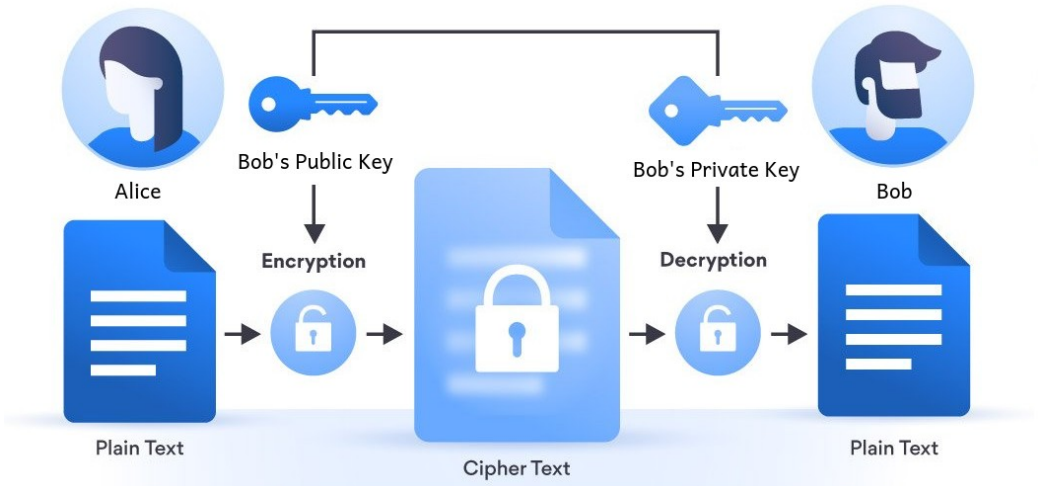
Una delle operazioni più difficili e lunghe da eseguire anche per i più potenti elaboratori è la **fattorizzazione di numeri** a molte cifre. Se poi il numero da fattorizzare è il prodotto di due numeri primi (quindi vi sono due e solo due fattori) molto grandi, allora diventa veramente difficile rompere il cifrario.

L'**RSA si basa proprio sulla difficoltà nel fattorizzare un numero intero N molto grande ottenuto dal prodotto di due numeri primi** (p e q, anch'essi molto grandi) che restano segreti.

L'ALGORITMO DI CRITTOGRAFIA RSA

Vediamo i passi dell'algoritmo con un esempio:

1. **Alice** vuole trasmettere un messaggio **m** a **Bob**: affinché il dialogo resti confidenziale sarà Bob a dover creare la coppia di chiavi $\mathbf{K_{PUB}}$ e $\mathbf{K_{PRI}}$, rispettivamente pubblica e privata.



L'ALGORITMO DI CRITTOGRAFIA RSA

2. **Bob** crea la chiave pubblica costituita da una coppia di numeri $\mathbf{K_{PUB} = (N, N_{PUB})}$ e la chiave privata costituita da una coppia di numeri $\mathbf{K_{PRI} = (N, N_{PRI})}$.

Come fa Bob a creare le due chiavi matematicamente correlate in modo che si possa cifrare con una chiave e decifrare con l'altra?

L'ALGORITMO DI CRITTOGRAFIA RSA

2.1. Sceglie due numeri primi **p** e **q**

2.2. N = p · q

2.3. V = (p - 1) · (q – 1)

2.4. Sceglie $\mathbf{N_{pri}}$ in modo tale che non abbia fattori primi con **V** ovvero, $\mathbf{N_{pri}}$ **coprimo con V**.

Nota: N_{pri} non necessariamente numero primo e $N_{pri} < V$

2.5. Ricava $\mathbf{N_{pub}}$ dall'equazione:

$$(\mathbf{N_{pub}} \cdot \mathbf{N_{pri}}) \bmod \mathbf{V} = 1$$

ovvero

$$\mathbf{N_{pub}} \cdot \mathbf{N_{pri}} \equiv 1 \bmod \mathbf{V}$$

L'ALGORITMO DI CRITTOGRAFIA RSA

3. **Bob** distribuisce la chiave pubblica ad Alice e sta molto attento a **non divulgare** N_{pri}.

4. Alice può cifrare e poi trasmettere il messaggio **m** usando la chiave pubblica ricevuta:

$$\mathbf{c = m^{Npub} \bmod N}$$

5. Bob ricevuto il messaggio cifrato **c** può decifrarlo usando la sua chiave privata tenuta segreta:

$$\mathbf{m = c^{Npri} \bmod N}$$

RSA – ESEMPIO:

- scelgo p = 3 e q = 11 come numeri primi, da cui N = 33;
- calcolo V = (3 – 1) · (11 – 1) = 20;
- scelgo N_{PRI} = 7 che non ha fattori in comune con V = 20;
- tra le possibili soluzioni dell'equazione (N_{PUB} · 7) mod 20 = 1 scelgo N_{PUB} = 3 visto che (3 · 7) mod 20 = 21 mod 20 = 1;
- avrò le chiavi K_{PRI} = (33, 7) e K_{PUB} = (33, 3)
- Se per esempio si vuole trasmettere il numero 16, allora:

$$c = 16^3 \bmod 33 = 4$$

- Mentre per decifrare il messaggio:

$$m = 4^7 \bmod 33 = 16$$

VANTAGGI E SVANTAGGI DELL'RSA

La forza di quest'algoritmo sta nel fatto che è difficile calcolare N_{PRI} anche per chi conosce la chiave pubblica $K_{PUB} = (N, N_{PUB})$, perché bisognerebbe prima trovare i due numeri primi *p* e *q* che fattorizzano N.

Fattorizzare i grandi numeri richiede anni e grande potenza di calcolo. Ecco perché i numeri primi sono alla base degli algoritmi di crittografia asimmetrica e vi sono grandi aziende pubbliche e private o enti di ricerca universitaria che non smettono di cercarli.

VANTAGGI E SVANTAGGI DELL'RSA

Il grosso problema dell'RSA e in generale degli algoritmi asimmetrici è la loro lentezza ed il largo uso delle risorse di elaborazione.

La soluzione ottimale è quella di usare la crittografia simmetrica per cifrare i testi e sfruttare la crittografia asimmetrica solo per la breve fase di scambio della chiave segreta simmetrica. In questo modo si protegge la fase delicata della distribuzione delle chiavi simmetriche (grazie alla maggior sicurezza della crittografia asimmetrica) e poi si cifra velocemente (grazie alla maggior velocità della crittografia simmetrica).