Il Criptosistema RSA

Come Funziona la Crittografia Moderna

Prof. Fedeli Massimo

IIS Fermi Sacconi Cpia
Ascoli Piceno

3 gennaio 2026

Perché Abbiamo Bisogno della Crittografia?

Ogni giorno usiamo la crittografia:

- Quando compriamo online (carta di credito)
- Quando chattiamo su WhatsApp
- Quando facciamo home banking
- Quando inviamo email

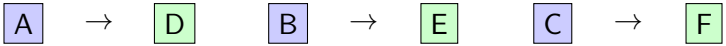
Obiettivo

Proteggere i nostri messaggi da occhi indiscreti!

Il Cifrario di Cesare: Un Esempio Semplice

Giulio Cesare usava un metodo semplicissimo per cifrare i suoi messaggi:

Regola: Spostare ogni lettera di un certo numero di posizioni in avanti (es. 3)



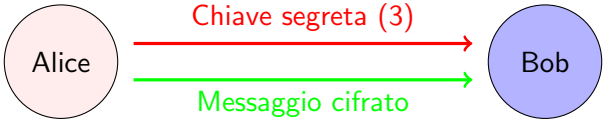
Esempio:

- Messaggio originale: CIAO
- Messaggio cifrato: FLDR

Problema: Se scopro la chiave (3), posso decifrare tutto!

Il Grande Problema delle Chiavi Segrete

Con il Cifrario di Cesare:



Problemi

1. Come faccio a dare la chiave a Bob in modo sicuro?
2. Se qualcuno intercetta la chiave, può leggere tutto!
3. Chi sa cifrare, sa anche decifrare

Oggi: Vogliamo comunicare con milioni di persone su Internet. Impossibile scambiare chiavi segrete con tutti!

La Rivoluzione: Crittografia a Chiave Pubblica

L'idea geniale (1977):

Invece di una chiave, usiamo DUE chiavi diverse:

Chiave Pubblica

- La do a TUTTI
- Serve per CIFRARE

Chiave Privata

- La tengo SOLO IO
- Serve per DECIFRARE

Magia della Matematica!

Cifrare è facile per tutti, decifrare è facile SOLO per me!

Come Funziona nella Vita Reale?

Esempio: Alice vuole ricevere messaggi segreti

1. Alice crea due chiavi:
   - Chiave pubblica: la pubblica su Internet
   - Chiave privata: la tiene nel suo computer
2. Bob vuole scrivere ad Alice:
   - Prende la chiave pubblica di Alice
   - Cifra il messaggio
   - Invia il messaggio cifrato
3. Alice riceve il messaggio cifrato:
   - Usa la sua chiave privata
   - Decifra il messaggio
   - Legge il contenuto

Anche se un hacker intercetta il messaggio, non può decifrarlo!

RSA: La Base Matematica

RSA usa i numeri primi!

Cos'è un numero primo?

Un numero divisibile solo per 1 e per se stesso.

Esempi di numeri primi:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47...

Il Trucco di RSA

- **Facile:** Moltiplicare due numeri primi grandi
- **Difficilissimo:** Fattorizzare il risultato (trovare i due numeri originali)

Esempio semplice:

- Facile: $13 \times 17 = 221$
- Più difficile: $221 = ? \times ?$ (devi provare vari numeri)

RSA: Un Esempio con Numeri Piccoli

Alice vuole creare le sue chiavi:

Passo 1: Sceglie due numeri primi piccoli

- $p_1 = 3$ e $p_2 = 11$
- Calcola: $q = 3 \times 11 = 33$

Passo 2: Sceglie due numeri speciali s e t

- Sceglie $s = 3$ (chiave pubblica)
- Calcola $t = 7$ (chiave privata)

Risultato:

- Chiave pubblica di Alice: $(q = 33, s = 3) \rightarrow$ pubblicata online
- Chiave privata di Alice: $t = 7 \rightarrow$ segreta!

Nota: Nella realtà si usano numeri ENORMI (centinaia di cifre)!

Come Bob Cifra un Messaggio

Bob vuole inviare ad Alice il numero 4

Bob usa la chiave pubblica di Alice: $(q = 33, s = 3)$

Formula di cifratura:

$$\text{messaggio cifrato} = 4^3 \mod 33$$

Calcolo:

$$4^3 = 64$$
$$64 \div 33 = 1 \text{ resto } 31$$
$$\text{Quindi: } 64 \mod 33 = 31$$

Risultato

Bob invia ad Alice il numero 31

Come Alice Decifra il Messaggio

Alice riceve il numero cifrato: 31

Alice usa la sua chiave privata: $t = 7$

Formula di decifratura:

$$\text{messaggio originale} = 31^7 \mod 33$$

Calcolo (semplificato):

$$\begin{aligned} 31^7 \mod 33 &= (\text{calcolo complesso}) \\ &= 4 \end{aligned}$$

Magia!

Alice recupera il messaggio originale: 4

Perché RSA è Sicuro?

Un hacker intercetta:

- Il messaggio cifrato: 31
- La chiave pubblica: $(q = 33, s = 3)$

Per decifrare, l'hacker deve:

1. Fattorizzare 33 per trovare 3×11
2. Calcolare la chiave privata $t = 7$

Con numeri piccoli (33) è facile!

Ma RSA usa numeri con centinaia di cifre...

Esempio reale:

- q ha circa 600 cifre (2048 bit)
- Fattorizzarlo richiederebbe miliardi di anni anche ai supercomputer più potenti!

RSA nella Vita Quotidiana

Dove usi RSA senza saperlo?

Browser Web (HTTPS)

- Quando vedi il lucchetto
- Protegge password e dati

Messaggistica

- WhatsApp, Signal
- Crittografia end-to-end

Email Sicure

- PGP, S/MIME
- Firma digitale

Bitcoin & Crypto

- Portafogli digitali
- Transazioni sicure

RSA protegge miliardi di transazioni ogni giorno!

Punti di Forza e Limitazioni di RSA

Punti di Forza

- Molto sicuro (se ben implementato)
- Non serve scambio di chiavi segrete
- Permette firma digitale
- Standard mondiale

Limitazioni

- Più lento della crittografia simmetrica
- Richiede chiavi lunghe (2048+ bit)
- Vulnerabile ai computer quantistici (futuro)

Nella Pratica

Si usa spesso RSA + crittografia simmetrica insieme:

- RSA per scambiare una chiave segreta
- Crittografia simmetrica (AES) per i dati veri e propri

Conclusioni

Cosa Abbiamo Imparato

- La crittografia moderna usa due chiavi: pubblica e privata
- RSA si basa sulla difficoltà di fattorizzare numeri grandi
- Cifrare è facile, decifrare senza la chiave è quasi impossibile
- RSA protegge la nostra vita digitale quotidiana

Chi ha inventato RSA?

Rivest, Shamir, Adleman (1977)

Il nome RSA viene dalle iniziali dei tre inventori!

Messaggio Finale

La matematica che studiate non è solo teoria: protegge il mondo digitale!

Domande?

fedeli.massimo@iisfermisacconiceciap.edu.it