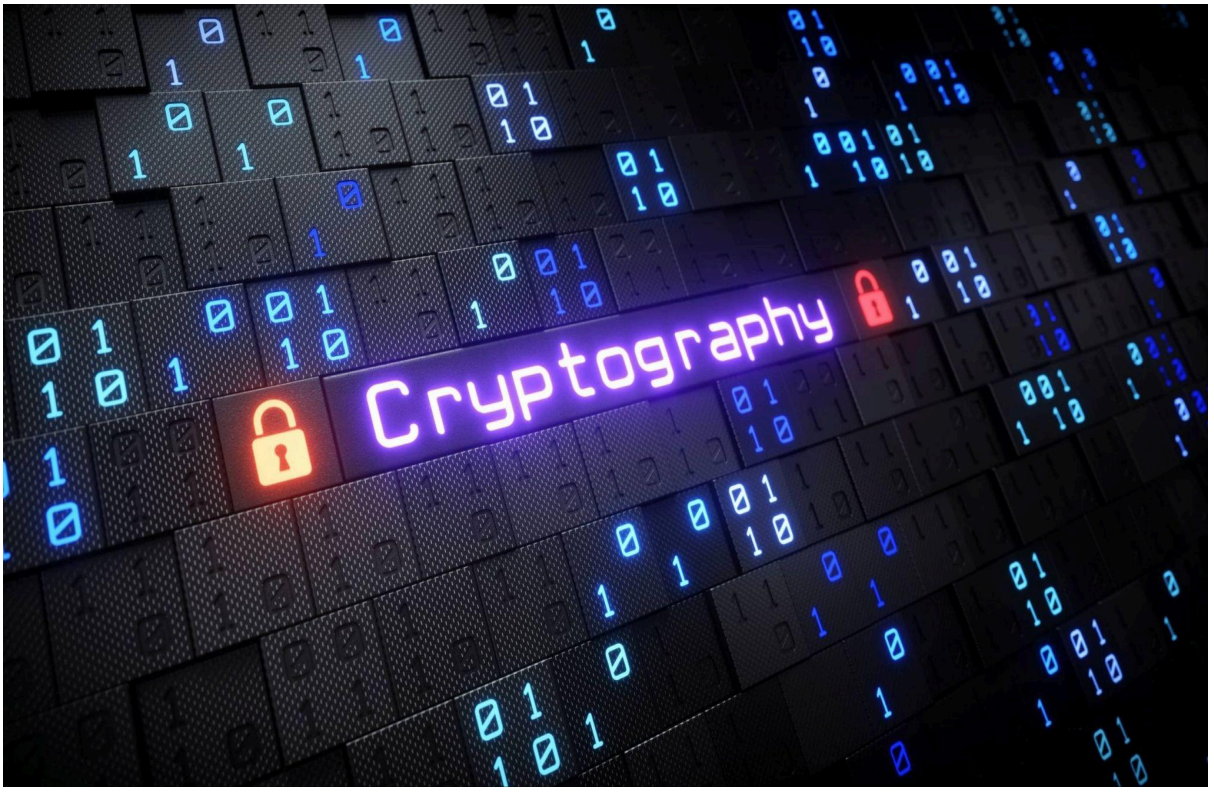
La Crittografia Nella Sicurezza Informatica

Redatto da: Riccardo Droghetti



🛡️ 1. La crittografia: la scienza del segreto

La **crittografia** è uno degli strumenti più importanti della sicurezza informatica. Il suo scopo è quello di garantire che i dati scambiati tra due o più parti siano protetti da accessi non autorizzati, anche se intercettati da terzi. In pratica, la crittografia converte le informazioni in un formato illeggibile (detto **testo cifrato**) e solo chi possiede la giusta **chiave di decifrazione** può ricondurre quei dati alla forma originaria.

🔐 Crittografia simmetrica

La **crittografia simmetrica** si basa su una singola chiave segreta che viene usata sia per cifrare sia per decifrare i dati. È una tecnica molto efficiente in termini di velocità e viene utilizzata, ad esempio, per proteggere file, database e backup.

Tuttavia, presenta un'importante debolezza: la chiave deve essere condivisa tra il mittente e il destinatario in modo sicuro. Se un attaccante riesce a intercettare la chiave, potrà accedere a tutti i dati cifrati.

Esempi di algoritmi simmetrici:

- AES (Advanced Encryption Standard)
- DES (Data Encryption Standard)
- RC4

🔑 Crittografia asimmetrica

La **crittografia asimmetrica**, invece, utilizza una coppia di chiavi: una **chiave pubblica** e una **chiave privata**. La chiave pubblica può essere condivisa con chiunque, mentre quella privata deve essere tenuta segreta. Se un messaggio è cifrato con la chiave pubblica, può essere decifrato solo con la corrispondente chiave privata.

Questo metodo è molto sicuro per la trasmissione di informazioni sensibili, perché elimina la necessità di condividere segreti tramite canali potenzialmente compromessi.

Esempi di algoritmi asimmetrici:

- RSA
- ECC (Elliptic Curve Cryptography)
- ElGamal

🔄 Cifratura ibrida

Nel mondo reale, spesso si utilizza un sistema **ibrido**: la **crittografia asimmetrica** serve per scambiare in sicurezza una chiave simmetrica, che poi viene usata per cifrare il contenuto della comunicazione. Questo metodo combina sicurezza e velocità, ed è alla base dei protocolli HTTPS, TLS/SSL utilizzati nei siti web sicuri.

🌐 2. Le VPN: navigare in sicurezza anche su reti pubbliche

Una **VPN (Virtual Private Network)** è un sistema che crea un collegamento cifrato tra il proprio dispositivo (computer, smartphone, tablet) e un server remoto, creando un “tunnel virtuale” attraverso cui passano tutti i dati.

🔒 Come funziona una VPN

Quando ti connetti a una VPN, tutto il traffico Internet del tuo dispositivo viene incanalato attraverso questo tunnel sicuro. Il traffico viene cifrato, rendendolo illeggibile a chiunque cerchi di intercettarlo — come hacker, fornitori di servizi Internet o reti Wi-Fi pubbliche non sicure.

Il tuo **indirizzo IP viene mascherato** e sostituito con quello del server VPN, rendendo più difficile rintracciare le tue attività online.

🌍 Vantaggi principali delle VPN

- **Sicurezza nelle reti pubbliche**: Utilissima quando si è connessi a reti Wi-Fi pubbliche (bar, hotel, aeroporti), dove gli attacchi "man-in-the-middle" sono frequenti.
- **Protezione della privacy**: Nascondendo il tuo IP e cifrando i dati, una VPN impedisce il tracciamento da parte di siti web e pubblicitari.
- **Accesso a contenuti geo-bloccati**: Permette di "simulare" la connessione da un altro Paese, utile per accedere a contenuti disponibili solo in determinate regioni (es. Netflix USA, BBC iPlayer).
- **Bypassare la censura**: In alcuni Paesi, le VPN sono l’unico modo per accedere a informazioni censurate o bloccate.

✍️ 3. Le firme digitali: autenticità e integrità dei dati

Le **firme digitali** sono un tipo speciale di firma elettronica che utilizzano meccanismi crittografici per garantire **l'autenticità, l'integrità** e il **non ripudio** di un documento.

Sono sempre più utilizzate per firmare digitalmente contratti, atti amministrativi, documenti fiscali, email e file sensibili.

🛠️ Come funziona una firma digitale

1. Il sistema genera un **hash** del documento, cioè una sorta di "impronta digitale" univoca.
2. Questo hash viene poi **cifrato con la chiave privata** del mittente.
3. Chi riceve il documento può **decifrare l'hash con la chiave pubblica** del mittente e confrontarlo con un nuovo hash calcolato sul documento ricevuto.
4. Se i due hash corrispondono, si è certi che:
    - Il documento non è stato modificato (integrità)
    - È stato firmato realmente dal mittente (autenticità)

✅ Vantaggi delle firme digitali

- **Autenticità**: Conferma l'identità del firmatario.
- **Integrità**: Garantisce che il contenuto non sia stato alterato dopo la firma.
- **Non ripudio**: Il firmatario non può negare di aver firmato il documento, poiché solo lui possiede la chiave privata necessaria.

Le firme digitali sono riconosciute legalmente in molti Paesi (compresa l'Italia) e sono regolate da normative come eIDAS a livello europeo.