Tecniche Crittografiche

Francesco Pugliese, PhD

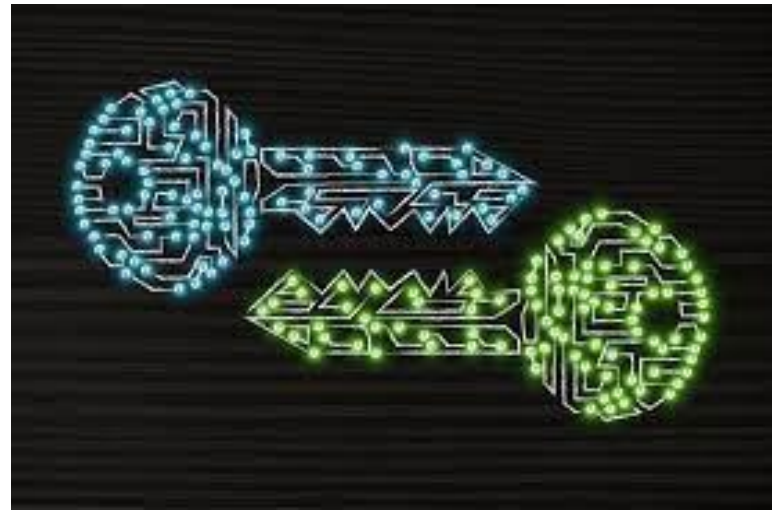
neural1977@gmail.com

Crittografia

- La **Crittografia** è una tecnica usata da moltissime aziende e realtà e ha origine già nell'antichità.

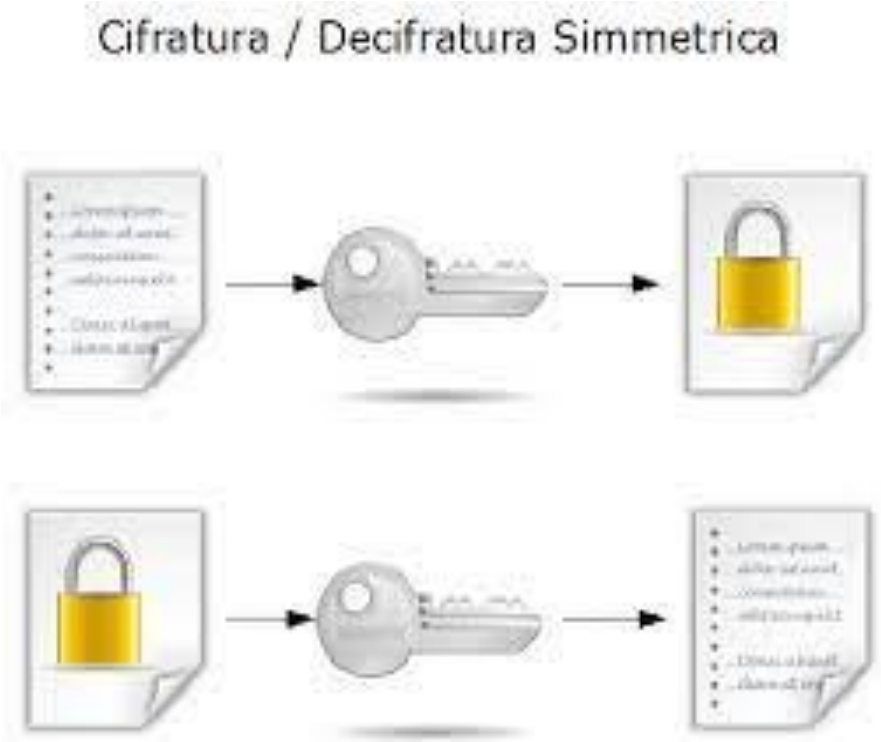
- Si è sempre rivelata, infatti, uno strumento fondamentale per **proteggere i dati** e veicolare informazioni tra più parti in maniera sicura.

- Ciò che è importante sapere, però, è che non esiste un'unica categoria di cifratura: i principali tipi di crittografia sono infatti ben tre, ognuno con **caratteristiche e vantaggi differenti**.



Tipi di Crittografia

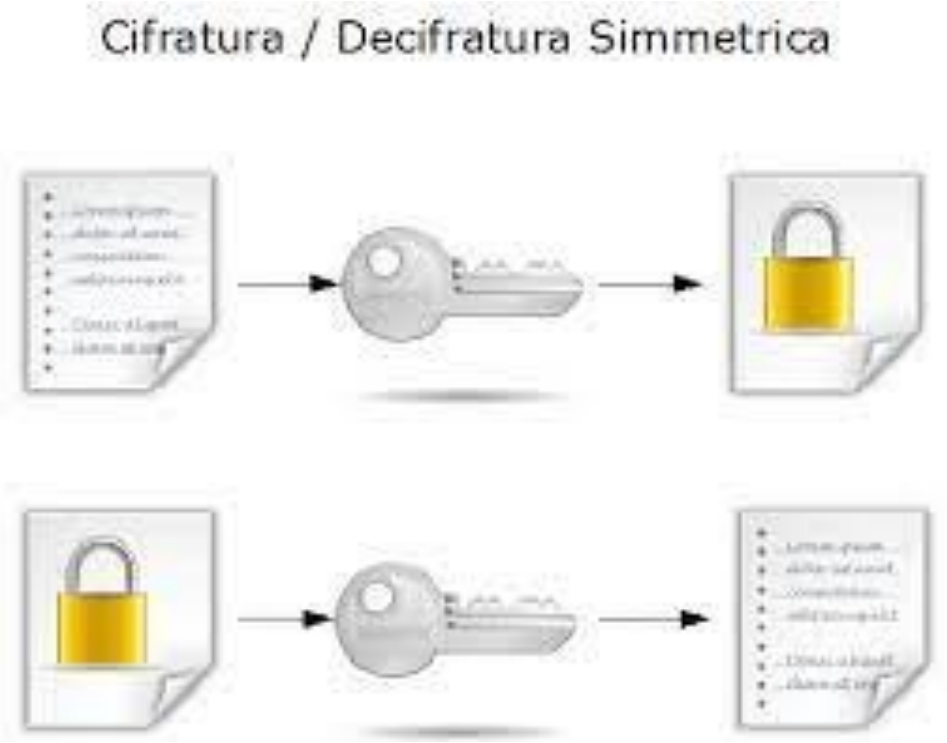
- ✓ I tipi di crittografia principali sono tre:
  - **crittografia simmetrica**
  - **crittografia asimmetrica**
  - **crittografia quantistica**



- ✓ La **crittografia simmetrica** si serve di un'unica chiave, per questo viene anche chiamata crittografia a chiave privata o a chiave segreta, con cui si possono cifrare le informazioni e poi decodificarle.

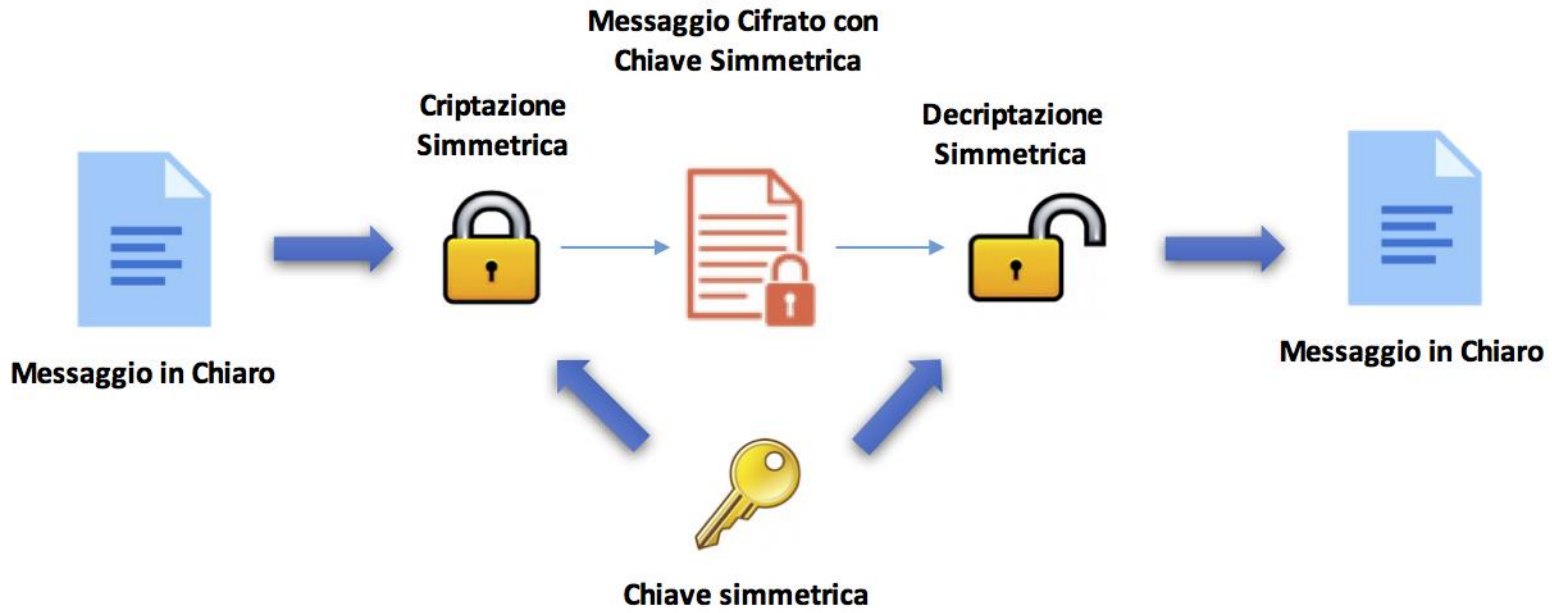
Crittografia a chiave simmetrica

- La **chiave di crittazione** è quindi la stessa della decrittazione e per decifrare i dati è necessario che tutti gli utenti coinvolti si scambino tale chiave e ne siano in possesso.
- La **cifratura simmetrica è rapida** e facile da usare rispetto ad altri metodi crittografici e risulta essere particolarmente adatta per singoli utenti e sistemi chiusi.
- Non è l'alternativa più evoluta e moderna tra le opzioni disponibili, ma presenta comunque dei benefici importanti.



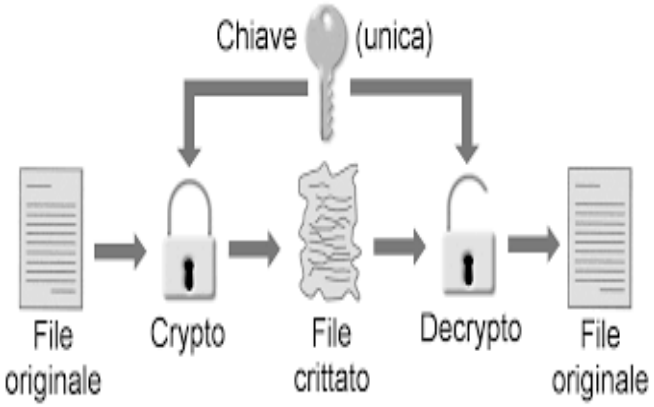
Crittografia a chiave simmetrica

- ✓ E' una tecnica veloce e basata su chiavi corte: le chiavi hanno infatti una lunghezza impostata a **128 o 256 bit**, richiedendo una **modesta potenza di calcolo** e rendendo il sistema agile e veloce.
- ✓ Inoltre non richiede un'infrastruttura apposita per garantire sicurezza, come invece succede con la crittografia asimmetrica che prevede l'implementazione di un'infrastruttura a chiave pubblica.



Crittografia a chiave simmetrica

- ✓ Lo **svantaggio** è che questo tipo di cifratura funziona grazie a un'unica chiave di lettura e **non fa distinzione** tra chiave privata e chiave pubblica.
- ✓ La chiave è solo privata e per far sì che entrambe le parti di una comunicazione ne entrino in possesso, è necessario creare un momento di scambio: che lo scambio avvenga in maniera fisica o virtuale, il **rischio è molto alto**, e c'è la concreta possibilità che la chiave venga intercettata da un malintenzionato.
- ✓ Il **livello di sicurezza** è quindi minore rispetto alla crittografia asimmetrica, perché una volta scoperta la chiave è possibile accedere ai messaggi senza difficoltà.

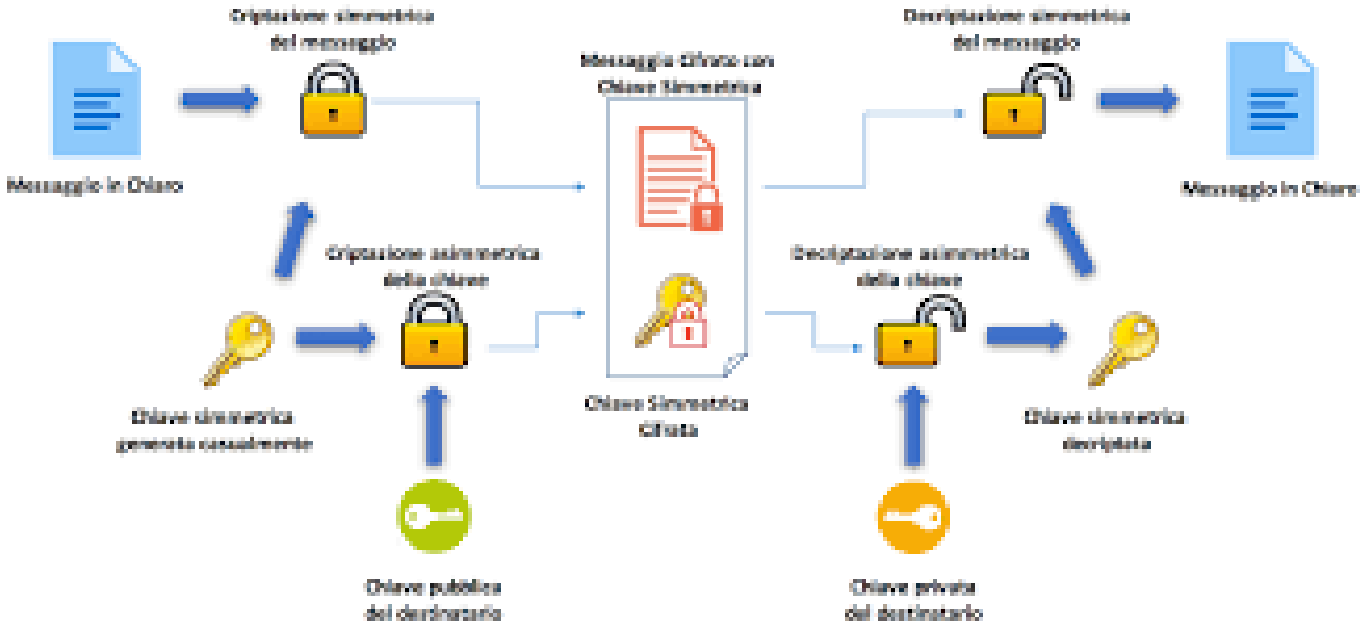


Crittografia asimmetrica

- La **crittografia asimmetrica** si distingue per essere un tipo di cifratura che non si basa su un'unica chiave di codifica, bensì su due chiavi distinte ma correlate.
- Gli **algoritmi** utilizzano infatti una **chiave pubblica** e una **chiave privata**: quella pubblica è condivisa tra mittente e destinatario e quella privata è individuale. La prima è accessibile a chiunque voglia scambiare informazioni con l'entità proprietaria, la seconda è segreta e conosciuta solo dal legittimo proprietario.

Crittografia asimmetrica

- ✓ Per poter **decifrare** il **messaggio** è necessario essere in possesso di entrambe le **chiavi** e il livello di **sicurezza** garantito è quindi decisamente maggiore rispetto alla **crittografia simmetrica**.
- ✓ Nell'ipotesi che qualcuno riesca a intercettare la **chiave pubblica**, infatti, non avrebbe comunque accesso a quella privata e non potrebbe, così, accedere alle **informazioni**.



Crittografia asimmetrica

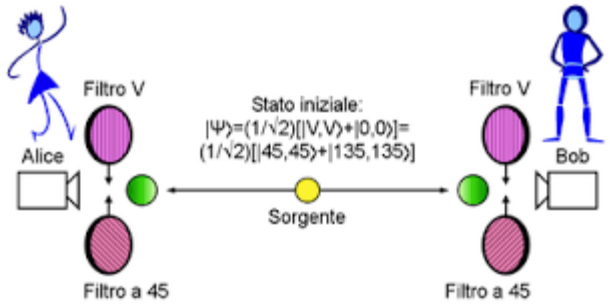
- Rispetto alla **crittografia simmetrica** che usa un'unica chiave, la **crittografia asimmetrica** si serve di due chiavi di codifica: la **chiave pubblica** e la **chiave privata**.
- Il primo evidente **vantaggio** di questo tipo di **cifratura** è, come già anticipato, la **maggiore sicurezza** che può **assicurare**.
- Basandosi su due **chiavi distinte**, infatti, riesce a **proteggere** i dati anche nel caso in cui un **utente** venga a conoscenza di una delle **chiavi di lettura**, dato che per **accedere** alle informazioni avrebbe comunque bisogno anche dell'altra chiave.

Crittografia asimmetrica

- ✓ Inoltre la **crittografia asimmetrica** riesce più facilmente a garantire l'integrità e **autenticità** dei dati e il non ripudio da parte del **mittente**.
- ✓ Parlando invece di **svantaggi**, è importante sottolineare che le due **chiavi** sono correlate tramite determinati **schemi matematici**: le chiavi vengono generate grazie a dei **calcoli predefiniti** che potrebbero essere sfruttati dagli **hacker** per forzare la **cifratura**.
- ✓ Per ovviare a questa **eventualità**, le chiavi della **crittografia asimmetrica** sono quindi molto **lunghe** e **complesse**, rendendo più sicuro il sistema ma allo stesso tempo **rallentando il funzionamento** della crittografia nel suo insieme.
- ✓ Infine non c'è alcuna **garanzia** che una **chiave** appartenga realmente alla **persona designata** e non è raro finire nel mirino di **attacchi "man in the middle e spoofing"**.

Crittografia quantistica

- La **crittografia quantistica** è un approccio alla crittografia che, nella fase dello scambio della chiave di decodifica, si serve dei **principi** della **meccanica quantistica**.
- In questo **modo** si evita che la **chiave** possa essere **intercettata** senza che le parti coinvolte se ne accorgano
- Entrando nel dettaglio, la **definizione** esatta è **distribuzione quantistica** di chiavi, cioè una trasmissione di dati in grado di vantare una condizione di **segretezza perfetta** dal punto di vista matematico.
- L'obiettivo è infatti creare una sorta di **cifrario perfetto** che non prevede un momento di scambio su un canale necessariamente sicuro.



Bibliografia

https://www.it-impresa.it/blog/tipi-di-crittografia/