Tecniche Crittografiche

Francesco Pugliese, PhD

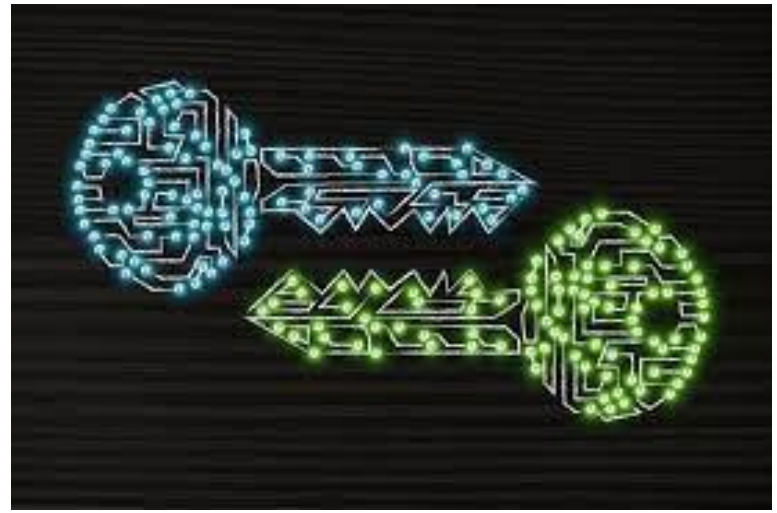
neural1977@gmail.com

Crittografia

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

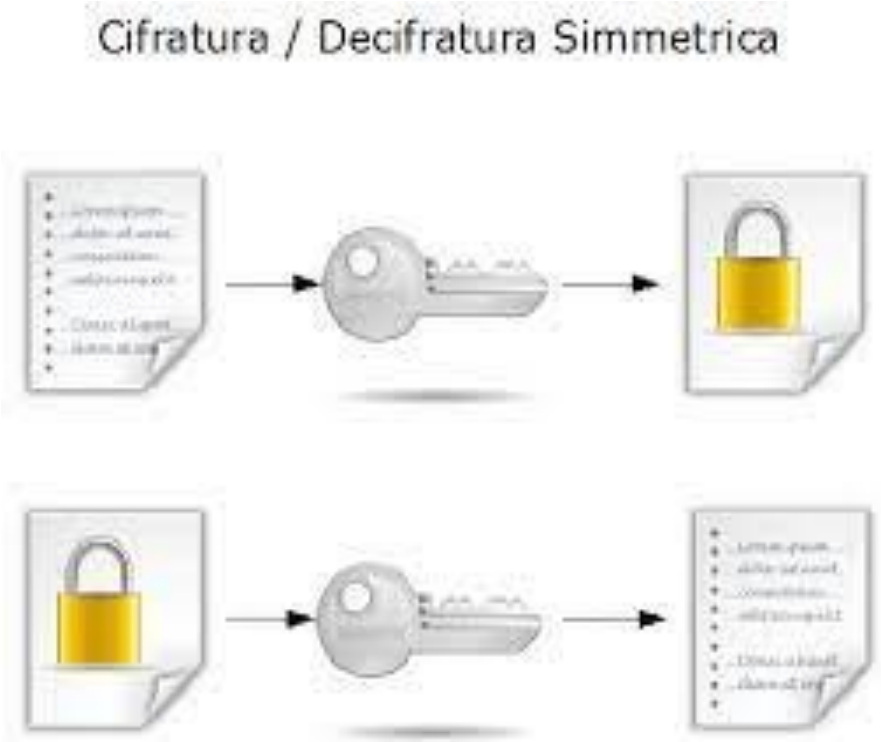
- Si è sempre rivelata, infatti, uno strumento fondamentale per **proteggere i dati** e veicolare informazioni tra più parti in maniera sicura.

- 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

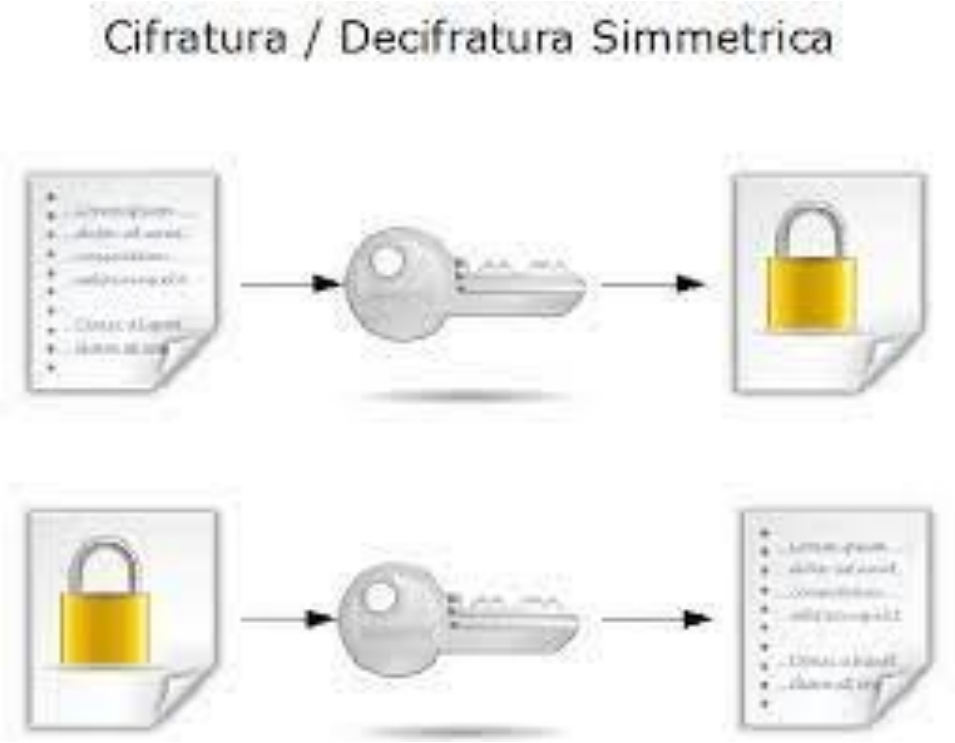
- ✓ I tipi di crittografia principali sono tre:
  - **crittografia simmetrica**
  - **crittografia asimmetrica**
  - **crittografia quantistica**



- ✓ 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.

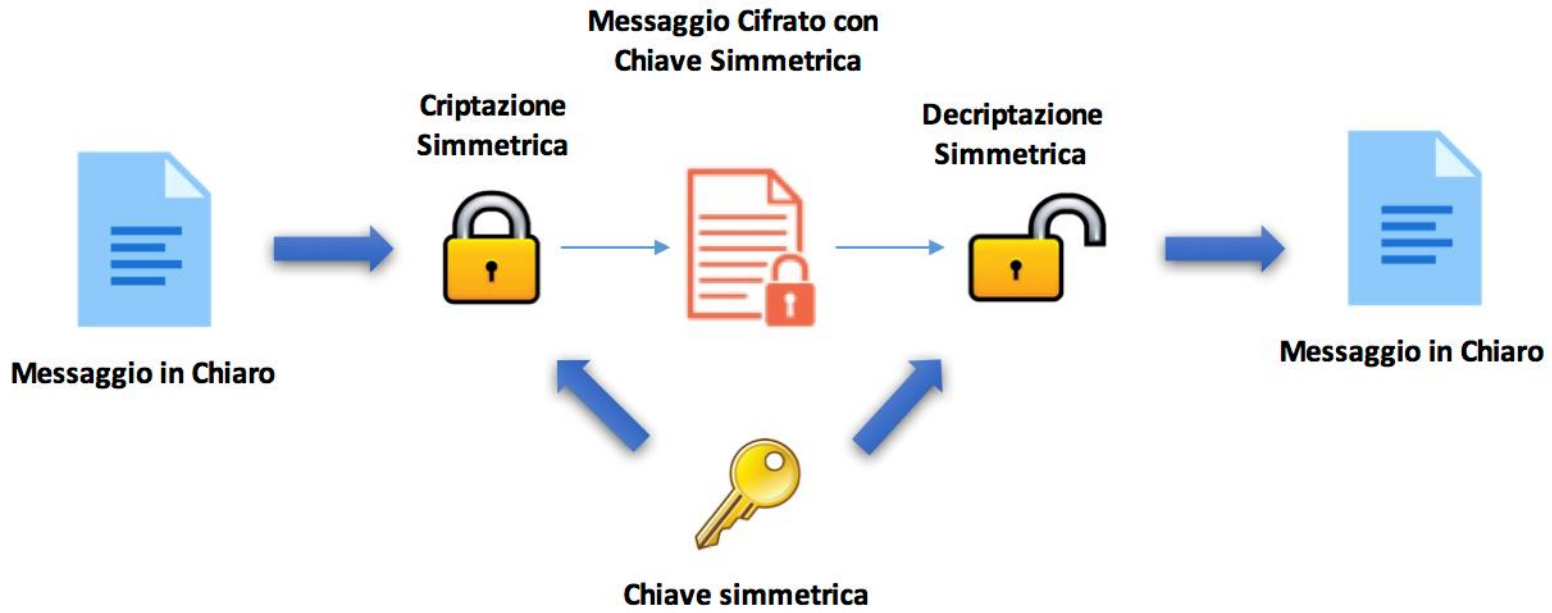
Crittografia a chiave simmetrica

- 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.



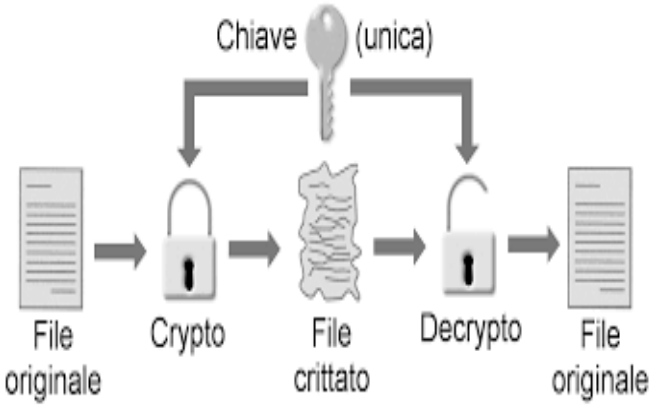
Crittografia a chiave simmetrica

- ✓ 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.

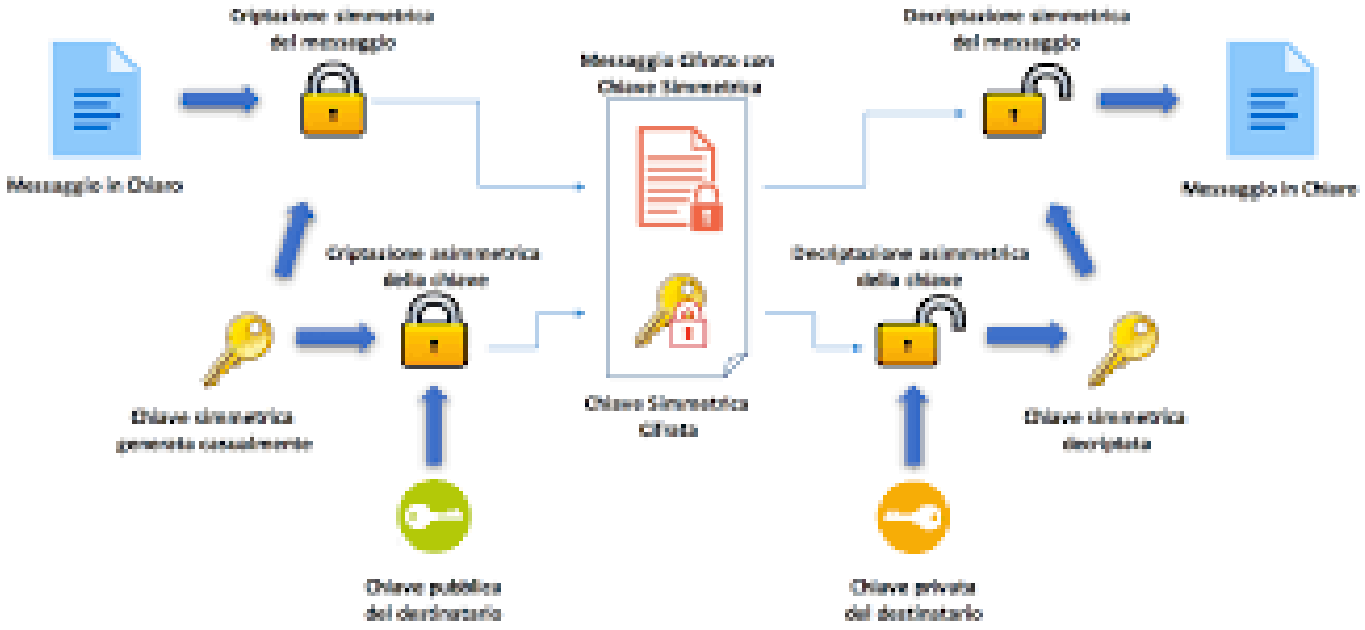


Crittografia asimmetrica

- 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

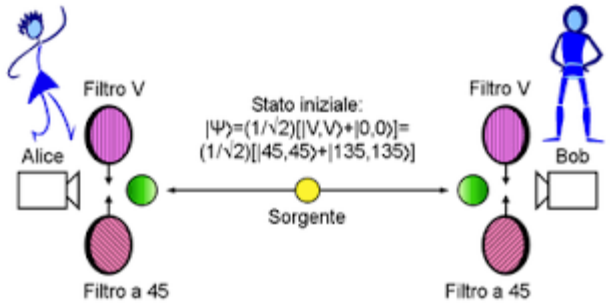
- Rispetto alla **crittografia simmetrica** che usa un'unica chiave, la **crittografia asimmetrica** si serve di due chiavi di codifica: la **chiave pubblica** e la **chiave privata**.
- Il primo evidente **vantaggio** di questo tipo di **cifratura** è, come già anticipato, la **maggiore sicurezza** 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"**.

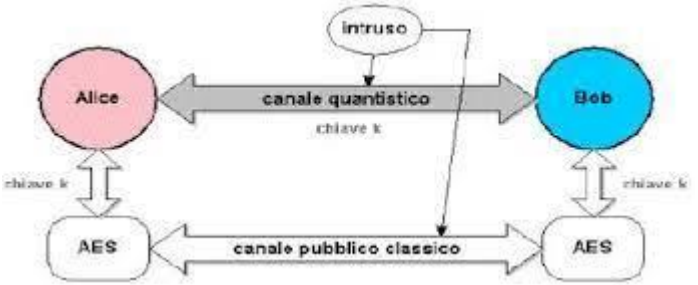
Crittografia quantistica

- 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**.



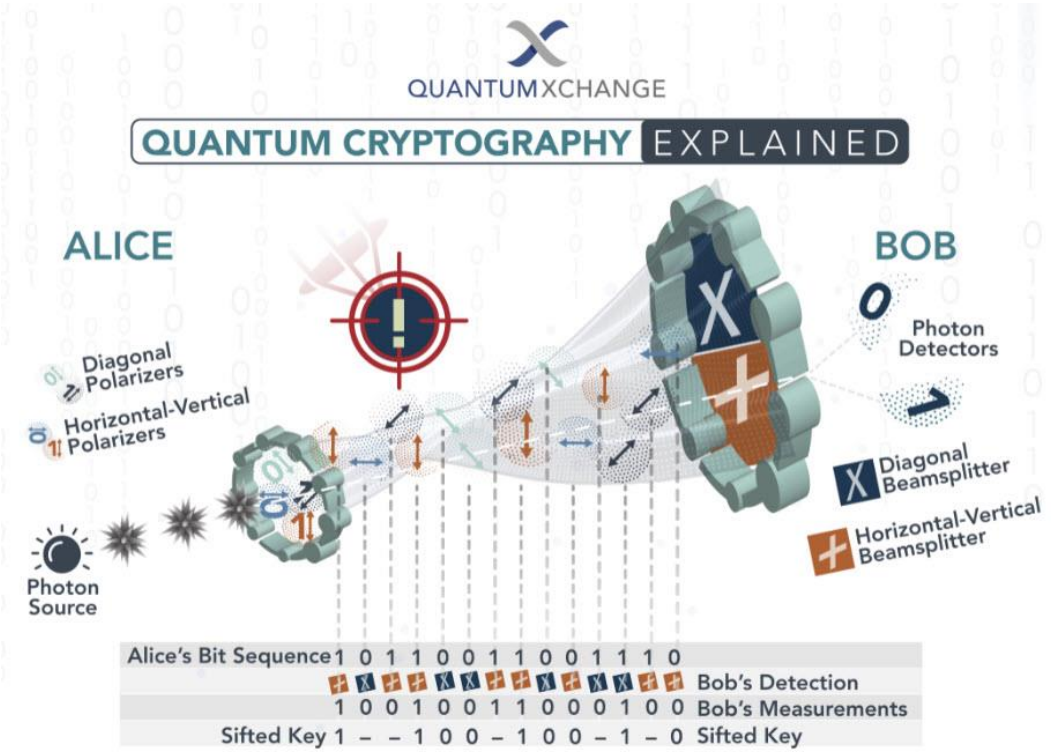
Crittografia quantistica

- ✓ Conviene, quindi, affidarsi a questa tecnica così **innovativa**?
- ✓ È **importante** precisare che la **crittografia quantistica** è sì una tecnologia ancora in via di **sviluppo**, ma che può già essere applicata – nonostante le **limitazioni** – portando dei sostanziali vantaggi.
- ✓ Con questo tipo di **cifratura**, infatti, si prevede di **rivoluzionare** radicalmente il modo in cui le informazioni verranno **comunicate**, sfruttando le leggi della **fisica** piuttosto che gli attuali **algoritmi matematici**.
- ✓ Questa **tecnica promette** quindi di essere **impenetrabile** e dovrebbe **distribuire** le informazioni garantendo un **livello di sicurezza** senza pari, codificandole su **stati quantistici** della luce.



Crittografia quantistica

- ✓ Gli **strumenti** e i **dispositivi** utilizzati, inoltre, sono in costante miglioramento ed evoluzione e ci si aspetta che in futuro questa tecnologia diventi di uso comune in molte realtà.
- ✓ Lo **svantaggio** è che la **crittografia quantistica**, oggi, è ancora una **tecnica** nuova e richiede **infrastrutture** particolari e **costose** da costruire. Inoltre le distanze su cui è stata eseguita e **testata** sono ancora limitate con **tassi** di errore significativi.



Tipi di Crittografia

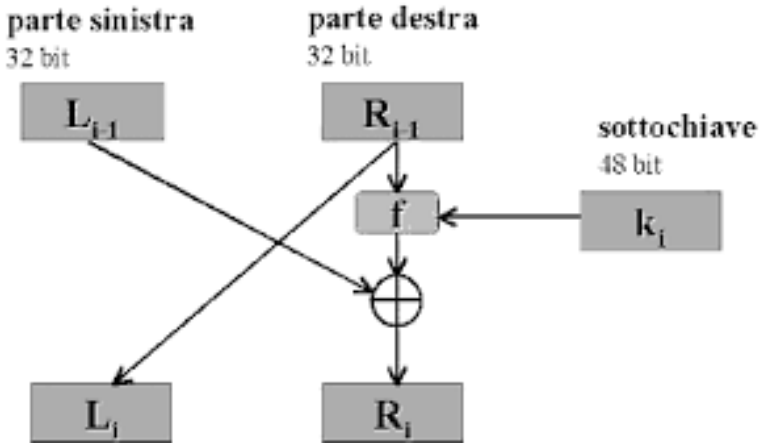
- ✓ Ora che **abbiamo** esaminato i diversi **tipi di crittografia**, come si può capire qual è l'opzione migliore?
- ✓ La via più **opportuna** per procedere è **comprendere** a fondo quali sono le proprie **esigenze** e quali obiettivi si vuol raggiungere, **individuando** così l'alternativa più in **linea** con la propria **realtà**.
- ✓ Se si **necessita** di una **tecnica di cifratura** di base **semplice** e si ha la certezza di poter **scambiare la chiave** di codifica in maniera sicura, allora la **crittografia simmetrica** può essere la soluzione giusta. Soprattutto se non si dispone di **infrastrutture** e mezzi particolarmente **evoluti** e potenti.
- ✓ La **crittografia asimmetrica**, invece, è più indicata per chi aspira a un livello di **sicurezza elevato** e sa come gestire chiavi lunghe e complesse, affidandosi a strumenti di calcolo adeguati.

Tipi di Crittografia e Algoritmi

- ✓ Infine la **crittografia quantistica** rappresenta la tecnologia del futuro, per ora accessibile solo ad aziende **mondiali** come **IBM** e **Google**, ma che presto diventerà **protagonista** anche di realtà più piccole e modeste.
- ✓ I principali algoritmi usati nella **crittografia simmetrica** sono: **DES** (Data Encryption Standard), **3DES** (Triple DES) e **AES** (Advanced Encryption Standard).
- ✓ I più diffusi e conosciuti **algoritmi asimmetrici** sono: **RSA**, **Diffie-Hellman**, **El-Gamal**. In questo schema crittografico si usano due **chiavi distinte** per la **codifica** e la **decodifica**. La prima viene utilizzata per codificare il messaggio **M**, la seconda per **decodificarlo** una volta che questo è giunto a **destinazione**.
- ✓ Gli algoritmi di **crittografia quantistica**: **CRYSTALS-Kyber**, **CRYSTALS-Dilithium**, **FALCON** e **SPHINCS+**

Crittografia Simmetrica: Algoritmo DES

- La sigla **DES** sta per **Data Encryption Standard**, ed è un sistema di **cifratura** adottato come **standard** dal governo degli Stati Uniti d'America nel **1976**.
- L'algoritmo su cui si basa è il **DEA (Data Encryption Algorithm)**, evoluzione di un altro algoritmo di cifratura, il Lucifer, sviluppato presso i laboratori della IBM da Horst Feistel (ideatore della rete omonima).
- Il DEA, sostanzialmente, è proprio una **rete di Feistel** ed il suo funzionamento può essere studiato utilizzando il solito approccio, ovvero partendo dai blocchi più esterni fino ad arrivare a quelli più interni.

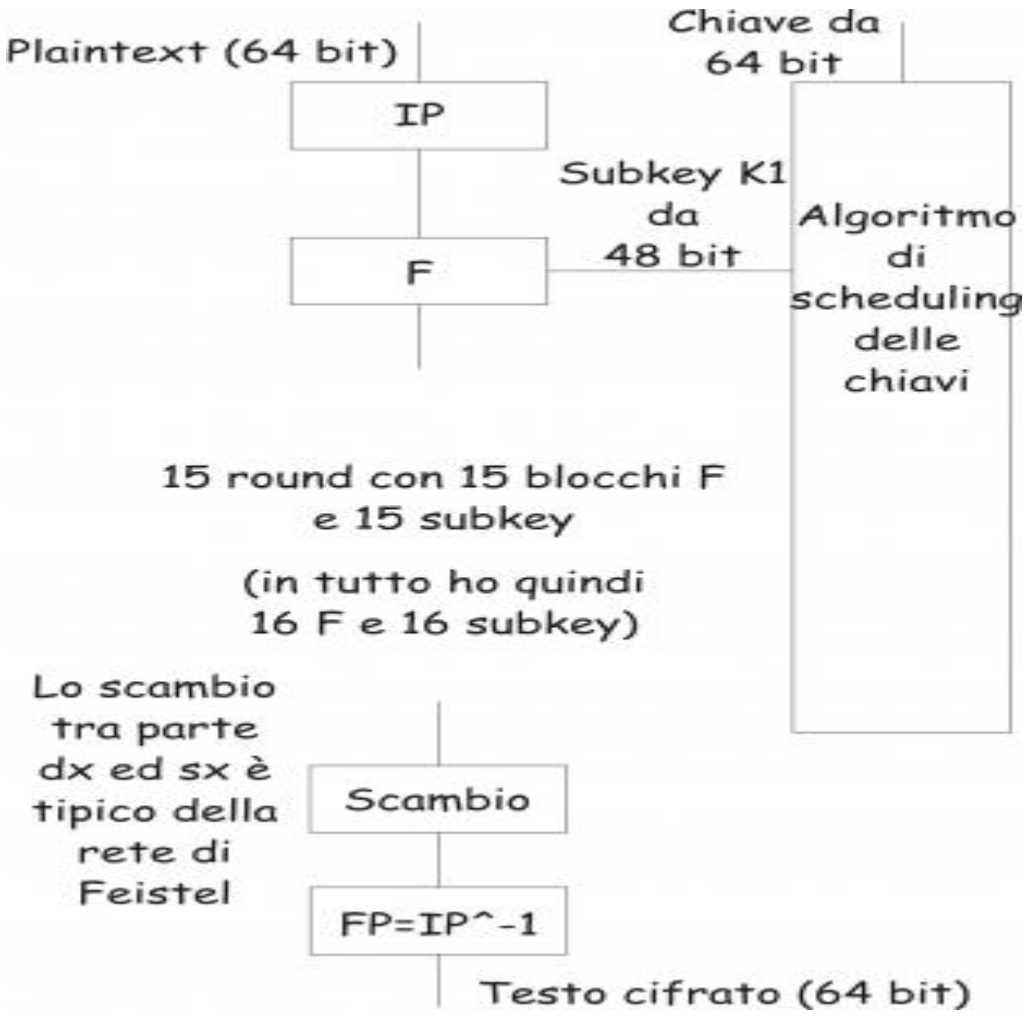


Crittografia Simmetrica: Algoritmo DES

- In **crittologia**, un **cifrario di Feistel** è un algoritmo di **cifratura** a blocchi con una particolare **struttura sviluppata** dal crittologo **dell'IBM Horst Feistel**, da cui ha preso il nome di rete di **Feistel**; moltissimi algoritmi di **cifratura a blocchi** la utilizzano, incluso il **Data Encryption Standard**.
- Il **DEA** si avvale di un **cifrario a blocchi**, il quale riceve in ingresso una stringa di **testo** di **lunghezza fissa** (**plaintext** – testo in chiaro) e la **trasforma**, mediante una serie di **operazioni complesse**, in un'altra stringa della stessa lunghezza, però cifrata.
- Nel caso del **DES** la dimensione di ogni blocco del **cifrario** è **pari** a **64 bit**. Nel caso in cui il **testo** in **chiaro** da cifrare dovesse essere superiore ai **64 bit**, esso verrà suddiviso in blocchi da **64 bit** ciascuno (aggiungendo eventualmente del **padding**). Ogni blocco verrà quindi dato in pasto ad un **cifrario** e gli output così generati verranno **combinati tra di loro**.

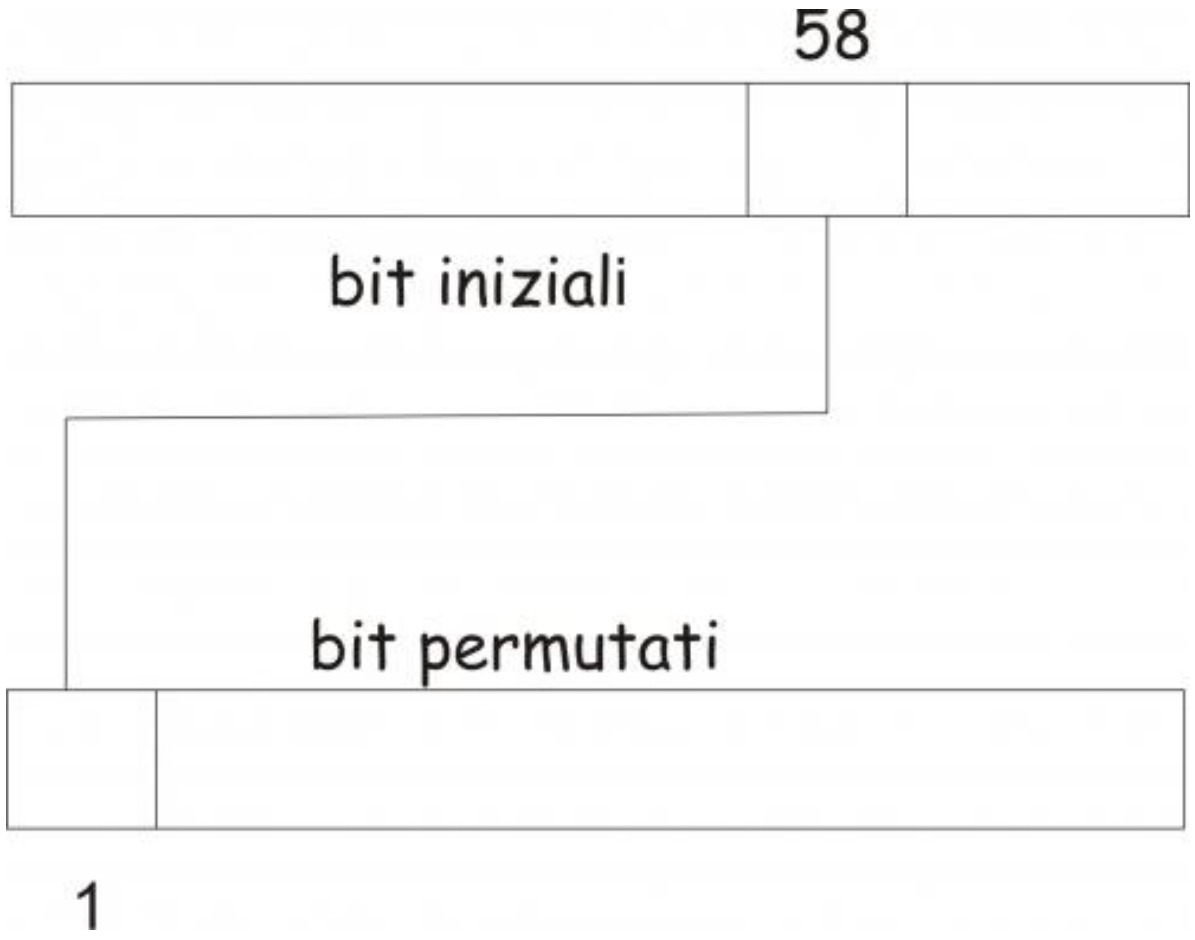
Crittografia Simmetrica: Algoritmo DES

- E' bene notare che **IP** (Initial Permutation) ed **FP** (Final Permutation, altrimenti conosciuta come **IP^-1**) non hanno alcun ruolo nell'ambito della **cifratura** vera e propria, ma sono state aggiunte per **facilitare** il **caricamento** dei vari **blocchi** di bit sui dispositivi **hardware** tipici degli **anni '70**.



Crittografia Simmetrica: Algoritmo DES

- ✓ Ciò significa che il **58-esimo bit** della sequenza di input (derivante dal testo in chiaro) verrà spostato in prima posizione della **sequenza** di **output**, il **50-esimo bit** della sequenza di input verrà **spostato** in seconda posizione della **sequenza** di output e così via (seguendo sempre delle **regole prefissate**). Alla fine **dell'IP** avremo la seguente **situazione** (rappresentata in forma matriciale per semplicità, anche se in realtà è un **vettore**)



Crittografia Simmetrica: Algoritmo DES

- ✓ Che, come si può notare, è una matrice **8×8** (contiene **64** elementi, ovvero i **64 bit** di input permutati).

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

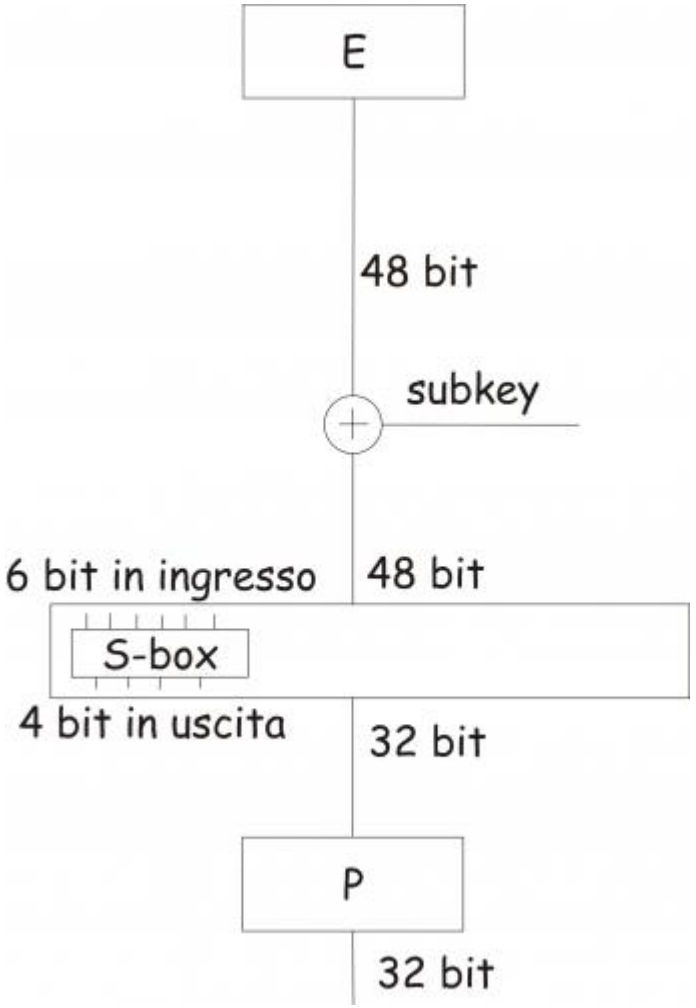
Crittografia Simmetrica: Algoritmo DES

- **Ora** che abbiamo visto cosa succede all'interno del **blocco** identificato dalla sigla **IP**, è facile andare a **descrivere** cosa succede in **FP**. Tale **blocco** viene anche identificato come **IP^-1** poichè non fa altro che invertire le operazioni svolte da **IP**. Ecco allora che la matrice **8×8** relativa all'output prodotto dal **blocco** in questione è la seguente.

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Crittografia Simmetrica: Algoritmo DES

- Osserviamo tale **matrice**. Il bit pari a **1**, nella **matrice** risultate associata **all'IP**, si trovava in posizione **40**. Al termine della FP il **bit 40** si troverà in posizione 1. Discorso **analogo** vale per il **bit 2**, che nella matrice relativa **all'IP** si trovava in **posizione 8**, quindi nella matrice prodotta dalla **FP l'8** si troverà in **posizione 2** (e così via).
- Vediamo adesso cosa succede all'interno del **blocco F** (ovvero la **funzione di Feistel**). Essa, sostanzialmente, opera su mezzo **blocco** per volta (formato da **32 bit**) e consiste in **4 passi**, illustrati di seguito.



Bibliografia

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

https://nazarenolatella.myblog.it/2009/01/17/des-come-funziona-e-perche-e-vulnerabile/