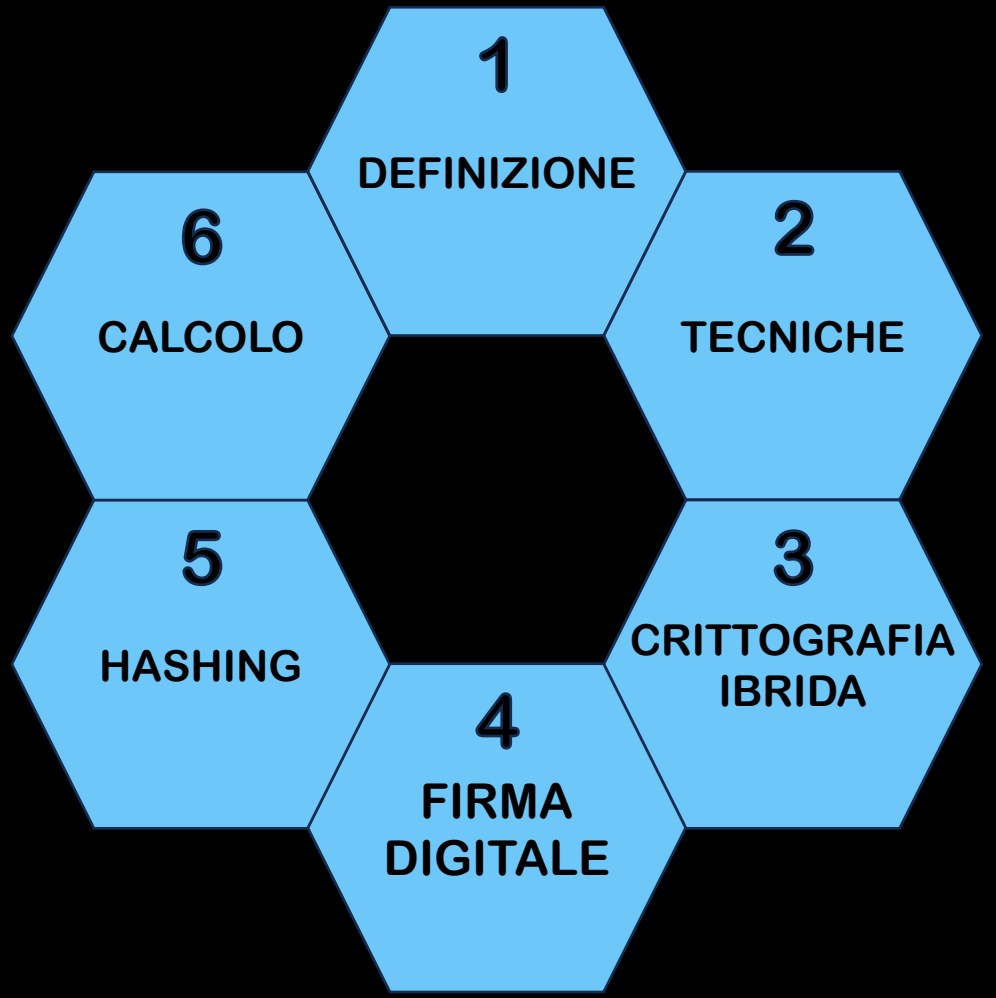
CRITTOGRAFIA

INDICE


1
DEFINIZIONE
2
TECNICHE
3
CRITTOGRAFIA IBRIDA
4
FIRMA DIGITALE
5
HASHING
6
CALCOLO

DEFINIZIONE

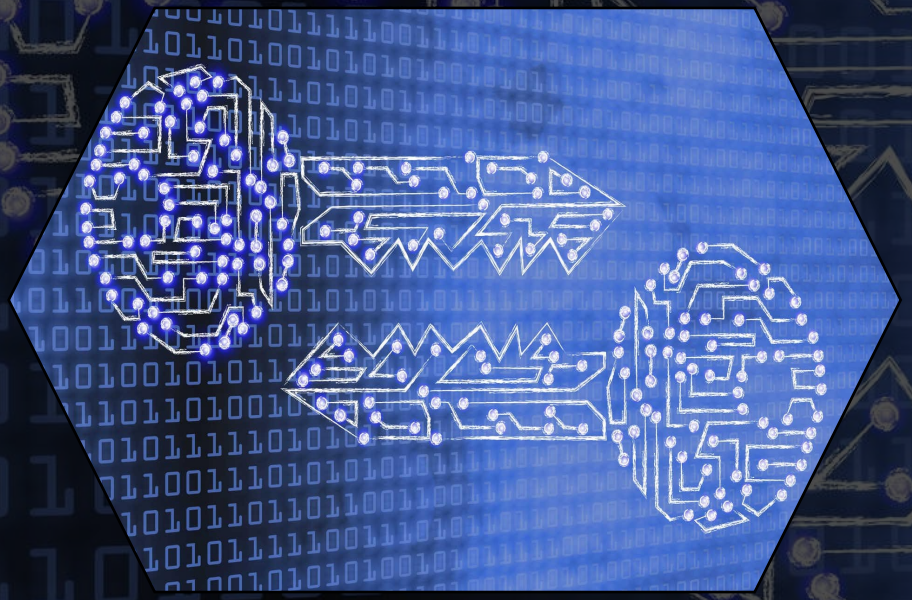
È la pratica di proteggere le informazioni attraverso l'uso di algoritmi codificati, hash e firme.
Le informazioni possono essere a riposo, in transito o in uso.
La crittografia ha 4 obiettivi:

- AUTENTICITA'
- RISERVATEZZA
- INTEGRITA'
- NON RIPUDIO

TECNICHE

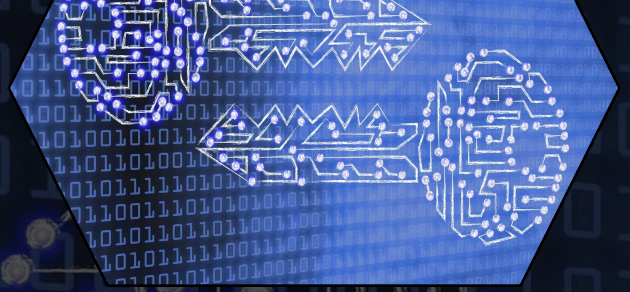
CHIAVE ASIMMETRICA

CHIAVE SIMMETRICA



CHIAVE ASIMMETRICA

È composta da un ampio set di algoritmi che si basano su problemi matematici da utilizzare in una direzione, ma che non possono essere invertiti.
Utilizza una chiave, quella pubblica, per crittografare i dati e una chiave diversa, ma matematicamente correlata, quella privata, per decrittografarli.



CHIAVE SIMMETRICA

Utilizza le stesse chiavi sia per la crittografia del testo semplice che per la decrittografia del testo criptato. La crittografia a chiave simmetrica richiede che tutti i destinatari dei messaggi abbiano accesso a una chiave condivisa.

CRITTOGRAFIA IBRIDA

In questo caso verranno utilizzate entrambe le tecniche di crittografia. Con quella simmetrica verranno cifrati i dati di scambio, mentre quella asimmetrica servirà per la condivisione della chiave simmetrica.
Questo permette una soluzione end-to-end pratica per la privacy dei dati.

FIRMA DIGITALE

È un tipo di crittografia a chiave pubblica che assicura le proprietà principali.
Il processo di firma è una crittografia del file tramite una chiave privata, che il firmatario utilizza per produrre una "firma" su un documento digitale.
La firma è unica e può essere allegata al e verificata con la chiave pubblica del firmatario.

HASHING

È uno strumento che trasforma i dati arbitrari in un'impronta a lunghezza fissa.
È creato in modo che sia difficile trovare due input diversi con la stessa impronta.
Le funzioni hash non hanno una chiave, pertanto chiunque può calcolare l'hash di un input.

CALCOLO CRITTOGRAFICO

Il termine si riferisce a un'ampia gamma di tecnologie, tra cui il calcolo multilaterale, la crittografia omomorfica e la crittografia ricercabile. Anche se differiscono per alcuni dettagli, queste tecnologie proteggono i dati a livello crittografico in modo tale da permetterti di realizzare operazioni di calcolo sui dati protetti preservando al contempo la loro riservatezza.