

CRITTOGRAFIA

HTTPS, CIFRARI E APPLICAZIONI DELLA CRITTOGRAFIA

Fonti:

- *Treccani*
- *Wikipedia - crittografia asimmetrica*
- *Wikipedia - NFT*
- *Fastweb Plus*
- *IBM - blockchain*
- *Kaspersky - criptovalute*

CRITTOGRAFIA

DEFINIZIONE

La crittografia è la disciplina che studia le **tecniche per trasformare un messaggio, detto testo in chiaro, in un altro messaggio, detto testo cifrato, che risulta incomprensibile** a chiunque non conosca tutti i dettagli della tecnica usata per la trasformazione. Solo il legittimo destinatario del messaggio è in grado di effettuare l'operazione inversa e di ottenere così dal testo cifrato il testo in chiaro originale. La trasformazione del testo in chiaro in testo cifrato è detta **cifratura**, mentre la ricostruzione del testo in chiaro a partire dal testo cifrato è detta **decifratura**. L'insieme delle operazioni che devono essere effettuate durante la cifratura e la corrispondente decifratura prende il nome di codice crittografico, o **cifrario**.

Curiosità

Crittografia end-to-end

HTTP vs HTTPS

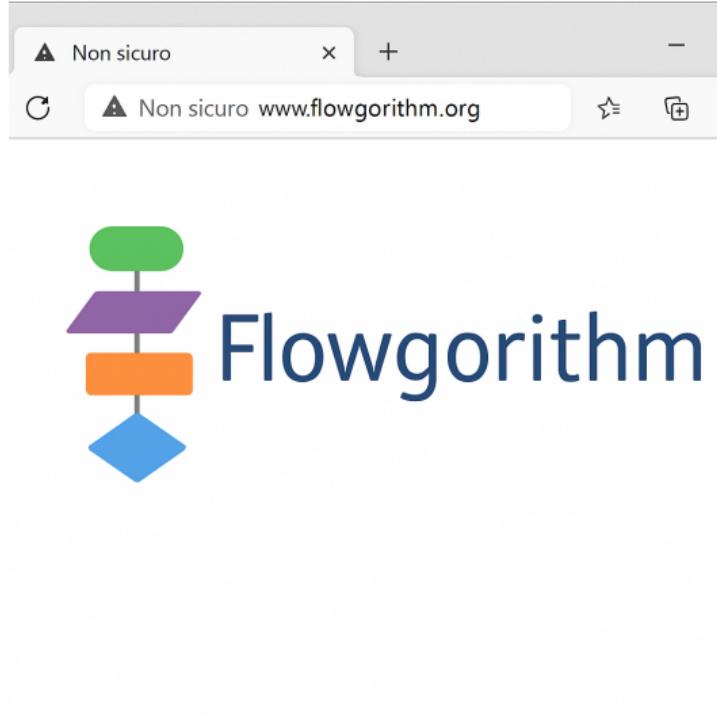


Figura 1: creata con ChatGPT



Figura 2: creata con [Canva](#)

CIFRARI SIMMETRICI

DEFINIZIONE

Il cifrario di Cesare è uno dei più antichi algoritmi crittografici di cui si abbia traccia storica. È un cifrario a **sostituzione monoalfabetica**, in cui ogni lettera del testo in chiaro è sostituita, nel testo cifrato, dalla lettera che si trova un certo numero di posizioni dopo nell'alfabeto. (nel caso del cifrario di Cesare, il numero di posizioni è 3). Questi tipi di cifrari sono detti anche cifrari a sostituzione o cifrari a scorrimento a causa del loro modo di operare: la sostituzione avviene lettera per lettera, scorrendo il testo dall'inizio alla fine.

Esempio

[Cifrario di Cesare](#)

CIFRARIO DI VERNAM (OTP)

DEFINIZIONE

Esempio di cifrario a **chiave non riutilizzabile**, in inglese **One Time Pad** abbreviato in **OTP**. Il cifrario di Vernam è perfetto, nel senso che il testo in chiaro e il testo cifrato sono del tutto indipendenti, la conoscenza dell'uno non dà alcuna informazione sull'altro. È quindi del tutto al sicuro dagli attacchi della crittanalisi statistica. **La chiave utilizzata per cifrare il messaggio deve essere lunga quanto il messaggio stesso** e non deve essere mai riutilizzata, per questo viene chiamata One Time Password. Per ottenere il testo cifrato è sufficiente eseguire un'operazione di **XOR** tra il testo in chiaro e la chiave.

Esempio

Cifrario OTP

CIFRARIO ASIMMETRICO

CIFRARIO ASIMMETRICO

DEFINIZIONE

La **crittografia asimmetrica** è un tipo di crittografia nel quale ad ogni attore coinvolto nella comunicazione è associata una **coppia di chiavi**:

- La **chiave pubblica**, che deve essere distribuita;
- La **chiave privata**, personale e segreta.

La crittografia asimmetrica evita il problema classico della crittografia simmetrica connesso alla necessità di uno scambio in modo sicuro dell'unica chiave utile alla cifratura/decifratura. Il meccanismo della crittografia asimmetrica si basa invece sulle seguenti assunzioni:

- La chiave privata non è ricavabile dalla chiave pubblica;
- Se con una delle due chiavi si cifra un messaggio, allora quest'ultimo sarà decifrato solo con l'altra.

Esempio

Cifrario RSA

CRITTOGRAFIA: VIDEO



Figura 3: Fonte [Cos'è la crittografia, come funziona e perché serve a proteggere i dati e la confidenzialità \(Geopop\)](#)

APPLICAZIONI BASATE SULLA CRITTOGRAFIA

BLOCKCHAIN

DEFINIZIONE

La **blockchain** funziona come un **databasse distribuito decentralizzato**, con dati archiviati su più computer, rendendolo resistente alle manomissioni. Le transazioni vengono convalidate attraverso un **meccanismo di consenso**, che garantisce l'accordo in tutta la rete. Nella tecnologia blockchain, **ogni transazione è raggruppata in blocchi**, che vengono poi collegati tra loro, formando una catena sicura e trasparente.

Video di approfondimento

[Te lo spiego - Che cos'è e come funziona una blockchain](#)

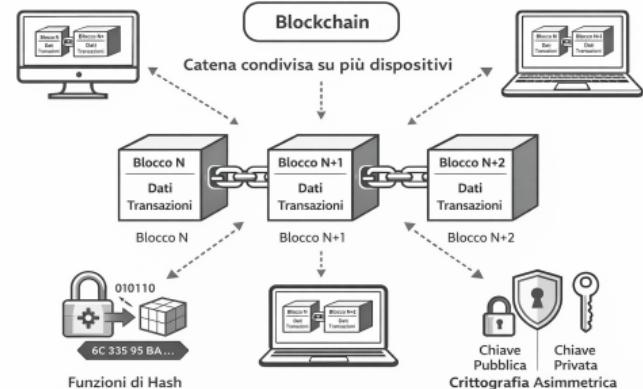


Figura 4: creata con [ChatGPT](#)

Funzione di Hash

[Wikipedia](#)

CRİPTOVALUTE

DEFINIZIONE

La **criptovaluta** è una forma di valuta digitale che **usa la crittografia per proteggere le transazioni**. Anziché avere un'autorità emittente o regolatrice centrale, le criptovalute **utilizzano una blockchain pubblica** per registrare le transazioni ed emettere nuove unità. Le unità di criptovaluta vengono **create tramite un processo chiamato mining**, che fa leva sull'elaborazione informatica per risolvere complicati problemi matematici da cui vengono generate le monete.

Video di approfondimento

Te lo spiego - Che cosa sono e come funzionano i Bitcoin

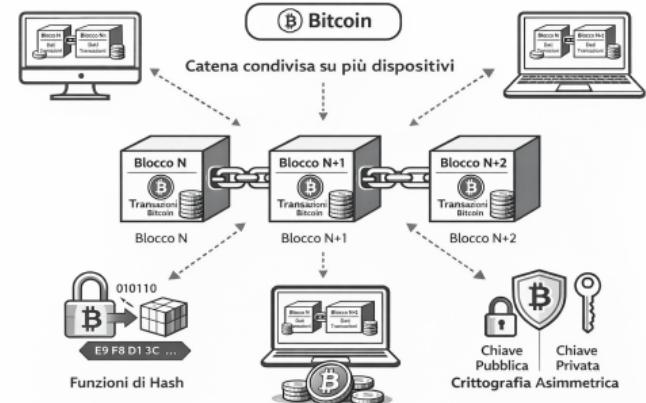


Figura 5: creata con ChatGPT

Prezzi delle criptovalute

Andamento delle principali criptovalute

Andamento dei principali Meme Coin

NON-FUNGIBLE TOKEN (NFT)

DEFINIZIONE

Un non-fungible token (**NFT**) è un tipo speciale di token, che rappresenta un **bene unico non fungibile**. A differenza di un bene fungibile (come una banconota), non può essere scambiato uno a uno con altri beni dello stesso tipo in modo indistinto. Gli NFT sono un tipo di bene non fungibile che possiede dati unici e possono essere **utilizzati per registrare e verificare la proprietà tramite la tecnologia della blockchain**.

Esempio di NFT
CryptoKitties



Figura 6: fonte Wikipedia

"Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world."

Curiosità

[Chi sono i Cypherpunks?](#)
[A Cypherpunk's Manifesto](#)