

# CRITTOGRAFIA

HTTPS, CIFRARI A CHIAVE SIMMETRICA

---

*Fonti:*

- *Treccani*
- *Wikipedia*

# 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

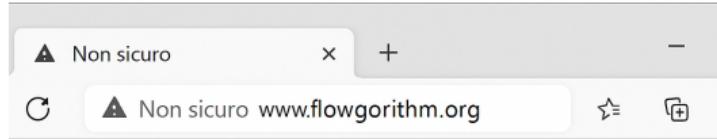


Figura 1: creata con ChatGPT



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