Crittografia

202303211233
Status:
Tags: Sistemi

Crittografia

La **Crittografia** è la pratica e lo studio delle tecniche di comunicazione per proteggere informazioni sensibili o segrete da letture non autorizzate da terzi.

La crittografia è composta da 3 principali caratteristiche:

- Autenticazione: Si riferisce alla capacità di verificare l'identità del mittente di un messaggio
- Affidabilità: Si riferisce alla capacità di garantire che il messaggio non sia stato modificato da terzi
- Segretezza: Si riferisce alla capacità di mantenere il contenuto di un messaggio privato e non accessibile a persone non autorizzate.

Gli Algoritmi di Cifratura nei quali le lettere vengono messe a corrispondenza si dividono in due tipi

- Alfabetismo Monoalfabetico: Nel quale si utilizza un solo alfabeto
- Alfabetismo Polialfabetico: Nel quale si utilizzano più alfabeti

Gli Algoritmi di Cifratura vengono anche identificati in base alla regola con la quale i caratteri vengono cifrati:

- Trasposizione: Relazione tra chiave di crittografia e testo cifrato più complessa possibile
- Sostituzione: Distribuzione delle informazioni sulla chiave in tutto il testo cifrato

Gli Algoritmi di Cifratura si identificano in base al numero di chiavi utilizzate

- Crittografia Simmetrica
- Crittografia Asimmetrica

Gli Algoritmi di Cifratura che utilizzano una o più chiavi seguono il Teorema di Kerckhoff, cioè che la sicurezza di un algoritmo è dato dalla chiave, non

dall'algoritmo

Altri principi di Crittografia sono:

- Confusione
- Diffusione

Esempi Un esempio di Algoritmo di Cifratura utilizzato durano il IX Secolo è il Cifrario a Campale Germanico, utilizzato dalle forze armate Tedesche durante la Prima Guerra Mondiale.

Un'altro esempio di Algoritmo di Cifratura è quello utilizzato dalla macchina Enigma, utilizzato dalle forze armate Tedesche durante la Seconda Guerra Mondiale

---

References