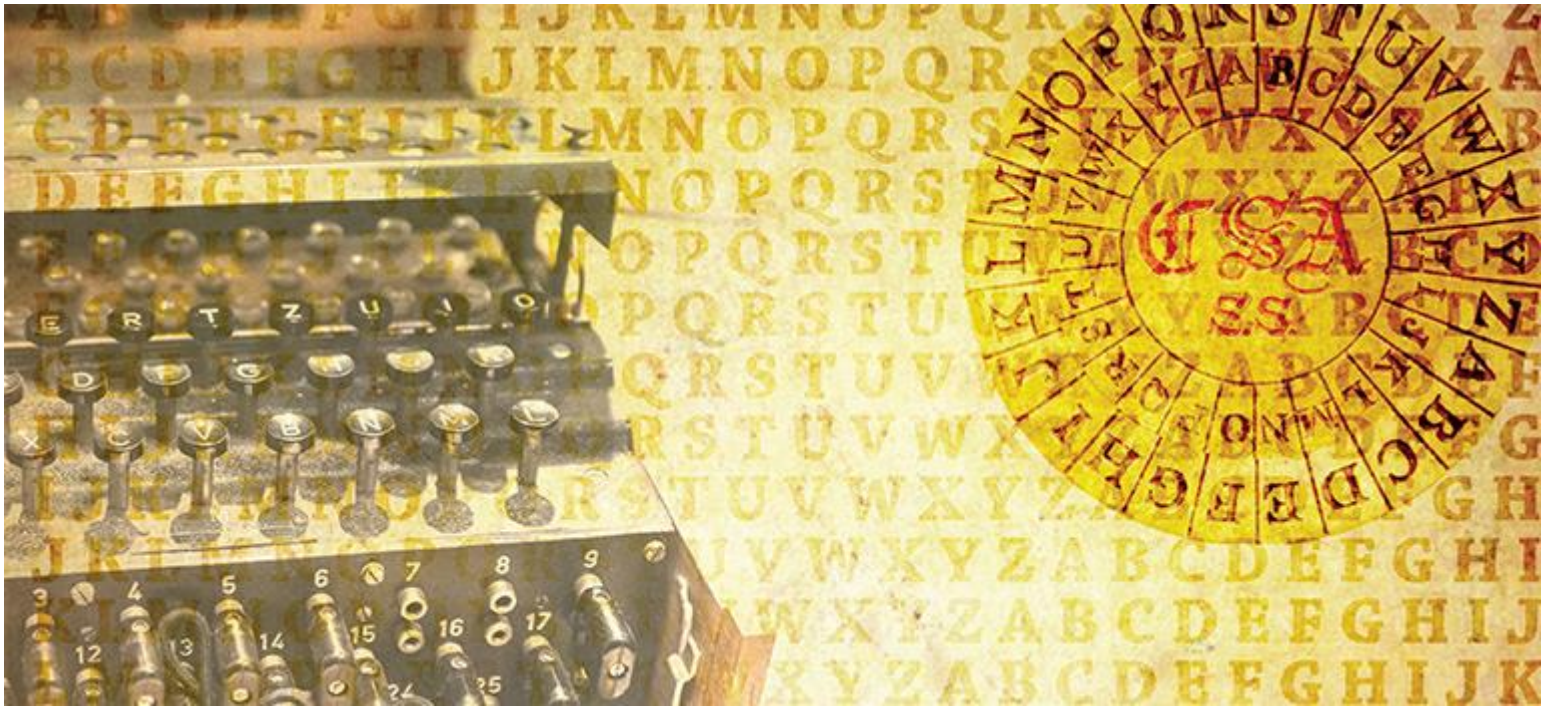

introduzione alla crittografia

A. Ferrari

- **steganografia**: occultamento del messaggio
- **crittografia**: occultamento del significato del messaggio
- **messaggio in chiaro**: testo da crittare
- **chiave**: informazione usata come parametro in un algoritmo crittografico
- **crittoanalisi**: scienza dell'interpretazione del messaggio di cui si ignora la chiave

- ***steganografia***
  - στεγανός (**coperto**) e γραφία (**scrittura**)
- nascondere l'esistenza di dati
- esempio: ***LSB*** (least significant bit, bit meno significativo)
  - l'aspetto di un'immagine digitale non cambia se i colori vengono modificati in modo impercettibile
  - il cambiamento del bit meno significativo della rappresentazione di ogni pixel, il suo colore non apparirà variato e il contenuto dell'immagine sarà preservato
  - l'insieme dei bit meno significativi di ogni pixel rappresenta il messaggio che risulta nascosto

un esempio di steganografia

A. Ferrari

Per il timore di ciascuna di queste cose [Aristagora] meditava una rivolta. Accadde anche che gli arrivasse da Susa, da parte di Istieo, un uomo con la ***testa tatuata*** che gli annunciava di ribellarsi al re. Infatti Istieo, volendo segnalare ad Aristagora di ribellarsi, non aveva d'altra parte nessun modo sicuro per farlo, dal momento che le strade erano sorvegliate e quindi, avendo ***rasato*** il capo del più fedele dei servi, vi ***incise*** dei segni, e attese che gli ***ricrescessero i capelli***; e non appena gli furono cresciuti lo mandava a Mileto, ordinandogli soltanto, una volta giunto a Mileto, di dire ad Aristagora di guardare sul suo capo dopo avergli ***rasato*** i capelli. E i segni indicavano, come ho detto prima, rivolta.

Erodoto, Storie

Erodoto (greco: Ἡρόδοτος, Herodotos; Alicarnasso, 484 a.C. – Thurii, 425 a.C.) è stato uno storico greco antico, famoso per aver descritto paesi e persone da lui conosciute in numerosi viaggi. In particolare ha scritto a riguardo dell'invasione persiana in Grecia nell'opera Storie (Ἱστορίαι, Istoriai)..

- ***crittografia***
  - κρυπτός (**nascosto**) e γραφία (**scrittura)**
- metodo per rendere un messaggio non comprensibile a persone non autorizzate a leggerlo
- il messaggio è definito crittogramma
- ***crittologia***
  - studio della crittografia e della crittanalisi

- ***chiave***
  - informazione usata come parametro in un algoritmo crittografico
- unico ***dato*** che è necessario mantenere ***segreto***
- la dimensione della chiave (misurata in bit) dipende dall'algoritmo usato
- ***brute force***
  - attacco a forza bruta (ricerca esaustiva)
  - provare tutte le chiavi possibili
  - una chiave di n bit ha 2^n chiavi distinte

- ***crittoanalisi***
  - kryptós (**nascosto**) e analýein (**scomporre**)
- studio dei metodi per ottenere il significato di informazioni cifrate senza avere accesso all'informazione segreta
  - ***trovare una chiave segreta***
- è la "***controparte***" della crittografia

crittografia classica
(dall'antichità al 1975)

A. Ferrari

- ***metodi antichi***
  - scitala spartana
  - scacchiera di Polibio
  - codice atbash
  - codice di Cesare
- ***rinascimento***
  - Blaise Vigenère
- ***XX secolo***
  - macchina Enigma
    - usata dai tedeschi durante la Seconda Guerra Mondiale
  - DES (Data Encryption Standard)

- ***crittografia moderna***
  - nasce nel 1975 con un articolo di Diffie & Hellman
  - si propone un **nuovo protocollo per lo scambio delle chiavi (**tallone d'Achille della crittografia classica)
- rende possibile la trasmissione sicura di dati fra entità che non hanno concordato preventivamente le chiavi
- esempio:
  - RSA