

# CRITTOGRAFIA

## Parte 1 - Crittografia Classica

# TABLE OF CONTENTS

- Perché la Crittografia?
- Crittografia Classica
- Cifrario di Vigenère
- Macchina Enigma
- I Problemi della Crittografia Classica
- Verso la Crittografia Moderna































**PERCHÉ LA CRITTOGRAFIA?**

Le società umane, nel corso degli anni, hanno sviluppato **sistemi informativi** sempre più complessi.

I **numeri** ad esempio sono stati introdotti intorno a 6.000 anni fa all'interno della civiltà dei **Sumeri**.

Il loro obiettivo?

**La burocrazia.** Tener traccia delle quantità dei vari oggetti di interesse (cibo, persone, armi, etc...)

1		11		100	
2		12		200	
3		20		300	
4		30		400	
5		40		500	
6		50		600	
7		60		700	
8		70		800	
9		80		900	
10		90		1000	

In alcuni contesti avere accesso a determinate informazioni può essere la differenza tra la vita e la morte.

# PROCESSO DI MARIA STUARDA

## Processo di Maria Stuarda (1/10)

---

Mercoledì 15 ottobre 1586.

Castello di Fotheringhay, Inghilterra centrale.

Maria Stuarda, nota come **la Regina degli Scozzesi**, è sotto processo per tradimento nei confronti della regine **Elisabetta I**.



## Processo di Maria Stuarda (2/10)

---

**Sir Francis Walsingham**, segretario di Stato, cerca prove schiaccianti contro di lei, in quanto consapevole che Elisabetta non firmerà la condanna altrimenti.

## Processo di Maria Stuarda (3/10)

---

Varie ragioni dietro al timore di Elisabetta:

- Maria è regina di Scozia
- Potenziale pericoloso precedente
- Maria è cugina di Elisabetta

## Processo di Maria Stuarda (4/10)

---

Maria rimane tranquilla, consapevole di aver precedentemente cifrato tutti i messaggi della congiura.

## Processo di Maria Stuarda (5/10)

---

**Francis Walsingham**, essendo consapevole di questo, chiamò immediatamente **Thomas Phelippes**, il migliore decifratore d'Inghilterra.

## Processo di Maria Stuarda (6/10)

---

Il metodo di cifratura utilizzato dalla Stuarda per comunicare con gli altri cospiratori, primo tra tutti il giovane **Anthony Babington**, è chiamato **nomenclatore**.

## Processo di Maria Stuarda (7/10)

---

Si utilizzavano 23 simboli da sostituire alle tipiche lettere dell'alfabeto chiaro (escludendo j , v , w) e di 35 simboli che rappresentavano parole o frasi.

# Processo di Maria Stuarda (8/10)

a b c d e f g h i k l m n o p q r s t u x y z  
 o † ʌ # a □ θ ∞ i ð n ll ø ▽ s m f Δ ε c 7 8 9

Nulles ff. — . — . d. Dowbleth σ

and for with that if but where as of the from by  
 2 3 4 4 4 3 ʝ n m 8 X ∞

so not when there this in wich is what say me my wyrt  
 ʝ X ++ ʝ 6 x 6 m n m m d

send lre receave bearer I pray you Mte your name myne  
 ʝ ʝ † T 1 1 1 ʝ ʝ ss

## Processo di Maria Stuarda (9/10)

---

A sua insaputa però, tutta la sua corrispondenza veniva letta e decifrata da **Walsingham**, che alla fine la inganno forgiando un messaggio falso nello scrivere una lista dei suoi collaboratori.



## Processo di Maria Stuarda (10/10)

---

Maria Stuarda viene decapitata l'8 febbraio 1587.

**PERCHÉ ABBIAMO BISOGNO DELLA CRITTOGRAFIA?**

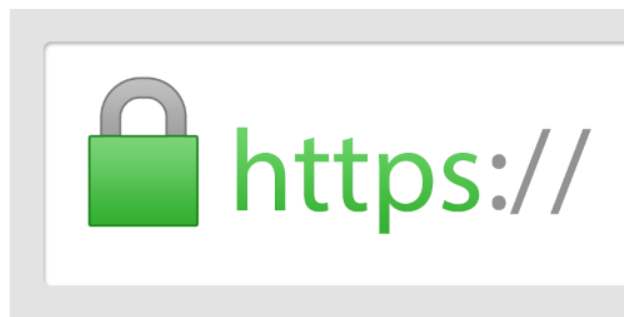
Perché oramai le **informazioni** hanno un diretto e  
irreversibile effetto sulla realtà.

La **crittografia** offre strumenti, tecniche e tecnologie che ci permettono di avere più controllo sul modo in cui le informazioni che ci riguardano influenzano la nostra vita.

Molte realtà di oggi si basano sull'offerta di servizi di crittografia



**Signal**



Cerchiamo quindi di capire come la crittografia si è evoluta nel corso del tempo.

# CRITTOGRAFIA CLASSICA

Iniziamo con qualche **etimologia** (dal greco)

---

- **steganografia:**
  - steganós → "coperto"
  - graphía → "scrittura"
- **crittografia:**
  - kryptós → "nascosto"
  - graphía → "scrittura"



In altre parole,

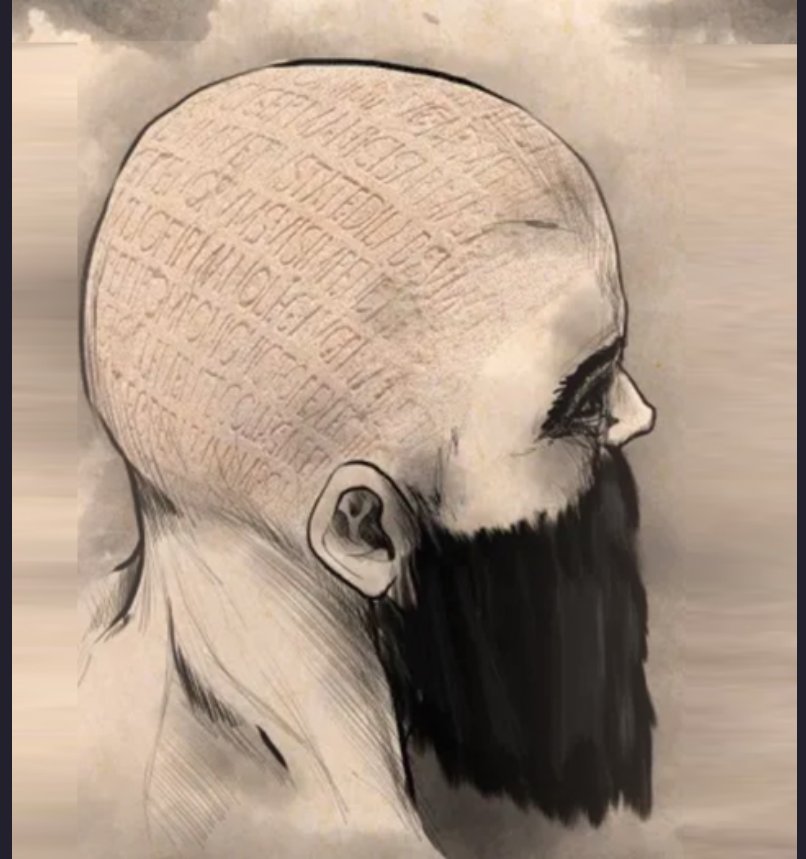
La **steganografia** vuole nascondere l'intero messaggio, sia il **contenuto** che il **contenitore**.

La **crittografia**, invece, vuole nascondere solo il **significato** del messaggio, ovvero solo il contenuto, ma non il contenitore.

**Queste tecniche possono essere combinate tra loro.**

# ESEMPIO DI STEGANOGRAFIA

Erodoto, uno dei primi scrittori della Storia, racconta la pratica, utilizzata durante le **Guerre persiane** (+2500 anni fa), di radere il capo dei corrieri, scrivere dei messaggi ed aspettare la ricrescita per nascondere i messaggi durante il tragitto.



# ESEMPIO DI CRITTOGRAFIA

## Cifrario di Cesare (1/5)

---

Nascondiamo il significato di un messaggio andando a **spostare** le lettere dell'alfabeto per una data quantità  $c = 3$ .

## Cifrario di Cesare (2/5)

---

Partiamo da un alfabeto in chiaro

ABCDEFGHIJKLMNOPQRSTUVWXYZ

## Cifrario di Cesare (2/5)

---

Per ottenere un alfabeto cifrante

ABCDEFGHIJKLMNOPQRSTUVWXYZ



DEFGHIJKLMNOPQRSTUVWXYZABC



## Cifrario di Cesare (3/5)

---

Data una singola lettera, otteniamo il cifrato utilizzando l'alfabeto cifrante

$$A \longrightarrow A + 3 = D$$

## Cifrario di Cesare (4/5)

---

Se abbiamo tante lettere, ne cifriamo una alla volta

HELLO WORLD



KHOOR ZRUOG

## Cifrario di Cesare (5/5)

---

```
#!/usr/bin/env python3
```

```
def main():  
    shift_value = 3  
    cipher = Caesar(shift=shift_value)  
    plaintext = "HELLO WORLD"  
    ciphertext = cipher.encrypt(plaintext)  
    print(f"[c={shift_value}] '{plaintext}' -> '{ciphertext}'")
```

`./code/caesar.py`

# TRASPOSIZIONE E SOSTITUZIONE

Il **cifrario di Cesare** è un **cifrario mono-alfabetico**  
basato sulla **sostituzione**.

In generale i **cifrari classici** lavorano sulle lettere dell'**alfabeto tradizionale** in due modi diversi:

**trasposizione**: le lettere del messaggio sono spostate di posto.

**sostituzione**: le lettere del messaggio sono sostituite con altre lettere.

# CIFRARIO DI VIGENÈRE

Il **cifrario di Vigenère** è una generalizzazione del cifrario di cesare. Al posto di avere un solo alfabeto cifrante, **abbiamo tanti alfabeti cifranti**, che sono utilizzati in modo alternato.



## Esempio (1/4)

---

Supponiamo di avere tre alfabeti cifranti

ABCDEFGHIJKLMNOPQRSTUVWXYZ



ABCDEFGHIJKLMNOPQRSTUVWXYZ

DEFGHIJKLMNOPQRSTUVWXYZABC

CDEFGHIJKLMNOPQRSTUVWXYZAB

## Esempio (2/4)

---

Per cifrare una sequenza di lettere scegliamo in modo sequenziale i vari alfabeti cifranti, e dopo aver cifrato tre lettere torniamo ad utilizzare il primo alfabeto cifrante.

## Esempio (3/4)

---

HELLO WORLD



HHNLR WRTLГ

## Esempio (4/4)

---

Piuttosto che descrivere gli alfabeti cifrante in modo interamente, possiamo abbreviarli utilizzando la prima lettera dell'alfabeto.

ABCDEFGHIJKLMNOPQRSTUVWXYZ → A

DEFGHIJKLMNOPQRSTUVWXYZABC → D

CDEFGHIJKLMNOPQRSTUVWXYZAB → C

La nostra **chiave di cifratura** è dunque ADC.

```
def main():  
    key = "ADC"  
    cipher = Vigenere(key)  
    plaintext = "HELLO WORLD"  
    ciphertext = cipher.encrypt(plaintext)  
    print(f"[key='{key}'] '{plaintext}' -> '{ciphertext}'")
```

`./code/vigenere.py`

**MACCHINA ENIGMA**

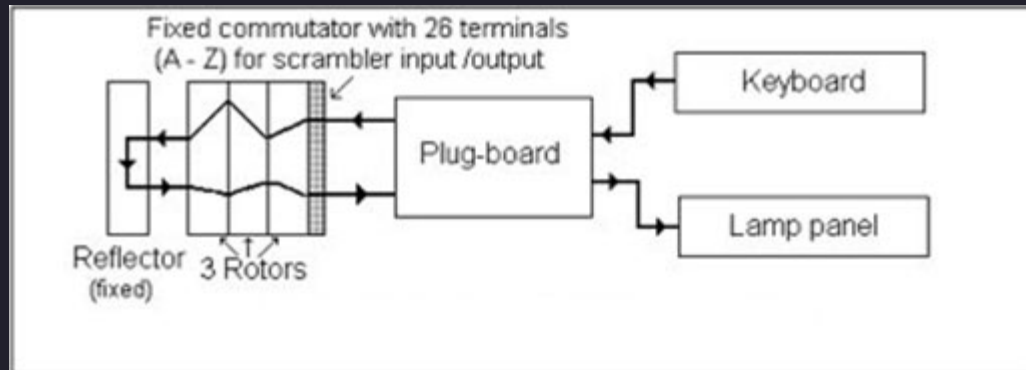
La macchina **Enigma** è un dispositivo **elettro-meccanico** che implementa un cifrario a sostituzione molto complesso.



Enigma è stata utilizzata dai tedeschi e dalle forze dell'Asse durante la seconda guerra mondiale per proteggere le informazioni di guerra.



Premendo un tasto sulla tastiera si chiude un circuito elettrico, accendendo una lampadina.



- tasto sulla tastiera → lettera in chiaro
- lampadina illuminata → lettera cifrata

Per chi fosse interessato, ho implementato un emulatore della macchina enigma in C. Il progetto è disponibile nella seguente github repository

<https://github.com/LeonardoE95/enigma-machine>

```
Enigma> info
Enigma> Current configuration...
      Rotors (from left to right): M3-II, M3-I, M3-III
            Position: 0, 0, 0
            Ring: 0, 0, 0
      Reflector: M3-B
      Plugboard: 6 plugs
                (A, M)
                (F, I)
                (N, V)
                (P, S)
                (T, U)
                (W, Z)
Enigma> encrypt HELLO
MIJEN
```

<https://github.com/LeonardoE95/enigma-machine>

# I PROBLEMI DELLA CRITTOGRAFIA CLASSICA

I primi cifrari, tra cui quello di Cesare e Vigenère, soffrivano di un problema di dimensione rispetto allo **spazio delle chiavi**. Lo spazio delle chiavi di questi cifrari è, semplicemente, troppo piccolo.

Nel **Cifrario di Cesare** abbiamo 26 possibili chiavi.

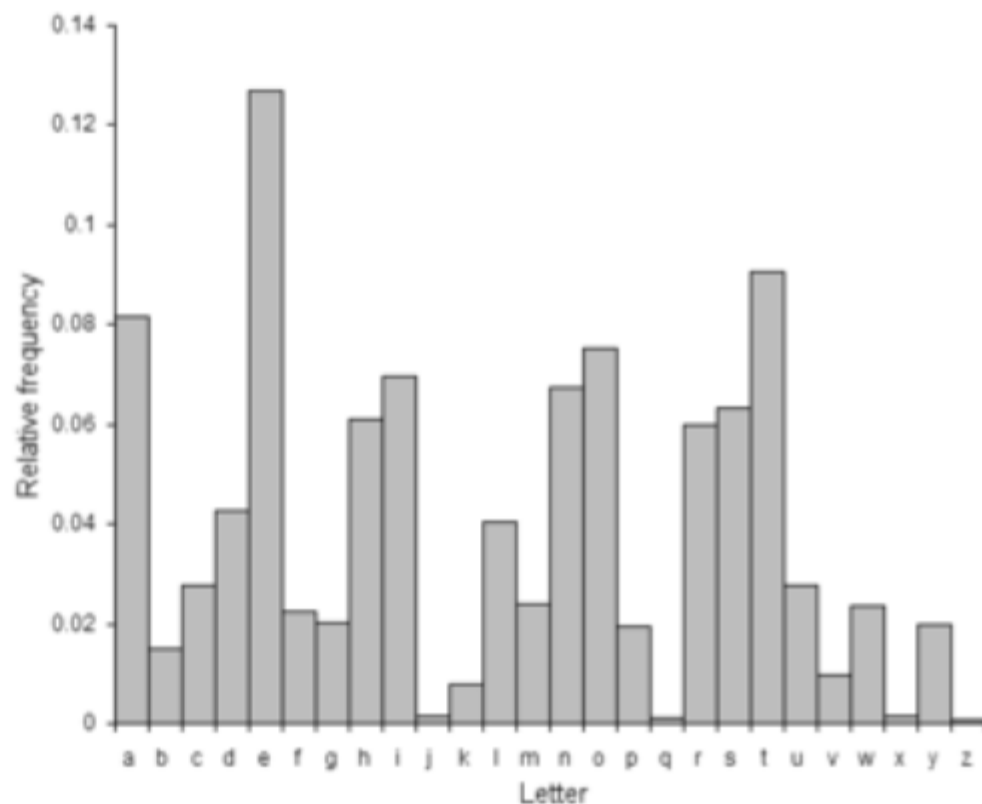
Nel **Cifrario di Vigenéré** abbiamo  $26^n$  possibili chiavi  
per una chiave di dimensione  $n$ .

Oltre alla dimensione dello spazio delle chiavi, un altro problema, assai più profondo, è legato al fatto che questi cifrari lavorano al livello delle **singole lettere**.

Il problema, in particolare, è che **la frequenza delle lettere nei linguaggi naturali NON è uniforme**.

# Frequenza delle lettere in inglese

E	11.1607%	56.88	M	3.0129%	15.36
A	8.4966%	43.31	H	3.0034%	15.31
R	7.5809%	38.64	G	2.4705%	12.59
I	7.5448%	38.45	B	2.0720%	10.56
O	7.1635%	36.51	F	1.8121%	9.24
T	6.9509%	35.43	Y	1.7779%	9.06
N	6.6544%	33.92	W	1.2899%	6.57
S	5.7351%	29.23	K	1.1016%	5.61
L	5.4893%	27.98	V	1.0074%	5.13
C	4.5388%	23.13	X	0.2902%	1.48
U	3.6308%	18.51	Z	0.2722%	1.39
D	3.3844%	17.25	J	0.1965%	1.00
P	3.1671%	16.14	Q	0.1962%	(1)





Questa osservazione ha portato alcuni arabi, intorno all'800, allo sviluppo delle prime tecniche di **crittoanalisi**, il cui obiettivo è quello di rompere i cifrari

- capire la chiave
- decifrare i testi cifrati

# Manuscript on Deciphering Cryptographic Messages



(al-Kindi)

**VERSO LA CRITTOGRAFIA MODERNA**

Per passare dalla crittografia classica alla crittografia moderna iniziamo da un principio, il **principio di Kerckhoffs**.

## Principio di Kerckhoffs

---

La sicurezza di un crittosistema non deve dipendere dal tenere celato il critto-algoritmo. La sicurezza deve dipendere solo dal tenere celata la chiave

Un cambiamento fondamentale tra la crittografia classica e la crittografia moderna è data dall'**introduzione del bit** come unità fondamentale di informazione.

Lavoro di **Claude Shannon**, che nel suo lavoro di tesi  
dimostrò la connessione tra

**algebra booleana  $\leftrightarrow$  circuiti logici**

**Claude Shannon, A symbolic analysis of relay and switching circuits, 1937**

## Prossimamente...

- Triade CIA
- Protocolli di crittografia
- Primitive crittografiche
- Matematica



