Segreti Digitali
Come l'Informatica Protegge le Nostre Vite

Andrea Pozzi

Università Cattolica del Sacro Cuore

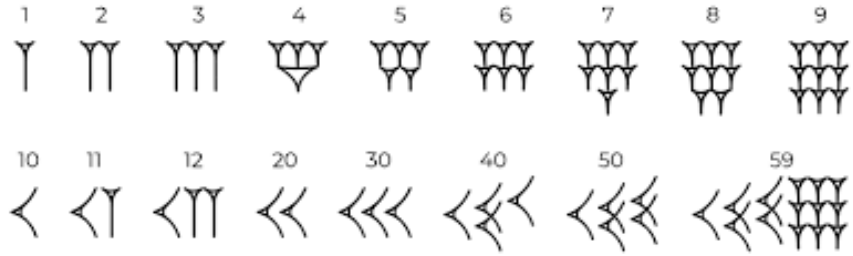
27 Ottobre 2025

Perchè la crittografia?

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

Un sistema informativo è un insieme organizzato di tecnologie e procedure che serve a raccogliere ed elaborare informazioni per supportare attività e decisioni di un'organizzazione o di una comunità.

I numeri ad esempio son stati introdotti circa nel 4000 a.C. dalle civiltà sumeriche. Il loro scopo era principalmente **contabilità e burocrazia**: tenere traccia delle quantità di cibo, di armamenti, di materie prime, etc.



Perchè la crittografia?

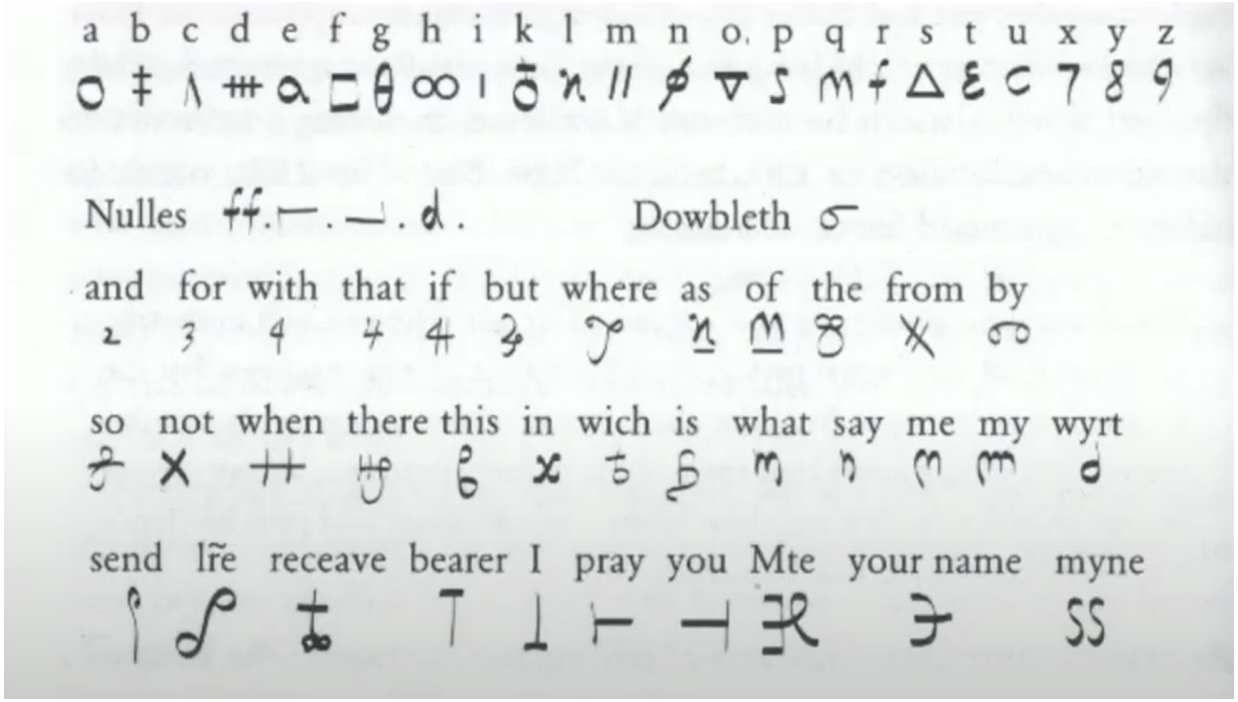
In alcuni contesti avere accesso a determinate informazioni può rappresentare la differenza tra la vita e la morte: ad esempio, in uno scenario di guerra, conoscere dove si trova il nemico o quali tecnologie utilizza può risultare fondamentale per decidere le sorti del conflitto.

Esempio classico: 15 ottobre 1586, Castello di Fotheringhay, Inghilterra, Mary Stuart (la Regina degli Scozzesi) è sotto processo per tradimento nei confronti della regina Elisabetta I.

Processo di Maria Stuarda

Mary Stuart, che tramava una congiura nei confronti di Elisabetta I, si è premurata di cifrare tutte le comunicazioni avute con gli altri cospiratori attraverso un algoritmo noto come **nomenclatore**.

Durante le indagini, il linguista Thomas Phelippes fu incaricato di decifrare le lettere: il suo successo dipendeva principalmente dalla robustezza dell'algoritmo usato da Mary Stuart.



Perchè la crittografia?

Conoscere alcune informazioni può avere un effetto diretto e irreversibile 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 oggi offrono servizi di crittografia: *Whatsapp*, *Telegram*, *https://*, etc.

La crittografia si è evoluta nel tempo: le tecniche usate da Giulio Cesare sono molto diverse da quelle usate da Mary Stuart, oppure dai servizi d'intelligence della Germania nazista.

Etimologia della Parola Crittografia

Steganografia: vuole rendere invisibile l'esistenza stessa del messaggio (nascosto dentro un'immagine, un audio o un file di testo).

- steganós → coperto
- graphía → scrittura

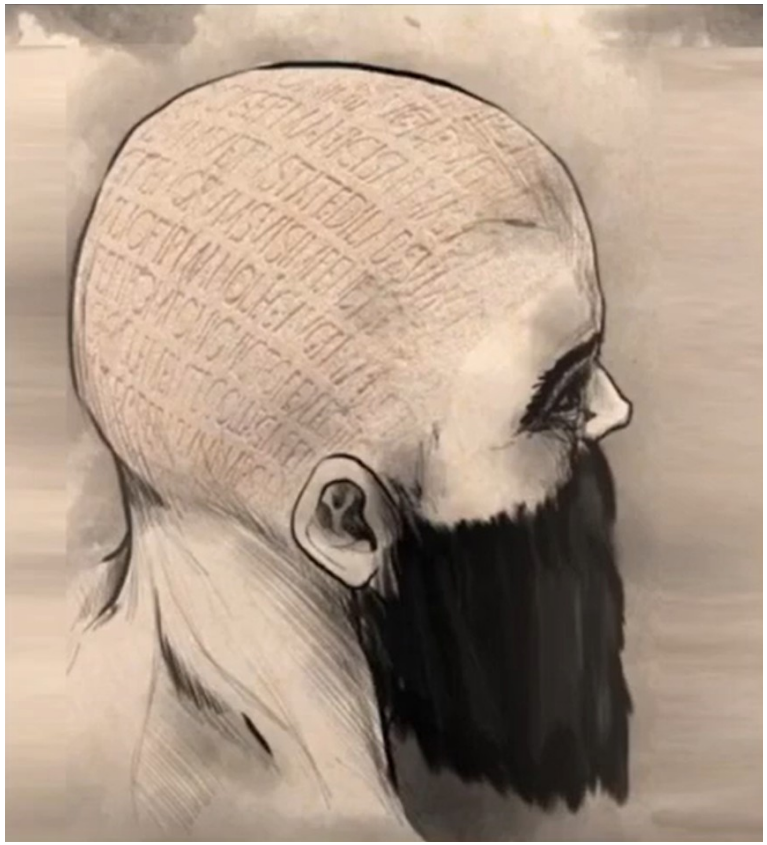
Crittografia: ha l'obbiettivo di rendere illeggibile il contenuto del messaggio a chi non ha la chiave, ma è evidente l'esistenza di un messaggio cifrato.

- kryptós → nascosto
- graphía → scrittura

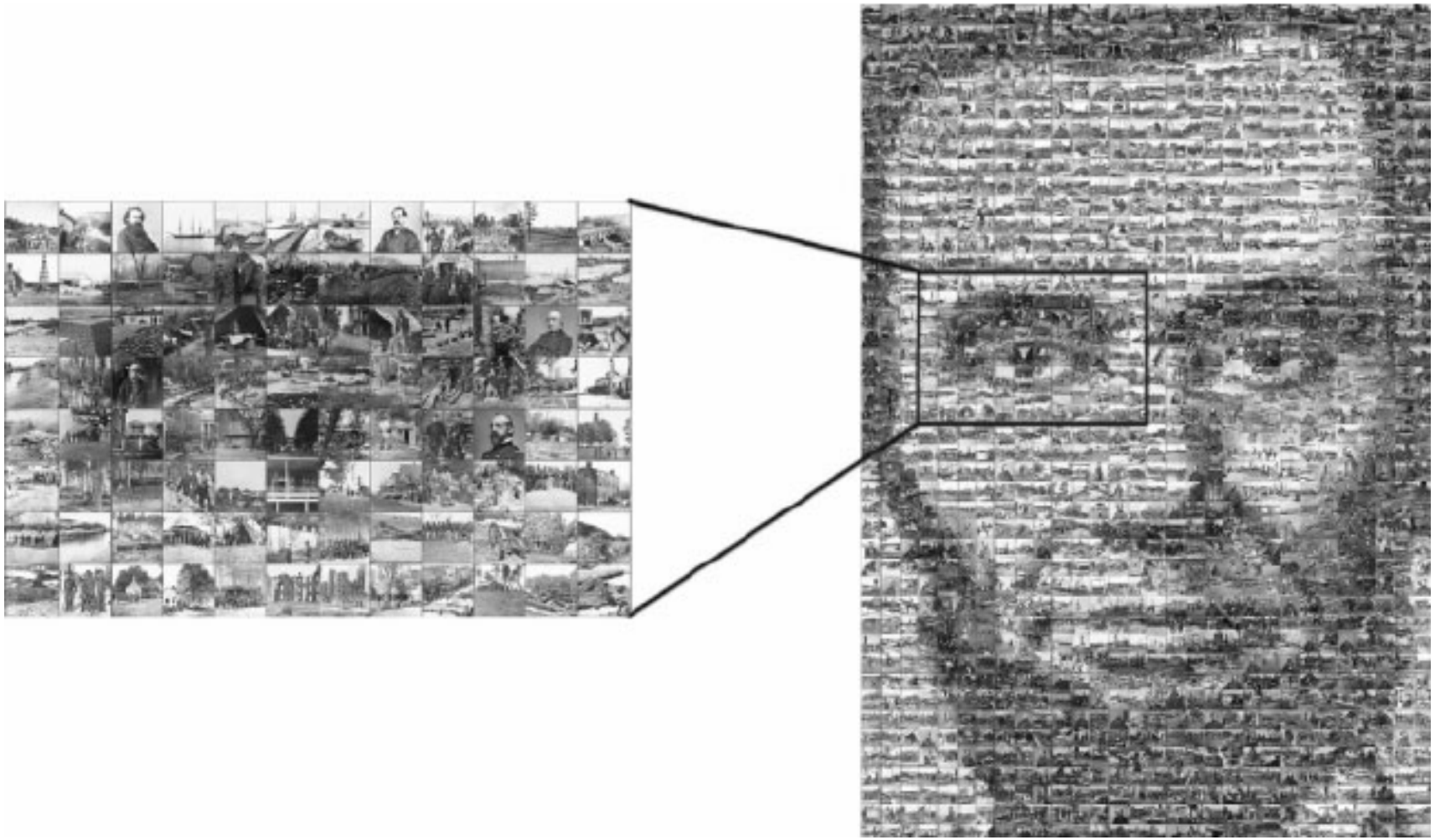
La steganografia è utile quando anche la sola presenza di un messaggio segreto può destare sospetti o rischi (es: in paesi con regimi autoritari dove la comunicazione cifrata è vietata, o attira l'attenzione). Le due tecniche possono essere combinate: prima si cifra il messaggio, poi lo si nasconde.

Esempio di Steganografia

Erodoto, uno dei primi scrittori della storia, descrive una sorprendente pratica steganografica utilizzata dai Greci durante le Guerre Persiane del V secolo a.C.: radere il capo dei corrieri, scrivere il messaggio segreto sul cranio rasato ed aspettare la ricrescita dei capelli per nascondere il messaggio durante il tragitto.

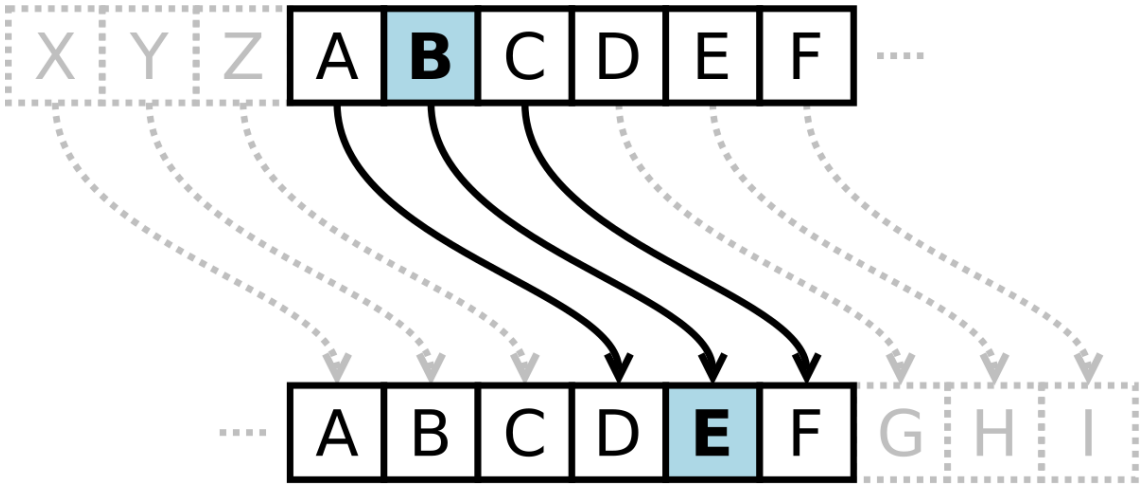


Esempio di Steganografia: Messaggio Nascosto in un'Immagine



Esempio di Crittografia: Cifrario di Cesare

Nel **cifrario di Cesare** il contenuto di un messaggio viene occultato andando a spostare le lettere dell'alfabeto di una certa quantità detta chiave (Giulio Cesare usava uno spostamento di 3 lettere).



Il Cifrario di Cesare è un cifrario **monoalfabetico** a **sostituzione**, poichè ogni lettera in chiaro è sostituita sempre dalla stessa lettera cifrata, fissata la chiave.

cifrare : HELLO WORLD $\rightarrow$ KHOOR ZRUOG

decifrare : KHOOR ZRUOG $\rightarrow$ HELLO WORLD

Trasposizione e Sostituzione

In generale **i cifrari classici** lavorano sulle lettere attraverso:

- **sostituzione**: ogni simbolo (o gruppo di simboli) del testo in chiaro viene sostituito da un altro simbolo, secondo una regola fissa (monoalfabetici: cifrario di Cesare, polialfabetici: cifrario di Vigenère);
- **trasposizione**: le lettere del testo in chiaro non vengono cambiate, ma il loro ordine viene riorganizzato secondo una regola;

Molti cifrari più complessi (come il cifrario di Playfair o Enigma) combinano entrambi i principi: prima sostituzioni, poi trasposizioni, per rendere il testo cifrato molto più difficile da analizzare.

Come è possibile **violare** il cifrario di Cesare (operazione detta **crittoanalisi**)? La strategia più immediata è provare tutte le traslazioni e scegliere quella che produce una frase in italiano sensata.

Disco Cifrante di Alberti

Il disco cifrante di Alberti è considerato il primo strumento meccanico per la crittografia polialfabetica, ideato nel XV secolo da Leon Battista Alberti. È composto da due dischi concentrici che ruotano indipendentemente: su ciascuno sono incise le lettere dell'alfabeto, ma in ordine diverso.

Esempio di Crittografia: Cifrario di Vigenère

Il **cifrario di Vigenère** (link online), ideato nel 1586, è una generalizzazione **polialfabetica** del cifrario di Cesare, basata sull'utilizzo alterno di diversi alfabeti cifranti.

Esempio: supponiamo di avere $k = 3$ alfabeti cifranti con chiavi $c_1 = 3$, $c_2 = 6$ e $c_3 = 1$. A partire dalla prima lettera del testo in chiaro, ciascuna lettera viene cifrata applicando, nell'ordine, la chiave corrispondente: la prima con c_1, la seconda con c_2 e la terza con c_3. Una volta utilizzate tutte le chiavi, la procedura ricomincia ciclicamente dalla prima chiave.

Viene di solito definita **chiave di cifratura** la sequenza di lettere in cui viene mappata la lettera A dell'alfabeto in chiaro dai diversi alfabeti cifranti.
Nell'esempio la chiave è **DGB**, poichè $D = A + c_1$, $G = A + C_2$ e $B = A + c_3$.

Ritenuto inviolabile per secoli, è stato in realtà **violato nel 1863** dal maggiore Friedrich Kasiski.

Esempio di Crittografia: la Macchina Enigma

Ideata nel 1923, la **macchina Enigma** è un dispositivo elettro-meccanico che implementa un cifrario polialfabetico estremamente complesso.

La macchina Enigma è stata **utilizzata dalla Germania nazista** e dalle altre forze dell'Asse durante la seconda guerra mondiale per proteggere le informazioni di guerra.

I Problemi della Crittografia Classica

I cifrari usati nella **crittografia classica** hanno uno spazio delle chiavi troppo ristretto:

- nel cifrario di Cesare lo spazio delle chiavi è pari a 26 interi;
- nel cifrario di Vigenère lo spazio delle chiavi è pari a 26^k, dove k è il numero degli alfabeti cifranti;

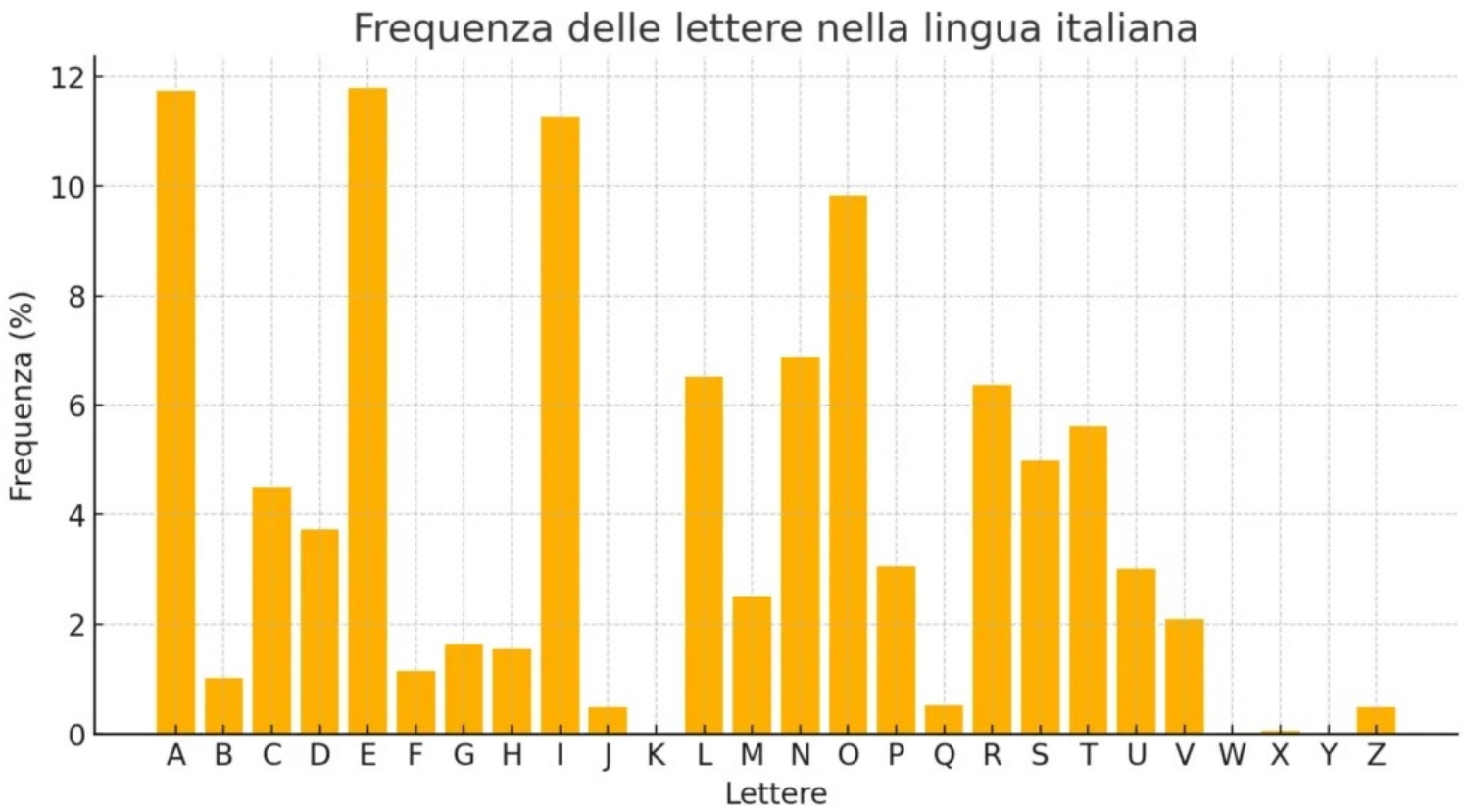
Inoltre un'altra problematica riguarda la comunicazione della chiave, specie nel caso di Vigenère in cui può essere particolarmente lunga.

In quest'ottica la crittografia ha fatto molti passi avanti, ovvero sono stati scoperti metodi molto sofisticati per comunicare la chiave ad un nuovo interlocutore (**crittografia contemporanea**).

I Problemi della Crittografia Classica

Inoltre i cifrari classici lavorano **a livello delle singole lettere**.

Questo è un problema poichè in ogni linguaggio naturale la frequenza delle lettere non è uniforme.



Nascita della Crittoanalisi

Questa intuizione porta nel IX secolo d.C. alla nascita della **crittoanalisi**, ovvero la disciplina che studia metodi per decifrare messaggi cifrati senza conoscere la chiave.

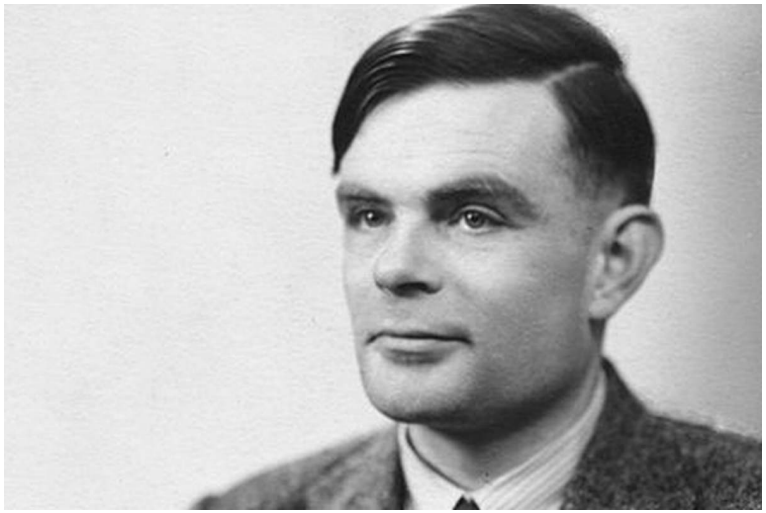
Tale disciplina nacque nel mondo arabo, grazie al matematico *al-Kindi*, che per primo descrisse l'*analisi delle frequenze* come tecnica per decifrare testi cifrati.

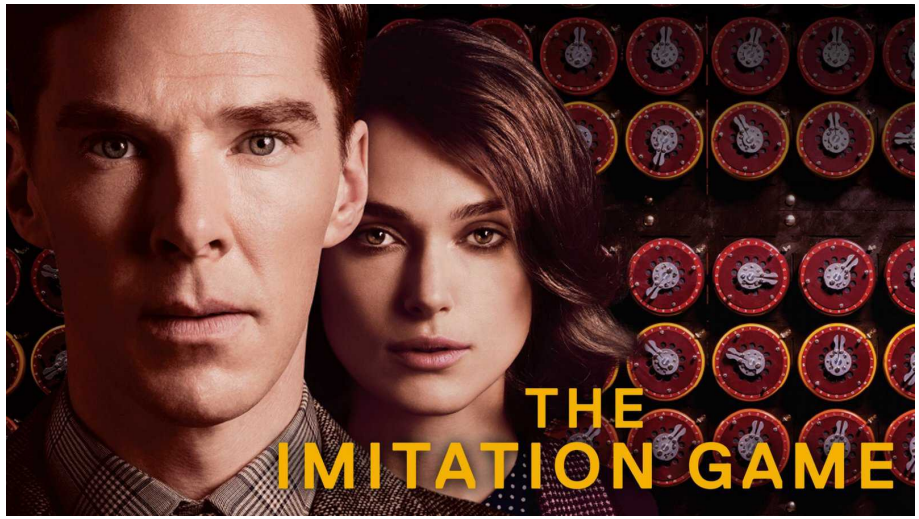
Per violare un testo cifrato la crittoanalisi segue questi due passaggi:

1. capire la chiave;
2. decifrare i testi cifrati;

La Decifrazione della Macchina Enigma

- Durante la Seconda Guerra Mondiale, la Germania nazista utilizzava la macchina **Enigma** per cifrare le comunicazioni militari.
- Il matematico britannico **Alan Turing**, insieme al team di **Bletchley Park**, sviluppò una macchina chiamata **Bombe** per decifrare i messaggi codificati.
- Questo lavoro fu cruciale per abbreviare la guerra e salvare milioni di vite.





Verso la Crittografia Moderna

Gli obbiettivi della crittografia non sono cambiati negli anni, ma le tecniche sono state migliorate significativamente.

Principio di Kerckhoffs: la sicurezza di un crittosistema non deve dipendere dal nascondere l'algoritmo che effettua le operazioni di cifratura e decifratura. **La sicurezza deve dipendere solamente dal nascondere la chiave**.

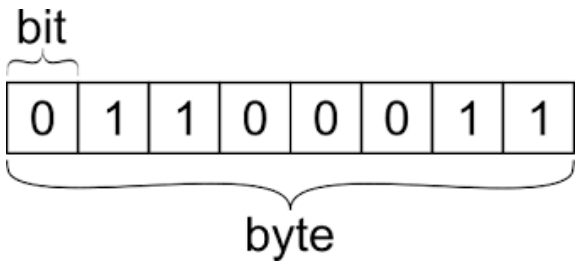
Questo ha senso poichè l'algoritmo può sempre essere compreso, e cercare di nasconderlo non è efficiente. Tutta la segretezza deve invece dipendere dalla chiave: se non la conosco non posso avere accesso, altrimenti la uso per accedere alle informazioni cifrate.

Verso la Crittografia Moderna

Un altro cambiamento fondamentale tra crittografia classica e moderna è l'**introduzione del bit** come unità fondamentale di informazione, rispetto alle lettere singole.

L'introduzione del bit permette la **rappresentazione digitale delle informazioni**. Tramite bit possiamo rappresentare numeri, testi, suoni e immagini.

Claude Shannon (1937, MIT) mostra che l'algebra di Boole può essere usata per rappresentare e manipolare informazioni usando circuiti elettrici (0 = off, 1 = on).



Numeri Binari

Il numero 154 in base 10 può essere scritto come:

$$154 = 1 \cdot 10^2 + 5 \cdot 10^1 + 4 \cdot 10^0$$

Lo stesso numero può essere rappresentato in base 2 (ovvero come numero binario che utilizza soltanto le cifre 0 e 1):

$$154 = 1 \cdot 2^7 + 0 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0$$

quindi il numero binario corrispondente a 154 è 10011010.

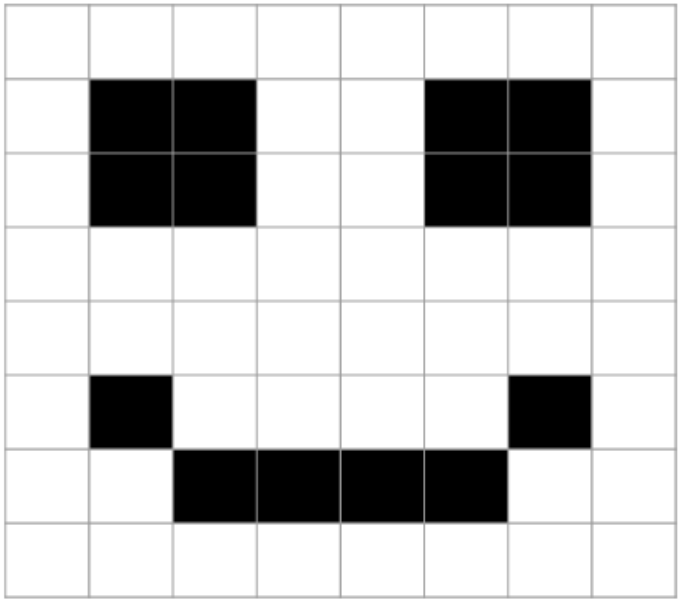
Bit e Testo

ASCII - Binary Character Table

Letter	ASCII Code	Binary	Letter	ASCII Code	Binary
a	097	01100001	A	065	01000001
b	098	01100010	B	066	01000010
c	099	01100011	C	067	01000011
d	100	01100100	D	068	01000100
e	101	01100101	E	069	01000101
f	102	01100110	F	070	01000110
g	103	01100111	G	071	01000111
h	104	01101000	H	072	01001000
i	105	01101001	I	073	01001001
j	106	01101010	J	074	01001010
k	107	01101011	K	075	01001011
l	108	01101100	L	076	01001100
m	109	01101101	M	077	01001101
n	110	01101110	N	078	01001110
o	111	01101111	O	079	01001111
p	112	01110000	P	080	01010000
q	113	01110001	Q	081	01010001
r	114	01110010	R	082	01010010
s	115	01110011	S	083	01010011
t	116	01110100	T	084	01010100
u	117	01110101	U	085	01010101
v	118	01110110	V	086	01010110
w	119	01110111	W	087	01010111
x	120	01111000	X	088	01011000
y	121	01111001	Y	089	01011001
z	122	01111010	Z	090	01011010

Bit e Immagini

Un'immagine è una matrice di tante piccole unità (**pixels**), in cui ogni pixel può essere rappresentato con un numero binario.



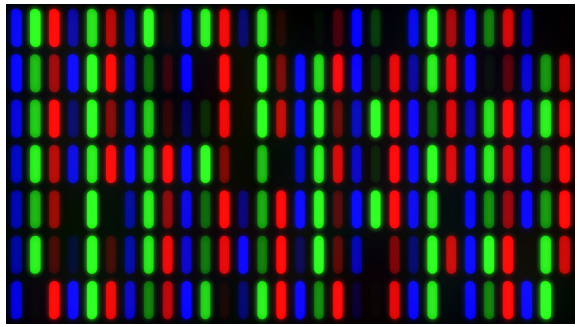
0	0	0	0	0	0	0	0
0	1	1	0	0	1	1	0
0	1	1	0	0	1	1	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	1	0	0	0	0	1	0
0	0	1	1	1	1	0	0
0	0	0	0	0	0	0	0

In un'immagine in scala di grigi, ogni pixel è rappresentato da 8 bits, i quali permettono di rappresentare 256 tonalità di grigio da nero (0) a bianco (255).

Bit e Immagini a Colori

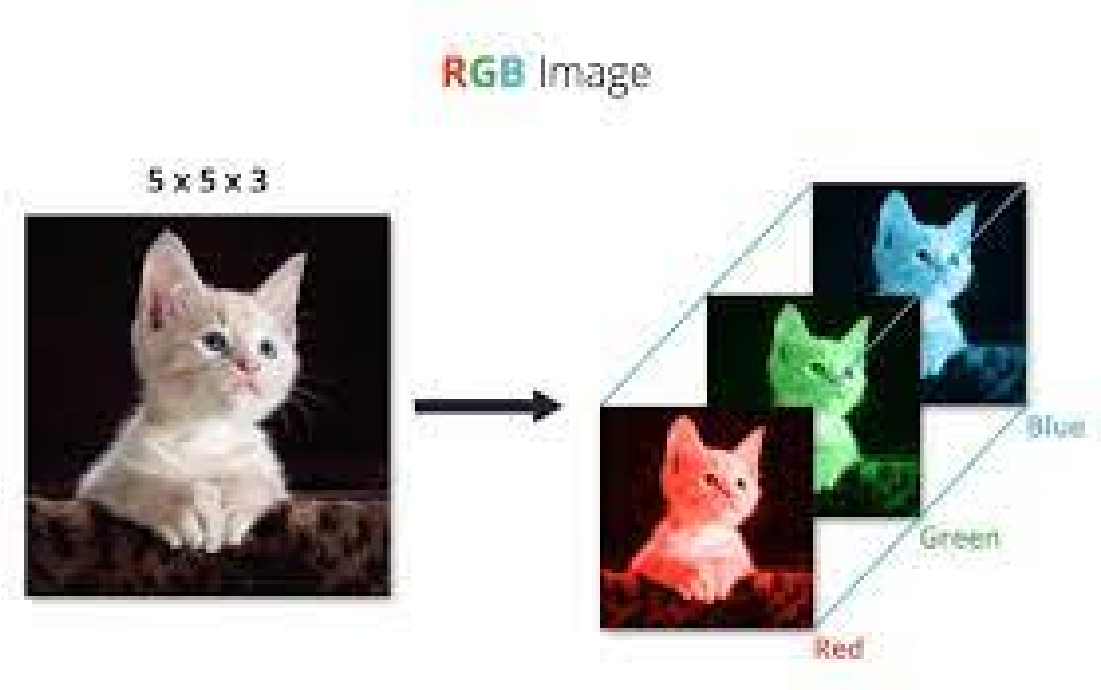
In immagini a colori, tipicamente, sono utilizzati 24 bits per ogni pixel: 8 bits per ogni canale RGB (**Rosso, Verde e Blue**). Questo permette di avere a disposizione 16 milioni di combinazioni diverse di colori!

Modificando questi bits, possiamo migliorare, modificare o addirittura creare immagini digitalmente.

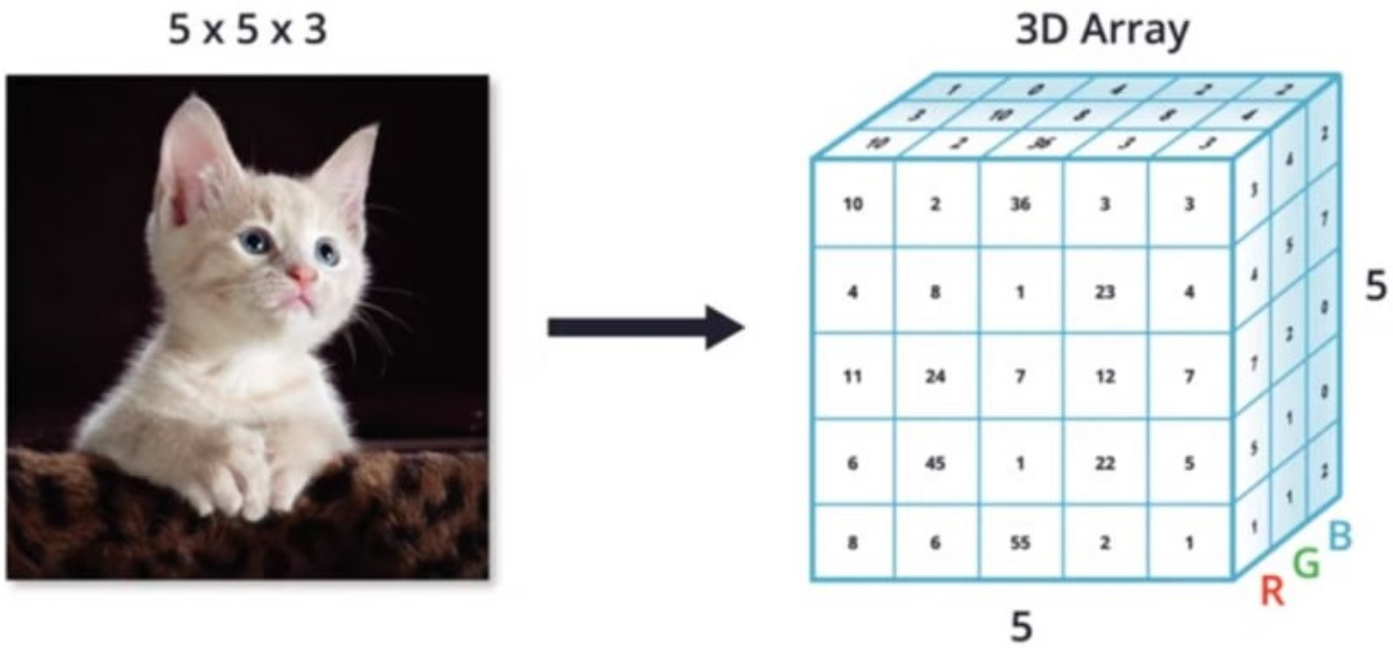


Bit e Immagini a Colori

- Per immagini a colori, ogni pixel ha tre canali ognuno associato ad un colore differente: rosso, verde e blu;
- Ogni canale ha un valore, tipicamente compreso tra 0 e 255, che indica la sua intensità;



Bit e Immagini a Colori



Cifratura Simmetrica: l'Operazione XOR

Idea di base: stessa chiave segreta per cifrare e decifrare. Operiamo *bit a bit* con XOR.

$$C = M \oplus K \qquad\qquad M = C \oplus K$$

- M = messaggio (in bit), K = chiave (in bit), C = cifrato.
- Proprietà chiave: applicare XOR due volte con la stessa chiave riporta al messaggio.
- Problema: riuso di chiavi/keystream $\Rightarrow$ emergono pattern e vulnerabilità.

Esempio: Cifratura e Decifratura con XOR

Messaggio originale (M): `101101`
Chiave (K): `110010`

Cifratura:

$$C = M \oplus K = \begin{array}{cccccc} 1 & 0 & 1 & 1 & 0 & 1 \\ \oplus & & & & & \\ 1 & 1 & 0 & 0 & 1 & 0 \\ \hline 0 & 1 & 1 & 1 & 1 & 1 \end{array} \Rightarrow C = \texttt{011111}$$

Decifratura:

$$M = C \oplus K = \begin{array}{cccccc} 0 & 1 & 1 & 1 & 1 & 1 \\ \oplus & & & & & \\ 1 & 1 & 0 & 0 & 1 & 0 \\ \hline 1 & 0 & 1 & 1 & 0 & 1 \end{array} \Rightarrow M = \texttt{101101}$$

Risultato: dopo la doppia applicazione di XOR con la stessa chiave si ottiene di nuovo il messaggio originale.

One-Time Pad: la cifratura perfetta

- Usa una **chiave casuale** lunga quanto il messaggio.
- Ogni bit del messaggio è combinato con la chiave tramite **XOR**.
- Se la chiave è:
  - totalmente **casuale**,
  - **usata una sola volta**,
  - e **mantenuta segreta**,

  allora la cifratura è **teoricamente inviolabile**.

Limite pratico

È difficile distribuire e conservare chiavi così lunghe e segrete.

DES: la nascita della crittografia industriale

DES (Data Encryption Standard) è lo standard di cifratura dei dati approvato nel 1977, sviluppato da IBM (da un progetto detto *Lucifer*) e adottato come standard federale negli Stati Uniti.

Idea a grandi linee:

- Cifrario *a blocchi* (64 bit) con chiave effettiva di **56 bit**.
- Struttura a *Feistel* con 16 round: sostituzioni (S-box) e permutazioni per confusione e diffusione.

Limite:

- **1998:** macchina costruita dalla Electronic Frontier Foundation (**$250k**) dimostrò la rottura pratica di DES in poche decine di ore.

AES: Advanced Encryption Standard

AES (Advanced Encryption Standard) (dal 2001): blocchi da 128 bit, chiavi da 128/192/256 bit, rete di sostituzione-permutazione.

Perché si usa ovunque:

- Altissima sicurezza (nessun attacco pratico noto sull'algoritmo completo).
- Molto veloce in software e hardware (AES-NI).

Ma resta un problema:

- **Scambio della chiave**: come condividere la chiave segreta iniziale in modo sicuro su un canale pubblico?

Crittografia Asimmetrica

Idea di base: usare due chiavi diverse ma matematicamente collegate.

$$(\text{chiave pubblica}, \text{chiave privata})$$

- La **chiave pubblica** può essere condivisa con tutti (cifrare, verificare).
- La **chiave privata** deve rimanere segreta (decifrare, firmare).

$$\text{Cifratura: } C = E_{\text{pubblica}}(M)$$
$$\text{Decifratura: } M = D_{\text{privata}}(C)$$

Esempio intuitivo: il lucchetto

- Immagina un *lucchetto* aperto: chiunque può **chiuderlo** (usando la chiave pubblica).
- Solo tu possiedi la chiave fisica per **aprirlo** (la chiave privata).

Modello Ibrido Moderno

Crittografia moderna ibrida:

- Usa **asimmetrica** per negoziare una chiave segreta.
- Usa **simmetrica** (AES/ChaCha20) per cifrare tutto il traffico dati poichè più veloce.

Esempi: TLS/HTTPS, VPN, messaggistica sicura.

$$\text{Pubblica/Privata} \Rightarrow \text{Chiave di sessione} \Rightarrow \text{AES su dati}$$

Esempio: la Crittografia di WhatsApp (semplificata)

Crittografia End-to-End: solo mittente e destinatario possono leggere i messaggi.

1. Ogni utente ha una **chiave pubblica** e una **chiave privata**.
2. Quando Alice scrive a Bob:
   - Alice genera una **chiave di sessione simmetrica** (per cifrare il messaggio con AES);
   - Cifra quella chiave di sessione con la **chiave pubblica di Bob**;
3. Quando Bob riceve un messaggio:
   - Decifra la chiave di sessione con la sua **chiave privata**.
   - Usa quella chiave per decifrare il messaggio.

Risultato:

- Solo Bob può leggere il messaggio.
- Neppure i server di WhatsApp conoscono le chiavi.
- La crittografia è **ibrida**: *asimmetrica per scambiare la chiave, simmetrica per cifrare i dati.*

Esempio: la Crittografia di HTTPS (semplificato)

Obiettivo: permettere al browser e al sito web di comunicare in modo cifrato e autentico.

Fasi principali:

1. Il browser si collega al sito e riceve il suo **certificato digitale**, che contiene la **chiave pubblica del server**;
2. Il browser verifica tramite una chiave pubblica emessa da una Certificate Authority (CA) che il certificato sia **autentico** (ovvero firmato dalla CA con la sua chiave privata);
3. Il browser genera una **chiave di sessione simmetrica**;
4. Cifra quella chiave con la **chiave pubblica del server** e la invia;
5. Il server la decifra con la sua **chiave privata**;

Da questo momento in poi:

- Tutto il traffico (HTML, immagini, dati...) è cifrato con la chiave simmetrica;
- La connessione è sicura, autentica e privata.

Criptovalute, QR Code, Computer Quantistico

- Criptovalute: il mittente firma con chiave privata;
- Il QR Code è crittografia?
- Crittografia post-quantistica?

Grazie a tutti per l'attenzione!

Domande e suggerimenti son ben accetti!