



# crittografia classica

A. Ferrari

- cifrario a *sostituzione monoalfabetica*
  - utilizza un alfabeto per il testo in chiaro e una *permutazione* dello stesso per il testo cifrato
  - la permutazione costituisce la chiave del sistema
  - ad ogni lettera del testo in chiaro viene associata la corrispondente lettera dell'alfabeto permutato

# 500-600 a.c. cifrario atbash

A. Ferrari

- *atbash*

- cifrario a sostituzione *monoalfabetica*
- la prima lettera dell'alfabeto è sostituita con l'ultima, la seconda con la penultima, e così via

- *testo in chiaro:*

- a b c d e f g h i l m n o p q r s t u v z

- *testo cifrato:*

- Z V U T S R Q P O N M L I H G F E D C B A

- esempio:

- PIANO LAUREE SCIENTIFICHE
- KRZML OZFIVV HXRVMGRURXSV



- **scitala** (σκυτάλη = bastone)
  - piccola bacchetta utilizzata dagli Spartani per trasmettere messaggi segreti
- il messaggio veniva scritto su di una striscia di pelle arrotolata attorno alla scitala, come se fosse stata una superficie continua
- una volta srotolata e tolta dalla scitala la striscia di pelle, era impossibile capire il messaggio
- la decifrazione era possibile se si aveva una bacchetta identica alla scitala del mittente: vi si arrotolava nuovamente la striscia di pelle ricostruendo la primitiva posizione
- si tratta del più antico metodo di crittografia per **trasposizione** conosciuto



# 150 a.c. scacchiera di Polibio

A. Ferrari

- la scacchiera originale è costituita da una **griglia** composta da 25 caselle ordinate in 5 righe ed altrettante colonne
- le lettere dell'alfabeto vengono inserite da sinistra a destra e dall'alto in basso
- le righe e le colonne sono numerate: tali numeri sono gli indici o "**coordinate**" delle lettere costituenti il messaggio in chiaro
- esempio (6x6)
  - PIANO LAUREE SCIENTIFICHE
  - FGDFAAFDFDFDXAAGFFXAVAVGAADFDFAVFDGDDFAXDFAFDDAV

Substitution matrix

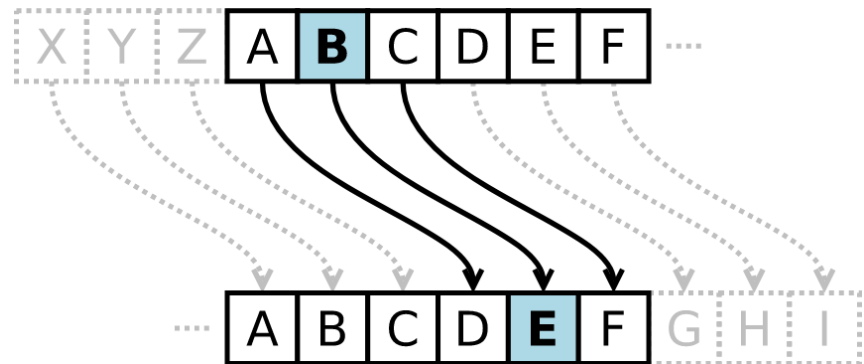
|   | A | D | F | G | V | X |
|---|---|---|---|---|---|---|
| A | A | B | C | D | E | F |
| D | G | H | I | J | K | L |
| F | M | N | O | P | Q | R |
| G | S | T | U | V | W | X |
| V | Y | Z | 0 | 1 | 2 | 3 |
| X | 4 | 5 | 6 | 7 | 8 | 9 |

|   | α | β | γ | δ | ε |
|---|---|---|---|---|---|
| α | A | B | Γ | Δ | E |
| β | Z | H | Θ | I | K |
| γ | Λ | M | N | Ξ | O |
| δ | Π | P | Σ | T | Υ |
| ε | Φ | X | Ψ | Ω | † |

# 50-60 a.c. metodo di Cesare

A. Ferrari

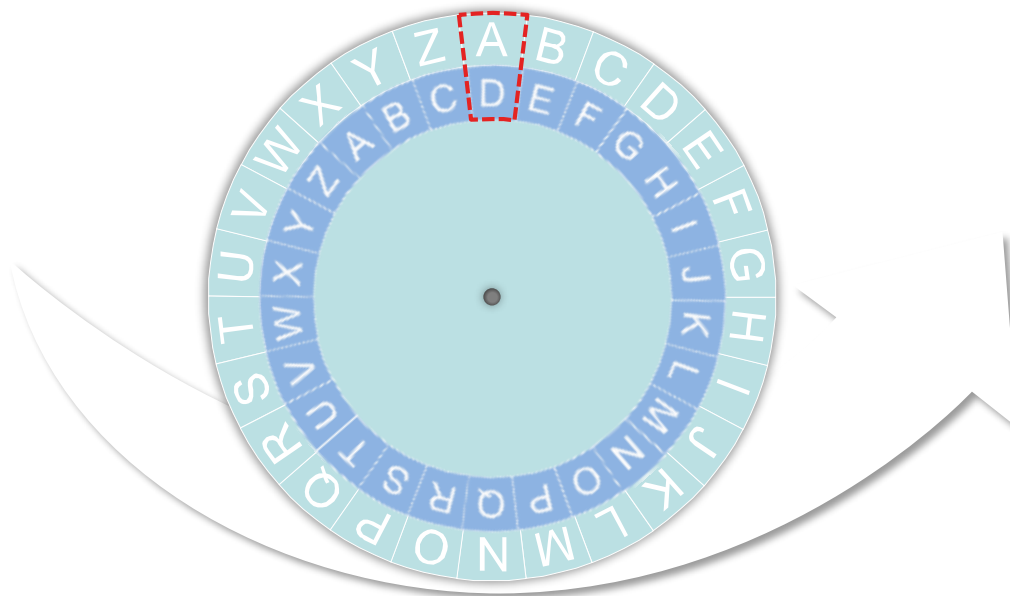
- cifrario di *Cesare*
  - cifrario a sostituzione monoalfabetica in cui ogni lettera del testo in chiaro è sostituita nel testo cifrato dalla lettera che si trova un certo numero di *posizioni successive* nell'alfabeto
- Cesare utilizzava uno spostamento di **3** posizioni
  - la chiave era 3
- esempio:
  - PIANO LAUREE SCIENTIFICHE
  - SLDQR ODXUHH VFLHQWLILFKH



- $P$  (alfabeto testo in chiaro [plaintext])
  - $C$  (alfabeto testo crittato)
  - $K_E$  (chiave di cifratura, parametro per  $f$ )
  - $K_D$  (chiave di decifratura, parametro per  $f^{-1}$ )
  - $f()$  (funzione di trasformazione crittografica)
- 
- $P = C = \{A, B, C, \dots, X, Y, Z\}$   
 $= \{0, 1, 2, \dots, 23, 24, 25\}$
  - $K_E = k \in P, k \neq 0$
  - $f(x_i) = (x_i + k) \bmod 26$
  - $K_D = k_d \in P, k_d = 26 - k$
  - $f^{-1}(x_i) = (x_i + k_d) \bmod 26$

# cifrari a scorrimento

A. Ferrari





# debolezze del metodo di Cesare

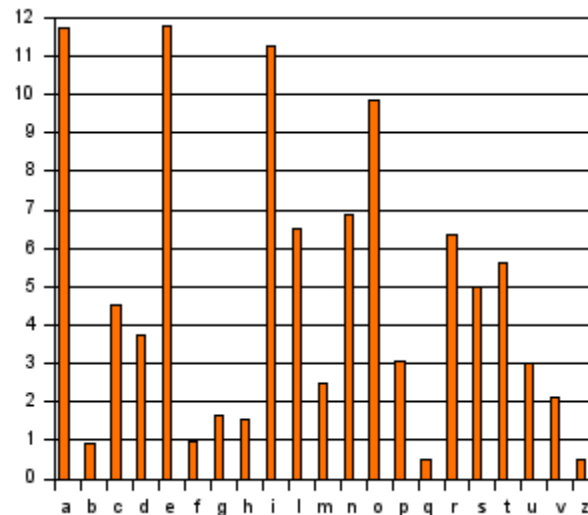
A. Ferrari

- il metodo di Cesare ha due principali **debolezze**:
  - è sensibile all'**analisi di frequenza**
  - sono possibili solo **poche chiavi** diverse ( $n - 1$ ) se  $n$  è il numero di caratteri dell'alfabeto
- chi intercetta un messaggio cifrato con il metodo di Cesare può limitarsi a provare successivamente tutte le possibili chiavi di cifratura e trovare il testo in chiaro in un tempo ragionevolmente breve (attacco a **forza bruta**)

# analisi di frequenze

- *analisi delle frequenze*

- studio della frequenza di utilizzo delle lettere o gruppi di lettere in un testo cifrato
- in ogni lingua la **frequenza** di uso di ogni lettera è piuttosto determinata



| Lettera | Frequenza |
|---------|-----------|
| a       | 11.74%    |
| b       | 0.92%     |
| c       | 4.50%     |
| d       | 3.73%     |
| e       | 11.79%    |
| f       | 0.95%     |
| g       | 1.64%     |
| h       | 1.54%     |
| i       | 11.28%    |
| l       | 6.51%     |
| m       | 2.51%     |
| n       | 6.88%     |
| o       | 9.83%     |
| p       | 3.05%     |
| q       | 0.51%     |
| r       | 6.37%     |
| s       | 4.98%     |
| t       | 5.62%     |
| u       | 3.01%     |
| v       | 2.10%     |
| z       | 0.49%     |

- il cifrario di Blaise de Vigenère è il più semplice dei ***cifrari polialfabetici***
- fu **ritenuto per secoli inattaccabile**
- si può considerare una ***generalizzazione*** del cifrario di Cesare
  - invece di spostare sempre dello stesso numero di posti la lettera da cifrare, questa viene spostata di un numero di posti variabile ma ripetuto
  - lo spostamento è determinato da una parola chiave da scrivere ripetutamente sotto il messaggio, carattere per carattere
- esempio:
  - PIANO LAUREE SCIENTIFICHE
  - ITIS
  - XBIFW EIMZXM KKBMFBBNAKAM



- $P$  (*alfabeto testo in chiaro [plaintext]*)
  - $C$  (*alfabeto testo crittato*)
  - $K_E$  (*chiave di cifratura, parametro per  $f$* )
  - $K_D$  (*chiave di decifratura, parametro per  $f^{-1}$* )
  - $f()$  (*funzione di trasformazione crittografica*)
- 
- $P = C = \{A, B, C, \dots, X, Y, Z\}$   
 $\quad = \{0, 1, 2, \dots, 23, 24, 25\}$
  - $K_E = k = [k_0, k_1, k_2, \dots, k_{m-1}] \in P^m, k \neq [0, \dots, 0]$
  - $f(x_i) = (x_i + k_i) \bmod 26$

# confronto Vigenère - Cesare

A. Ferrari

- il metodo di Vigenère rende impossibile l'analisi di frequenza perché le lettere più frequenti sono codificate con lettere diverse da colonna a colonna, con il risultato di rendere quasi uguali le frequenze relative delle lettere del testo cifrato
- il metodo di Vigenère sembra essere molto più robusto di quello di Cesare perché il crittografo ha due problemi:
  - determinare la lunghezza  $k$  della chiave
  - e poi la chiave stessa
- se l'alfabeto ha  $n$  caratteri, vi sono  $n^k$  possibili chiavi di cifratura, mentre sono solo  $n!/(n - k)!$  se vogliamo che i caratteri siano tutti diversi fra loro

*Cryptographia ad usum Delphini – A.Zaccagnini*

# debolezza del metodo di Vigenère

A. Ferrari

- considerato sicuro per alcuni secoli, finché un'analisi statistica più raffinata, di Kasinski, mostrò che è possibile “indovinare” la lunghezza  $k$  della chiave di cifratura, riducendo il problema della decifratura a  $k$  problemi di decifratura del metodo di Cesare
- l'analisi si basa sul fatto che in ogni lingua vi sono alcune combinazioni di due lettere piuttosto frequenti: se due istanze di questa coppia di lettere compaiono nel testo in chiaro ad una distanza che è un multiplo della lunghezza della chiave, saranno cifrate allo stesso modo, perché vanno a finire nelle stesse colonne

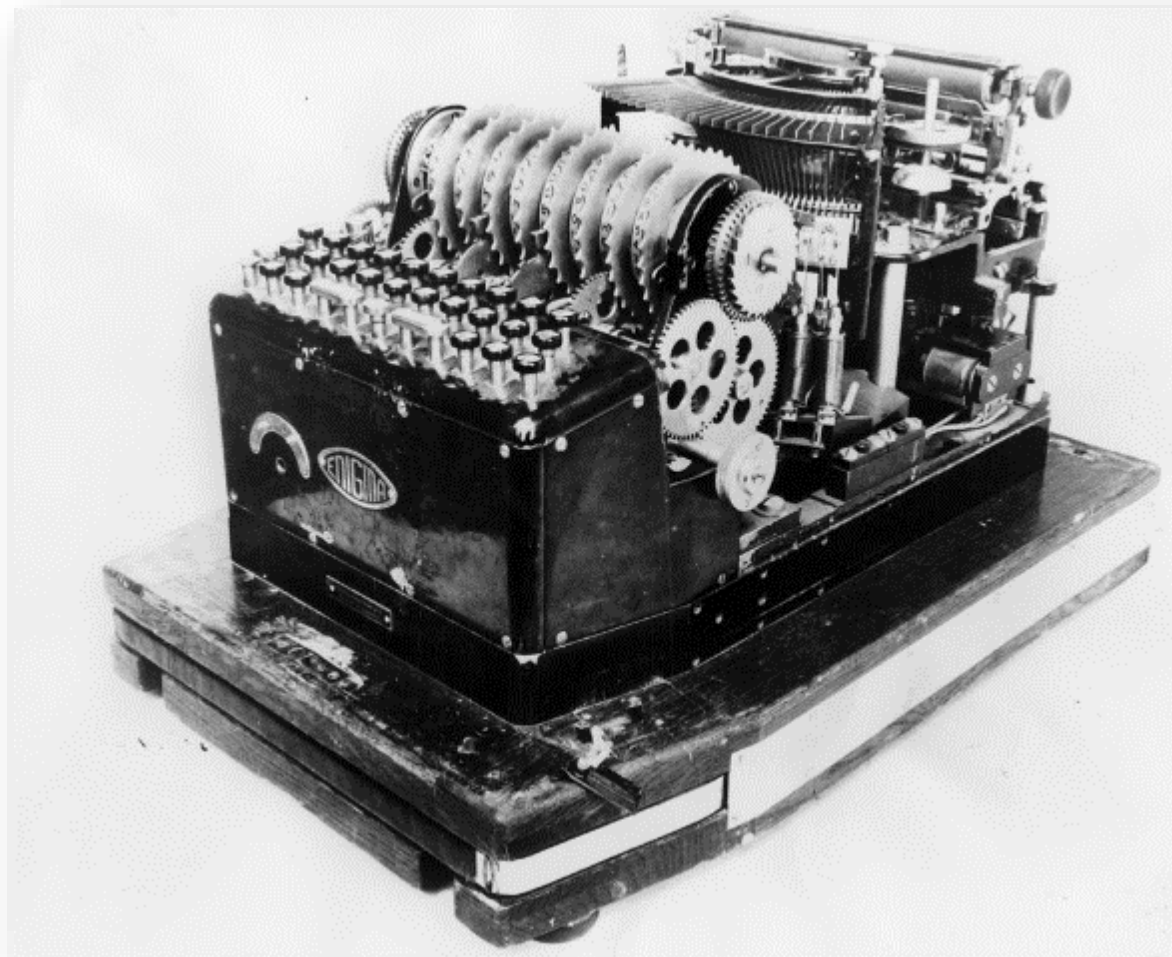
*Cryptographia ad usum Delphini – A. Zaccagnini*

- ***Enigma***
  - macchina elettromeccanica usata dai tedeschi nella seconda guerra mondiale.
- una serie di rotori effettuano la trasformazione di un carattere dell'alfabeto in un altro che veniva a sua volta trasformato dal rotore successivo
- dopo la digitazione di ogni carattere il primo rotore effettua una rotazione che può comportare la rotazione eventuale del successivo
- la scelta della posizione iniziale dei rotori (e di altri meccanismi di traslazione) costituisce la chiave
- ritenuta per molto tempo inattaccabile
- il matematico polacco Marin Rejewsky con il suo lavoro riuscì a decifrare numerosi messaggi militari tedeschi, un fattore che probabilmente contribuì alla vittoria finale degli alleati



# Enigma

A. Ferrari





- Data Encryption Standard (**DES**) è un algoritmo di cifratura scelto come standard per il governo degli Stati Uniti d'America nel 1976 e in seguito diventato di utilizzo internazionale
- si basa su un algoritmo a chiave **simmetrica** con chiave a 56 bit
- DES è considerato **insicuro** per moltissime applicazioni. La sua insicurezza deriva dalla chiave utilizzata per cifrare i messaggi, che è di soli 56 bit
- nel gennaio del 1999 si dimostrò pubblicamente la possibilità di individuare una chiave di crittazione in 22 ore e 15 minuti
- l'algoritmo è ritenuto sicuro reiterandolo 3 volte (Triple DES)
- DES è stato sostituito dall'Advanced Encryption Standard (AES) un nuovo algoritmo che elimina molti dei problemi del DES

# protocollo del doppio lucchetto

A. Ferrari

- A mette il suo messaggio per B in una scatola, che chiude con un lucchetto e invia a B.
- B mette il suo lucchetto alla scatola e la rispedisce ad A.
- A toglie il suo lucchetto e rispedisce la scatola a B.
- B toglie il suo lucchetto e legge il messaggio.
- la scatola non viaggia mai senza lucchetto
- ne A ne B ha dovuto inviare all'altro la chiave del proprio lucchetto
- è possibile comunicare con sicurezza senza dover effettuare un preventivo scambio delle chiavi !!!

