# Codici Segreti

Agostino Dovier

Dip di Matematica e Informatica, Univ. di Udine

*Ringrazio l'amico e maestro Andrea Sgarro per il materiale tratto dal suo meraviglioso quanto introvabile testo*

Gennaio 2013

# Codici Segreti

## Il festino di Baldassarre (Rembrandt)

# Codici Segreti

## La profezia di Daniele

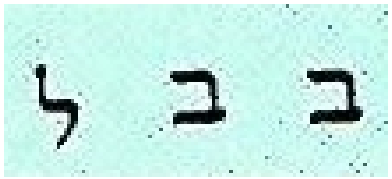
- MENE TEKEL PERES (mina, siclo, mezza mina: tre monete)
- Spiegazione nel V Libro del profeta Daniele:
  - ✓ Mene $\approx$ mnh (misurare)
  - ✓ Tekel $\approx$ tql (pesare)
  - ✓ Peres $\approx$ prs (dividere).
- Dio ha misurato il regno di Baldassarre e gli ha posto un termine, l'ha pesato sulla bilancia trovandolo mancante, il regno sta per essere diviso e consegnato ai Medi e ai Persiani.

- MENE TEKEL PERES (mina, siclo, mezza mina: tre monete)
- Spiegazione nel V Libro del profeta Daniele:
  - ✓ Mene $\approx$ mnh (misurare)
  - ✓ Tekel $\approx$ tql (pesare)
  - ✓ Peres $\approx$ prs (dividere).
- Dio ha misurato il regno di Baldassarre e gli ha posto un termine, l'ha pesato sulla bilancia trovandolo mancante, il regno sta per essere diviso e consegnato ai Medi e ai Persiani.

# Codici Segreti

## Atbash Ebraico (libro di Geremia) — sostituzione

| aleph | beth | gimel | daleth | he | waw | zayin | heth | teth | yod | kaph |
|---|---|---|---|---|---|---|---|---|---|---|
| א | ב | ג | ד | ה | ו | ז | ח | ט | י | כ |
| **taw** | **sin shin** | **resh** | **qoph** | **sadhe** | **pe** | **ayin** | **samkeh** | **nun** | **mem** | **lamed** |
| ת | ש | ר | ק | צ | פ | ע | ס | נ | מ | ל |



Babel/Babilonia

Sheschach

# Cifrari a sostituzione monoalfabetica

## Giulio Cesare (100–44 AC)

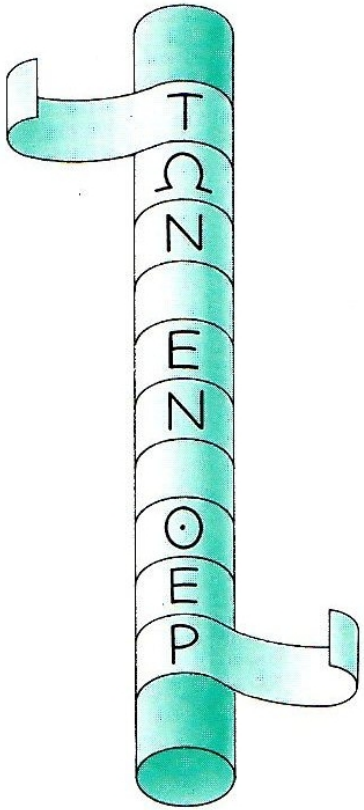
M A L I G N A N I

P D O M K Q D Q M

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

# Codici Segreti

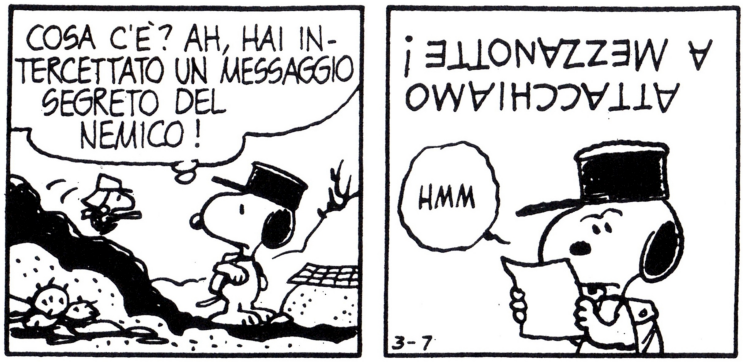
## Scitala spartana (≈ 400 AC) — trasposizione




| | | | | |
|---|---|---|---|---|
| Τ | Μ | Α | Κ | Α |
| Ω | Ο | Ν | Λ | |
| Ν | Π | Ο | Ε | Τ |
| | Υ | Ν | Η | Υ |
| Ε | Λ | Τ | Σ | Χ |
| Ν | Α | Ω | | Α |
| | Ι | Ν | Μ | |
| Θ | Σ | | Ε | |
| Ε | | Ε | Ν | |
| Ρ | Θ | Υ | | |

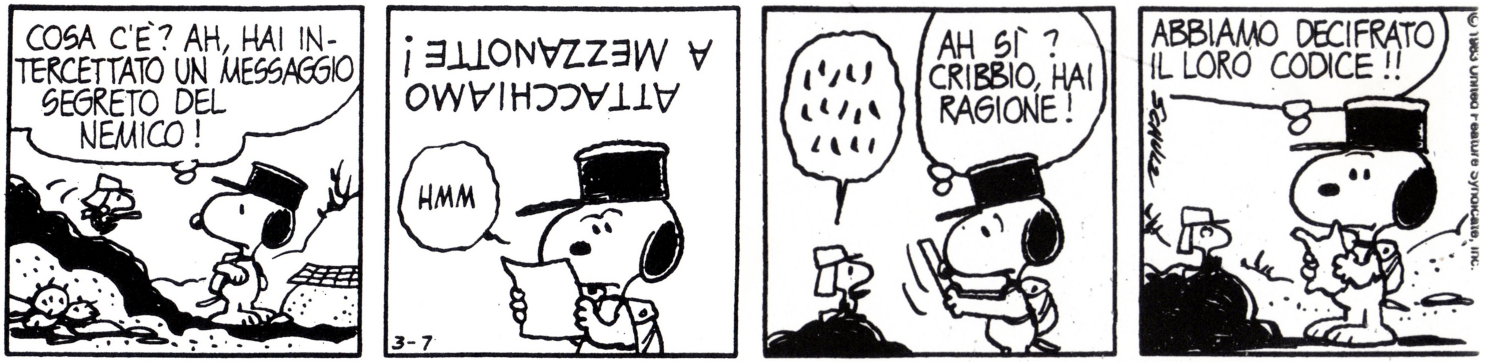
# Codici Segreti

## Altro codice a Trasposizione



# Codici Segreti

## Altro codice a Trasposizione



# Codici Segreti

## Steganografia (nascondere l'informazione)

- Scrivere in messaggio sotto la cera nuova delle tavolette di cera (block notes dell'epoca)
- Se non c'è fretta: radere i capelli, scrivere sul cuoio capelluto, attendere che ricrescano e inviare il messaggero col messaggio (Istiéo ad Aristagona di Mileto)
- Usare una miscela di allume e aceto per scrivere sul guscio d'uovo (sodo). Il messaggio si vedrà solo a uovo pelato (G.B. Della Porta)
- Inchiostri simpatici di vario tipo ...
- il messaggio non è cifrato, è solo nascosto. Se cade in mano del nemico viene compreso in poco tempo: non approfondiremo la steganografia!

# Codici Segreti

## Steganografia (nascondere l'informazione)

- Scrivere in messaggio sotto la cera nuova delle tavolette di cera (block notes dell'epoca)
- Se non c'è fretta: radere i capelli, scrivere sul cuoio capelluto, attendere che ricrescano e inviare il messaggero col messaggio (Istiéo ad Aristagona di Mileto)
- Usare una miscela di allume e aceto per scrivere sul guscio d'uovo (sodo). Il messaggio si vedrà solo a uovo pelato (G.B. Della Porta)
- Inchiostri simpatici di vario tipo . . .
- il messaggio non è cifrato, è solo nascosto. Se cade in mano del nemico viene compreso in poco tempo: non approfondiremo la steganografia!

# Codici Segreti

## Mary Stuart (1542–1587)

- Regina di Scozia (dall'età di nove mesi), con vita parecchio travagliata,
- usò un nomenclatore per corrispondere con gli alleati francesi per cospirare contro l'Inghilterra.
- I crittografi di corte inglesi decrittarono i messaggi.
- Finì male.

# Codici Segreti

## Il telegramma Zimmerman (1917)

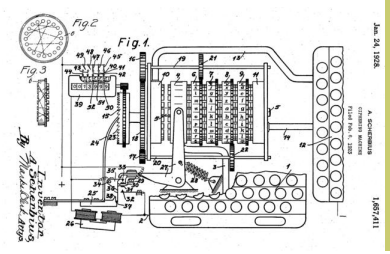
I servizi segreti inglesi intercettano un telegramma cifrato del ministro tedesco Zimmermann all'ambasciatore tedesco a Washington. Fu decrittato ma non volevano far sapere che erano in grado di farlo.

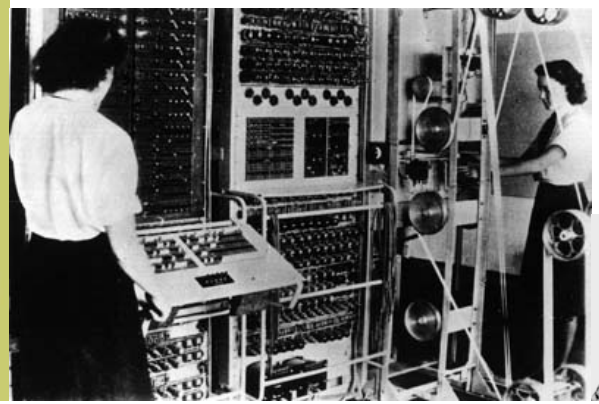

- Il telegramma ripartì da Washington per il Messico
- Fu decrittato anche quello.
- Si proponeva alleanza con Messico offrendo in cambio territori del Texas, New Mexico e Arizona.
- Gli USA furono costretti ad entrare nella I guerra mondiale.

# CODICI SEGRETI

## ENIGMA

Durante la seconda guerra mondiale la macchina da cifra denominata ENIGMA (Arthur Scherbius 1878–1929) fu uno dei punti di forza dell'esercito tedesco.



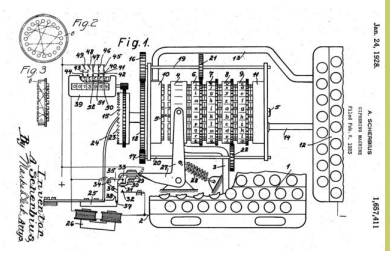


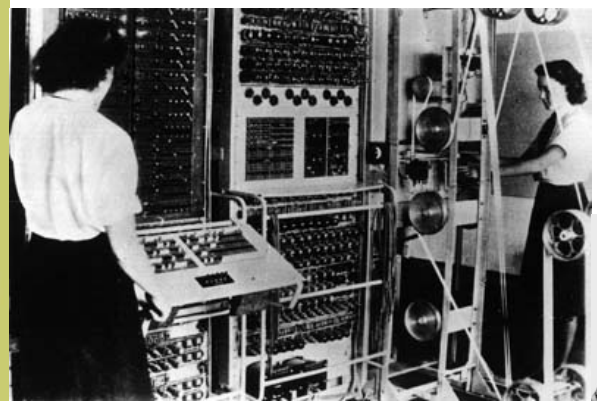
Il controspionaggio britannico coordinato da Alan M. Turing (1912–1954) a Bletchley Park lo riuscì a forzare invertendo le sorti del conflitto. Furono usate delle macchine elettromeccaniche (BOMBE) e fu progettato il primo calcolatore elettronico a valvole (COLOSSUS)

# Codici Segreti

## ENIGMA

Durante la seconda guerra mondiale la macchina da cifra denominata ENIGMA (Arthur Scherbius 1878–1929) fu uno dei punti di forza dell'esercito tedesco.



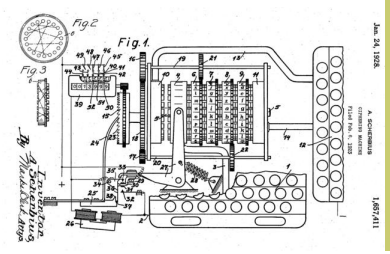


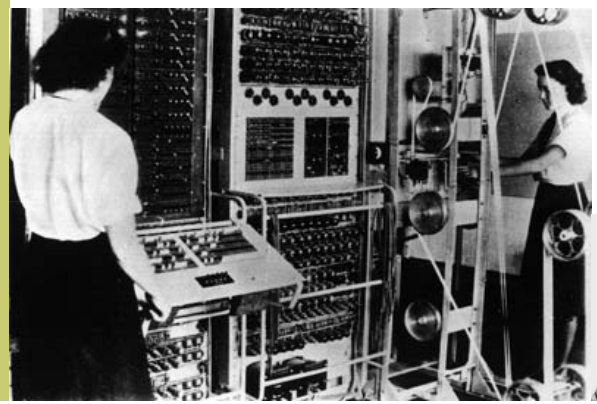
Il controspionaggio britannico coordinato da Alan M. Turing (1912–1954) a Bletchley Park lo riuscì a forzare invertendo le sorti del conflitto. Furono usate delle macchine elettromeccaniche (BOMBE) e fu progettato il primo calcolatore elettronico a valvole (COLOSSUS)

# Codici Segreti

## ENIGMA

Durante la seconda guerra mondiale la macchina da cifra denominata ENIGMA (Arthur Scherbius 1878–1929) fu uno dei punti di forza dell'esercito tedesco.



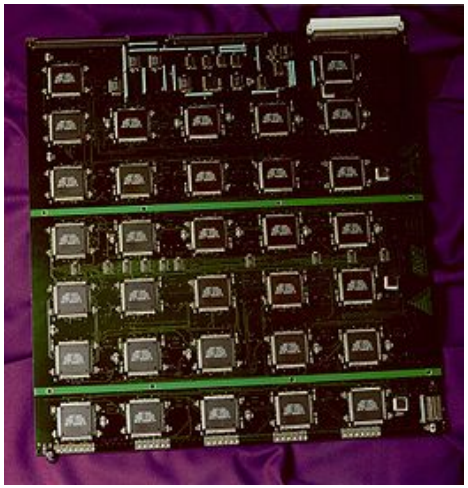


Il controspionaggio britannico coordinato da Alan M. Turing (1912–1954) a Bletchley Park lo riuscì a forzare invertendo le sorti del conflitto. Furono usate delle macchine elettromeccaniche (BOMBE) e fu progettato il primo calcolatore elettronico a valvole (COLOSSUS)

# Codici Segreti

## Data Encription Standard (DES)

Negli anni ’70 viene pubblicato il DES come standard per la crittografia. Per la prima volta viene fornito liberamente al crittografo l’algoritmo usato per la cifra (ma non la chiave). Combina sostituzione e trasposizione.

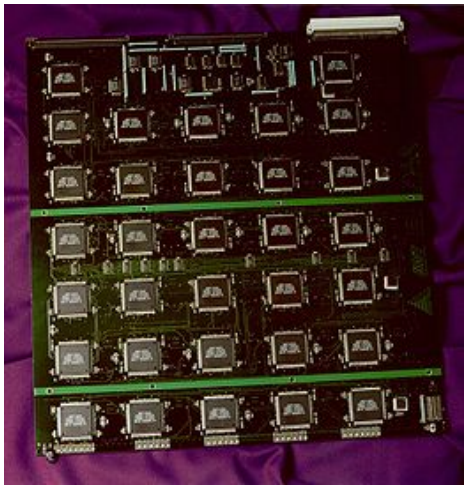


Nel 1996 il DES è violato, nel 1997 (progetto DESCHALL) è violato in pubblico, nel 1998 Il DES cracker dell’EFF (Deep Crack—250K$) viola una chiave DES in 56 ore.

# Codici Segreti

## Data Encription Standard (DES)

Negli anni ’70 viene pubblicato il DES come standard per la crittografia. Per la prima volta viene fornito liberamente al crittografo l’algoritmo usato per la cifra (ma non la chiave). Combina sostituzione e trasposizione.



Nel 1996 il DES è violato, nel 1997 (progetto DESCHALL) è violato in pubblico, nel 1998 Il DES cracker dell’EFF (Deep Crack—250K$) viola una chiave DES in 56 ore.

# Codici Segreti

## AES, RSA, PGP, ...

- Il DES fu sostituito dall'AES (sempre sostituzione e trasposizione)
- Nacque l'idea della crittografia a chiave pubblica (RSA)
- Le due tecnologie si combinano (PGP)
- A novembre 2010 Wikileaks dichiara di avere milioni di file riservati e inizia la loro pubblicazione in rete.


- ...

# Codici Segreti

## Terminologia

- Il testo in chiaro o messaggio viene trasformato in un
- testo in cifra o crittogramma
- Tale operazione si dice cifratura
- La decifrazione o decifratura è l'operazione legittima, facile per il destinatario desiderato.
- La spia che intercetta il crittogramma e vuole decifrarlo opera (se ci riesce) una decrittazione
- Similmente ci sono termini diversi per la crittografia (parte costruttiva), per la crittanalisi (parte distruttiva), e per la crittologia (disciplina complessiva).
- Spesso si usa comunque crittografia come sinonimo di crittologia.

# Codici Segreti

## Terminologia

- Il testo in chiaro o messaggio viene trasformato in un
- testo in cifra o crittogramma
- Tale operazione si dice cifratura
- La decifrazione o decifratura è l'operazione legittima, facile per il destinatario desiderato.
- La spia che intercetta il crittogramma e vuole decifrarlo opera (se ci riesce) una decrittazione
- Similmente ci sono termini diversi per la crittografia (parte costruttiva), per la crittanalisi (parte distruttiva), e per la crittologia (disciplina complessiva).
- Spesso si usa comunque crittografia come sinonimo di crittologia.

# Codici Segreti

## Terminologia

- Il testo in chiaro o messaggio viene trasformato in un
- testo in cifra o crittogramma
- Tale operazione si dice cifratura
- La decifrazione o decifratura è l'operazione legittima, facile per il destinatario desiderato.
- La spia che intercetta il crittogramma e vuole decifrarlo opera (se ci riesce) una decrittazione
- Similmente ci sono termini diversi per la crittografia (parte costruttiva), per la crittanalisi (parte distruttiva), e per la crittologia (disciplina complessiva).
- Spesso si usa comunque crittografia come sinonimo di crittologia.

# Codici Segreti

## Il principio di Kerckhoffs

- Auguste Kerchoffs von Nieuvenhof (1835–1903)
- Scrive La cryptographie militaire (1883)
- Illustra differenza tra crittografia di tipo tattico (basta che il segreto duri qualche ora o giorno) e strategico (meglio se per sempre)
- Enuncia il principio: *La sicurezza di un sistema strategico è affidata interamente o comunque essenzialmente alla segretezza della chiave*
- Dobbiamo assumere che il nemico conosca il tipo di cifrario impiegato (se non lo sa, meglio).
- La crittografia moderna (da DES in poi) l'ha preso come dogma.

# Cifrari a sostituzione monoalfabetica

## Giulio Cesare (100–44 AC)

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

# Cifrari a sostituzione monoalfabetica

- L'operazione di cifratura avviene mediante l'applicazione di una sostituzione di lettere.
- Vi è dunque una funzione biiettiva

$$f : \{A, \ldots, Z\} \longrightarrow \{A, \ldots, Z\}$$

- Essendo biiettiva, è invertibile, ovvero esiste $f^{-1}$ tale che $f^{-1}(f(x)) = x$ per ogni $x \in \{A, \ldots, Z\}$.
- Per la cifratura si usa $f$.
- Per la decifratura si usa $f^{-1}$, nota al legittimo destinatario ma non alla spia.
- La spia, ammettendo conosca il sistema di cifratura usato deve "indovinare" $f^{-1}$ (in questo caso va bene anche $f$).
- Nel caso del cifrario di Cesare, ci sono solo 21 (anzi 20) funzioni possibili (chiave: lettera iniziale).

# Cifrari a sostituzione monoalfabetica

- L'operazione di cifratura avviene mediante l'applicazione di una sostituzione di lettere.
- Vi è dunque una funzione biiettiva

$$f : \{A, \ldots, Z\} \longrightarrow \{A, \ldots, Z\}$$

- Essendo biiettiva, è invertibile, ovvero esiste $f^{-1}$ tale che $f^{-1}(f(x)) = x$ per ogni $x \in \{A, \ldots, Z\}$.
- Per la cifratura si usa $f$.
- Per la decifratura si usa $f^{-1}$, nota al legittimo destinatario ma non alla spia.
- La spia, ammettendo conosca il sistema di cifratura usato deve "indovinare" $f^{-1}$ (in questo caso va bene anche $f$).
- Nel caso del cifrario di Cesare, ci sono solo 21 (anzi 20) funzioni possibili (chiave: lettera iniziale).

# Cifrari a sostituzione monoalfabetica

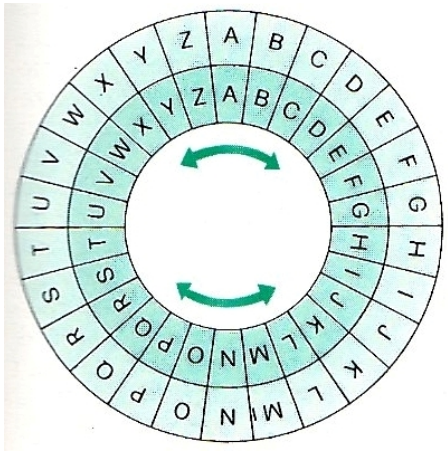
- L'operazione di cifratura avviene mediante l'applicazione di una sostituzione di lettere.
- Vi è dunque una funzione biiettiva

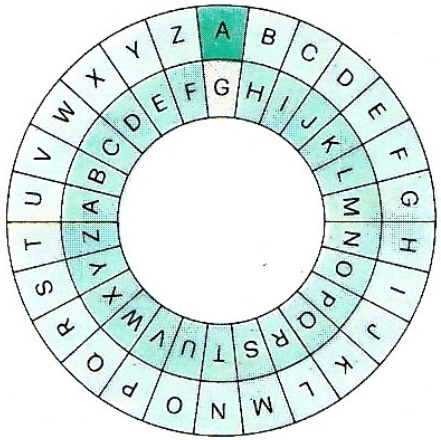
$$f : \{A, \ldots, Z\} \longrightarrow \{A, \ldots, Z\}$$

- Essendo biiettiva, è invertibile, ovvero esiste $f^{-1}$ tale che $f^{-1}(f(x)) = x$ per ogni $x \in \{A, \ldots, Z\}$.
- Per la cifratura si usa $f$.
- Per la decifratura si usa $f^{-1}$, nota al legittimo destinatario ma non alla spia.
- La spia, ammettendo conosca il sistema di cifratura usato deve "indovinare" $f^{-1}$ (in questo caso va bene anche $f$).
- Nel caso del cifrario di Cesare, ci sono solo 21 (anzi 20) funzioni possibili (chiave: lettera iniziale).

# Cifrari a sostituzione monoalfabetica

## Leon Battista Alberti (1404–1472)



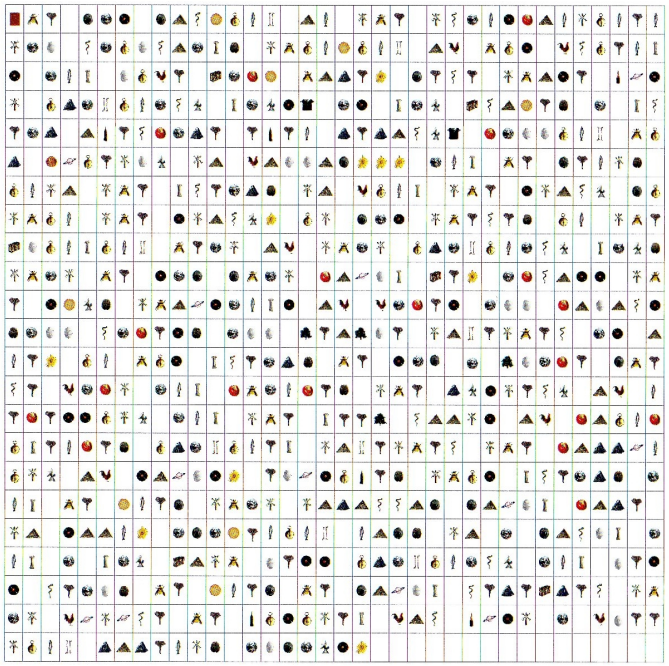


# Cifrari a sostituzione monoalfabetica

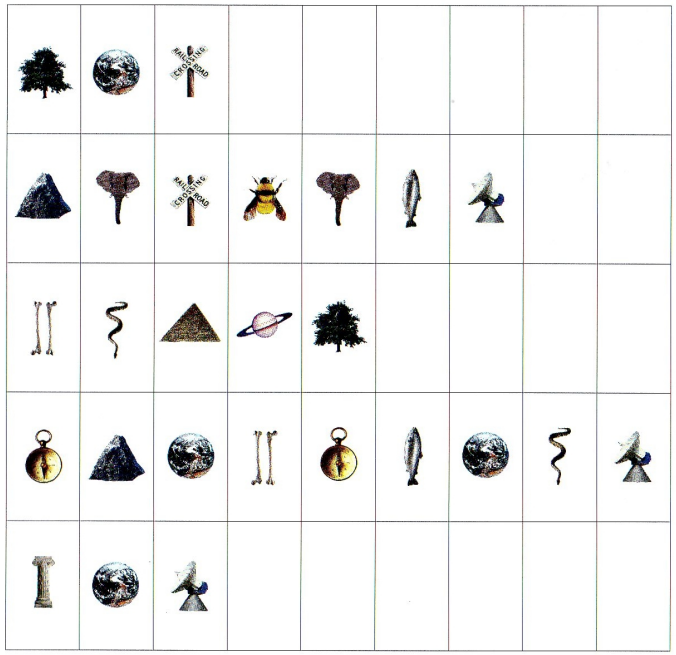
## Giovan Battista Della Porta (1535–1615)

# Codici Segreti

## Pat Metheny (1997)



9 46791-2

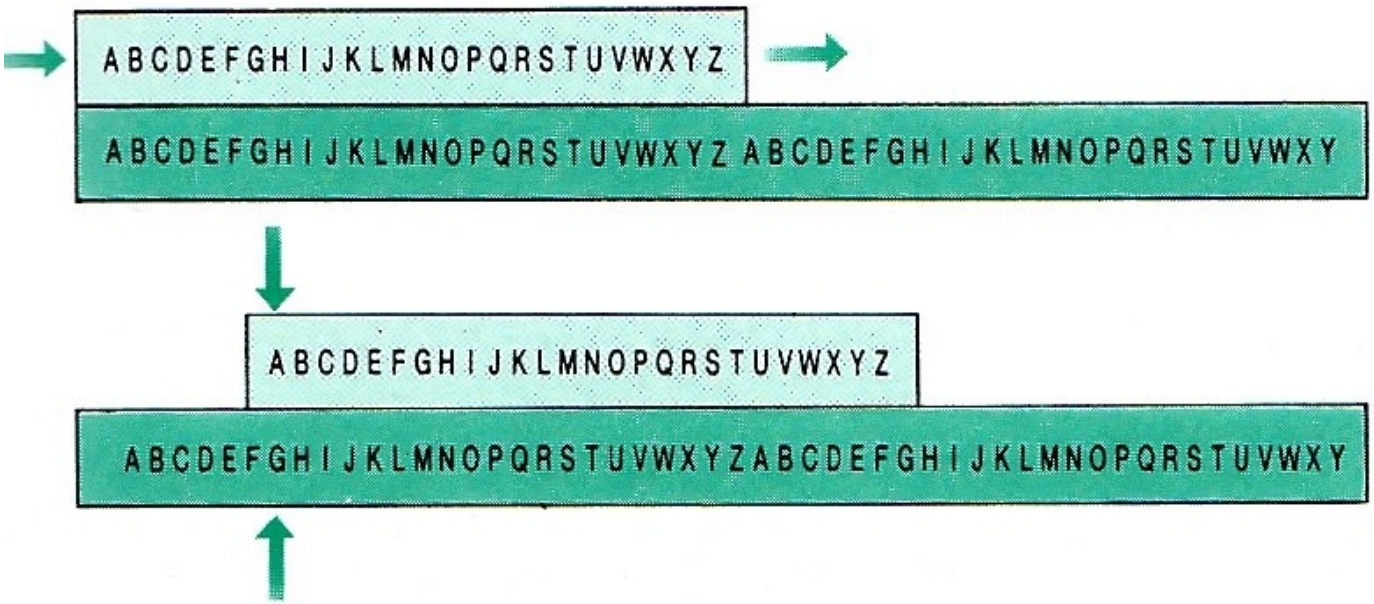


# Codici Segreti

## Pat Metheny (1997)

# Cifrari a sostituzione monoalfabetica

## Il regolo di Saint Cyr



# Cifrari a sostituzione monoalfabetici

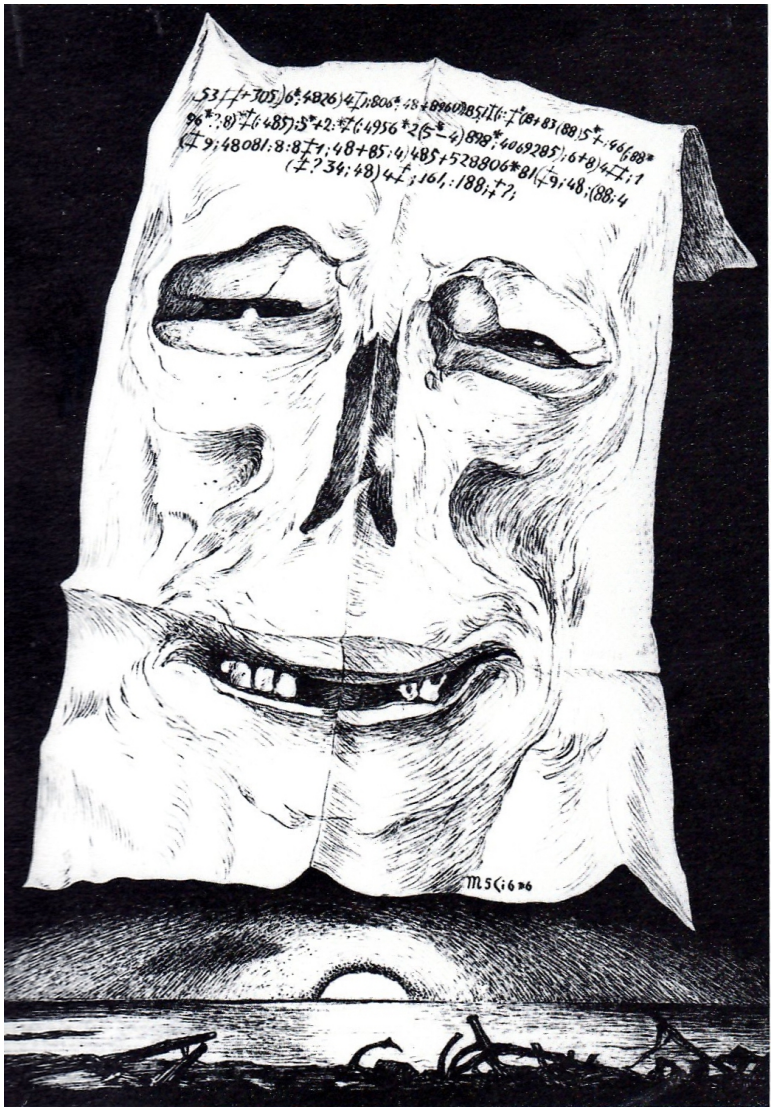
## Cifrari completi

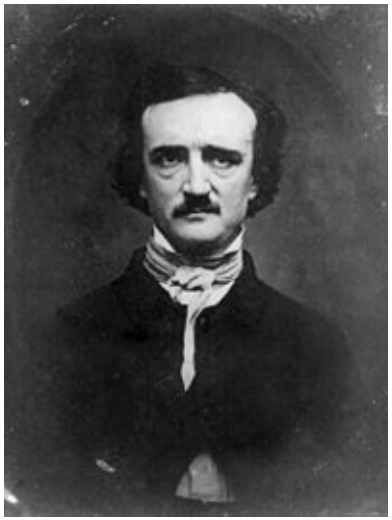
- Con dischi e regoli possiamo rappresentare qualunque permutazione di $\{A, \ldots, Z\}$.
- Le funzioni possibili diventano 21! (in realtà un po' meno ... non vogliamo troppe identità...)
- La chiave è l'intera permutazione delle lettere dell'alfabeto.
- Ma cominciano a diventare numeri pesanti per la forza bruta.

- Con dischi e regoli possiamo rappresentare qualunque permutazione di $\{A, \ldots, Z\}$.
- Le funzioni possibili diventano 21! (in realtà un po' meno ... non vogliamo troppe identità...)
- La chiave è l'intera permutazione delle lettere dell'alfabeto.
- Ma cominciano a diventare numeri pesanti per la forza bruta.

# Cifrari a sostituzione monoalfabetica

## Lo scarabeo d'oro (E. A. Poe)





# Cifrari a sostituzione monoalfabetica

## Decrittazione

- (demo)
- Si calcolano le frequenze dei simboli nel crittogramma.
- Si comparano con le frequenze tipiche della lingua in cui ci aspettiamo sia scritto il messaggio.
- La tecnica è detta di statistica linguistica.
- Non si trova subito la sostituzione completa ma con un po' di tentativi iniziamo a intuire qualche parola e si completa la sostituzione usando la semantica.

# Cifrari a sostituzione monoalfabetica

## Decrittazione

- (demo)
- Si calcolano le frequenze dei simboli nel crittogramma.
- Si comparano con le frequenze tipiche della lingua in cui ci aspettiamo sia scritto il messaggio.
- La tecnica è detta di statistica linguistica.
- Non si trova subito la sostituzione completa ma con un po' di tentativi iniziamo a intuire qualche parola e si completa la sostituzione usando la semantica.

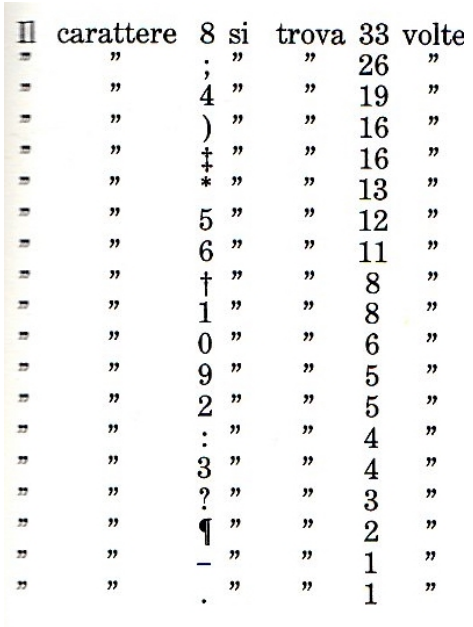
# Cifrari a sostituzione monoalfabetica

## Decrittazione

- (demo)
- Si calcolano le frequenze dei simboli nel crittogramma.
- Si comparano con le frequenze tipiche della lingua in cui ci aspettiamo sia scritto il messaggio.
- La tecnica è detta di statistica linguistica.
- Non si trova subito la sostituzione completa ma con un po' di tentativi iniziamo a intuire qualche parola e si completa la sostituzione usando la semantica.

# Cifrari a sostituzione monoalfabetica

## Decrittazione (Scarabeo d'oro)

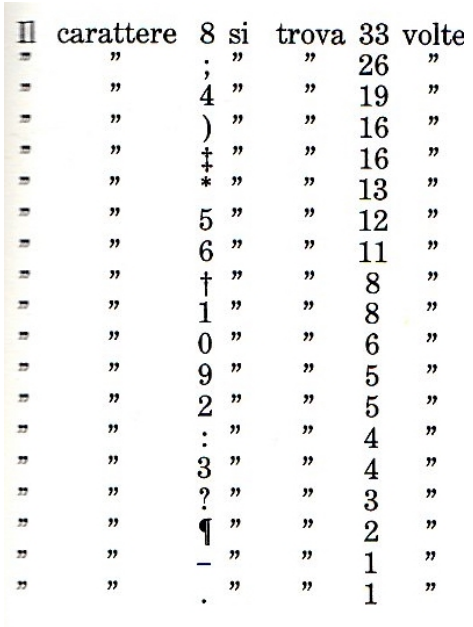


Il carattere 8 si trova 33 volte
= " ; " " 26 "
= " 4 " " 19 "
= " ) " " 16 "
= " ‡ " " 16 "
= " * " " 13 "
= " 5 " " 12 "
= " 6 " " 11 "
= " † " " 8 "
= " 1 " " 8 "
= " 0 " " 6 "
= " 9 " " 5 "
= " 2 " " 5 "
= " : " " 4 "
= " 3 " " 4 "
= " ? " " 3 "
= " ¶ " " 2 "
= " – " " 1 "
= " . " " 1 "

Eccezioni: *Gadsby* (E. W. Wright), *La disparition* (G. Perec) tradotto in *A void* (G. Adair). Tutti senza lettera e. Il crittogramma con la mappa del tesoro ha anche una versione reale: il crittogramma di Beale (ancora in parte irrisolto)

# Cifrari a sostituzione monoalfabetica

## Decrittazione (Scarabeo d'oro)



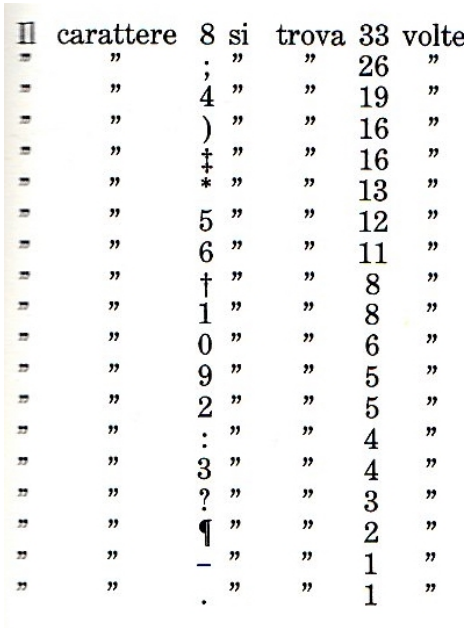
Il carattere 8 si trova 33 volte
= " ; " " 26 "
= " 4 " " 19 "
= " ) " " 16 "
= " ‡ " " 16 "
= " * " " 13 "
= " 5 " " 12 "
= " 6 " " 11 "
= " † " " 8 "
= " 1 " " 8 "
= " 0 " " 6 "
= " 9 " " 5 "
= " 2 " " 5 "
= " : " " 4 "
= " 3 " " 4 "
= " ? " " 3 "
= " ¶ " " 2 "
= " – " " 1 "
= " . " " 1 "

Eccezioni: *Gadsby* (E. W. Wright), *La disparition* (G. Perec) tradotto in *A void* (G. Adair). Tutti senza lettera e.

Il crittogramma con la mappa del tesoro ha anche una versione reale: il crittogramma di Beale (ancora in parte irrisolto)

# Cifrari a sostituzione monoalfabetica

## Decrittazione (Scarabeo d'oro)



Il carattere 8 si trova 33 volte
= " ; " " 26 "
= " 4 " " 19 "
= " ) " " 16 "
= " ‡ " " 16 "
= " * " " 13 "
= " 5 " " 12 "
= " 6 " " 11 "
= " † " " 8 "
= " 1 " " 8 "
= " 0 " " 6 "
= " 9 " " 5 "
= " 2 " " 5 "
= " : " " 4 "
" " 3 " " 4 "
" " ? " " 3 "
" " ¶ " " 2 "
" " – " " 1 "
" " . " " 1 "

Eccezioni: *Gadsby* (E. W. Wright), *La disparition* (G. Perec) tradotto in *A void* (G. Adair). Tutti senza lettera e. Il crittogramma con la mappa del tesoro ha anche una versione reale: il crittogramma di Beale (ancora in parte irrisolto)

# Confondere la statistica

## Francesco Bacone (1561–1626)

- Codifica binaria (5 bits dell'ASCII):
  $A \mapsto 00001$,
  $B \mapsto 00010$,
  $C \mapsto 00011, \ldots$
- Testo di copertura:
  IO NON DICO PAROLACCE
  QUANDO PARLO IN AULA
- Messaggio in chiaro: CRIBBIO

| C | R | I | B | B | I | O |
|---|---|---|---|---|---|---|
| 00011 | 10101 | 01001 | 00010 | 00010 | 01001 | 01111 |
| IONON | DICOP | AROLA | CCEQU | ANDOP | ARLOI | NAULA |

Crittogramma:

| IONon | dIcOp | ArOLa | CCEqU | ANDoP | ArLOi | Naula |
|---|---|---|---|---|---|---|

# Confondere la statistica

## Cifrari Omofonici

- Per confondere la statistica si inseriscono nel testo in chiaro prima della codifica le "nulle" ovvero lettere a bassa probabilità in posti casuali (una ogni tanto, che non pregiudicano la comprensione)
- Ad ogni lettera molto probabile (p.es. le vocali) venogono associati più nomi, per esempio:

$$e \mapsto \{i, \clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$$

  alternadole mediante lancio di monete.
- Il cifrario comincia ad essere robusto . . .

# Confondere la statistica

## Nomenclatori (omofonici)


Poi potevano essere ulteriormente cifrati.

# Confondere la statistica

## Testo ausiliario

*C'era una volta, tanto tempo fa, una principessa che non voleva uscire di casa per far le compere ma ordinare tutto senza alzarsi dalla scrivania utilizzando la connessione wifi a bassa protezione in hotel.*

Allora, il testo "attacchiamo" può essere cifrato con:

*24 6 5 31 19 1 35 34 24 20 21*

*n* indica l'iniziale della parola *n*-esima del testo.
Se non si conosce il testo chiave, e si evitano le ripetizioni, è un buon sistema.

Il secondo crittogramma di Beale è stato cifrato con questa tecnica, usando la dichiarazione d'indipendenza degli stati uniti (parole numerate da 1 a 1322).

# Confondere la statistica

## Testo ausiliario

*C'era una volta, tanto tempo fa, una principessa che non voleva uscire di casa per far le compere ma ordinare tutto senza alzarsi dalla scrivania utilizzando la connessione wifi a bassa protezione in hotel.*

Allora, il testo "attacchiamo" può essere cifrato con:

*24 6 5 31 19 1 35 34 24 20 21*

*n* indica l'iniziale della parola *n*-esima del testo.
Se non si conosce il testo chiave, e si evitano le ripetizioni, è un buon sistema.

Il secondo crittogramma di Beale è stato cifrato con questa tecnica, usando la dichiarazione d'indipendenza degli stati uniti (parole numerate da 1 a 1322).

# Confondere la statistica

## Testo ausiliario

*C'era una volta, tanto tempo fa, una principessa che non voleva uscire di casa per far le compere ma ordinare tutto senza alzarsi dalla scrivania utilizzando la connessione wifi a bassa protezione in hotel.*

Allora, il testo "attacchiamo" può essere cifrato con:

*24 6 5 31 19 1 35 34 24 20 21*

*n* indica l'iniziale della parola *n*-esima del testo.
Se non si conosce il testo chiave, e si evitano le ripetizioni, è un buon sistema.

Il secondo crittogramma di Beale è stato cifrato con questa tecnica, usando la dichiarazione d'indipendenza degli stati uniti (parole numerate da 1 a 1322).

# Confondere la statistica

## Testo ausiliario

*C'era una volta, tanto tempo fa, una principessa che non voleva uscire di casa per far le compere ma ordinare tutto senza alzarsi dalla scrivania utilizzando la connessione wifi a bassa protezione in hotel.*

Allora, il testo "attacchiamo" può essere cifrato con:

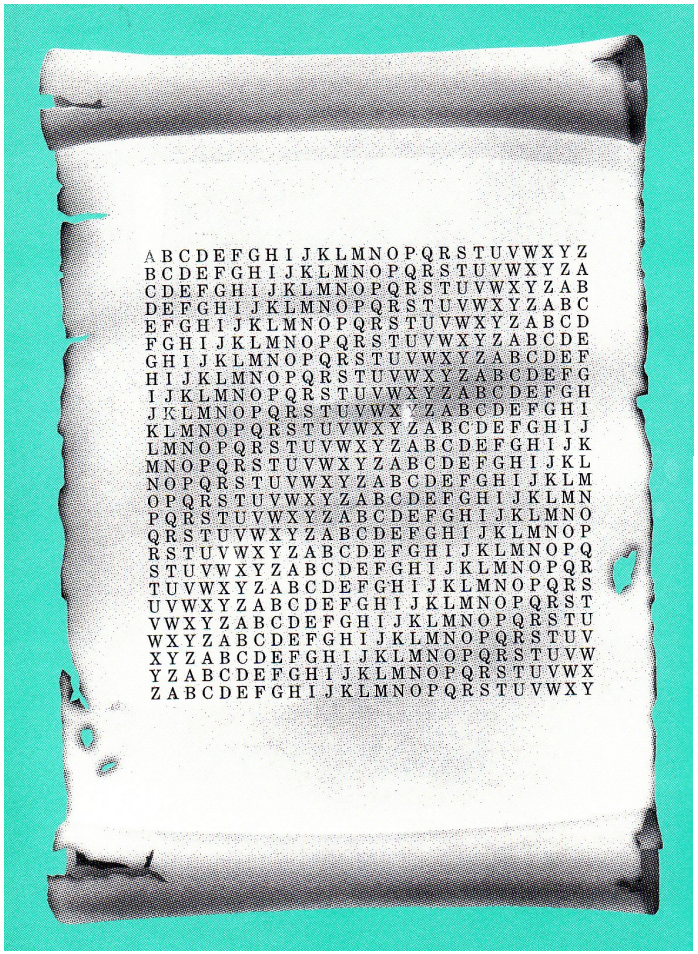
*24 6 5 31 19 1 35 34 24 20 21*

*n* indica l'iniziale della parola *n*-esima del testo.
Se non si conosce il testo chiave, e si evitano le ripetizioni, è un buon sistema.

Il secondo crittogramma di Beale è stato cifrato con questa tecnica, usando la dichiarazione d'indipendenza degli stati uniti (parole numerate da 1 a 1322).

# Cifrari a sostituzione polialfabetica

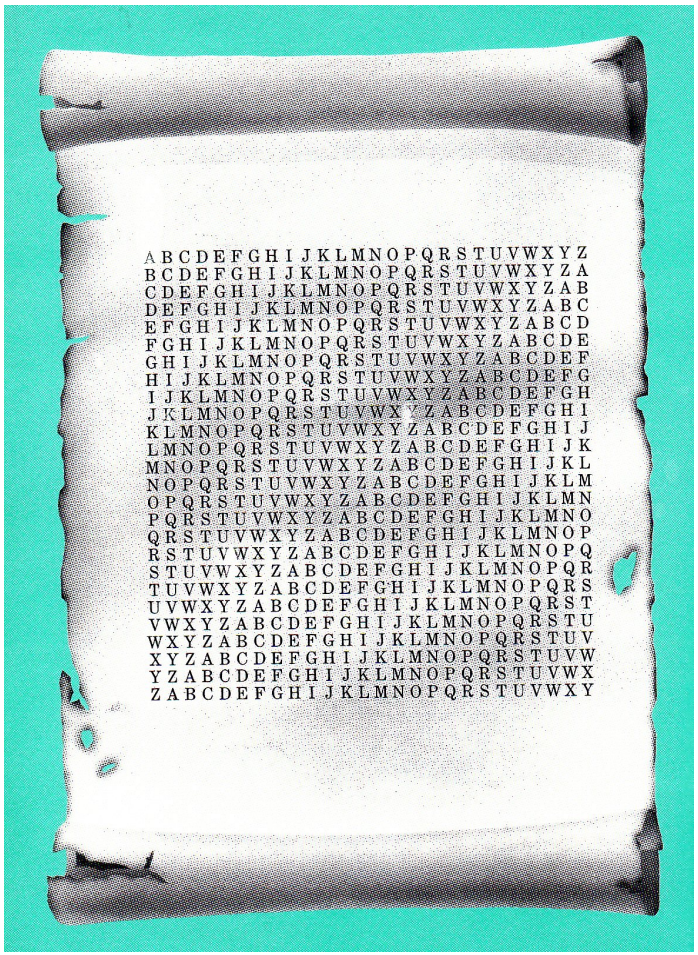
## Blaise de Vigenère (1523–1596)




# Cifrari a sostituzione polialfabetica

## Cifrazione

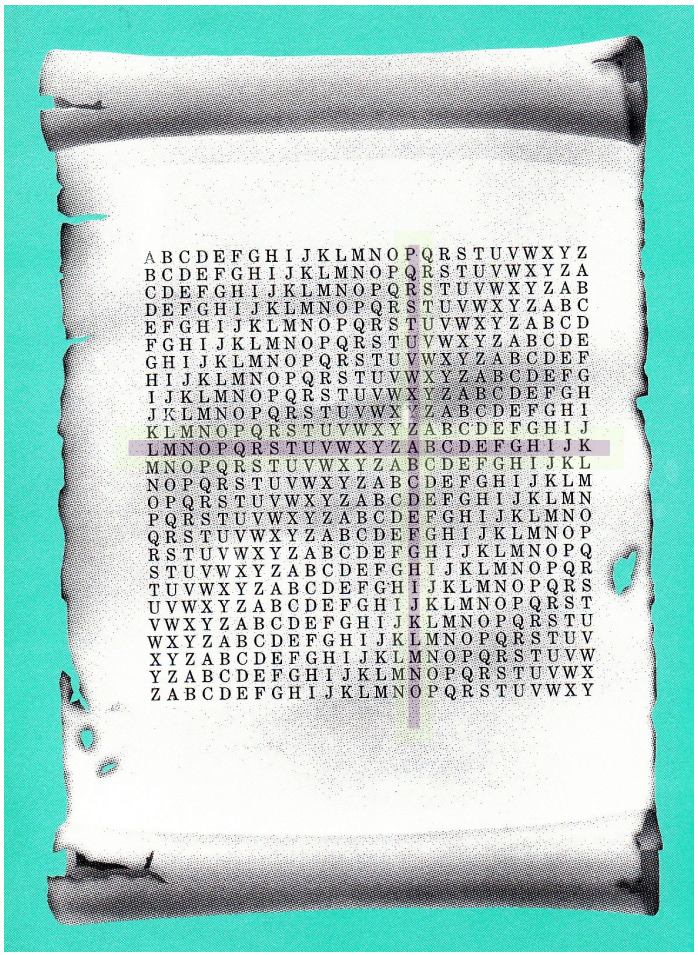
| P | A | R | I | S | V | A | U | T | B | I | E | N | U | N | E | M | E | S | S | E |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| L | O | U | P | L | O | U | P | L | O | U | P | L | O | U | P | L | O | U | P | L |



# Cifrari a sostituzione polialfabetica

## Cifrazione

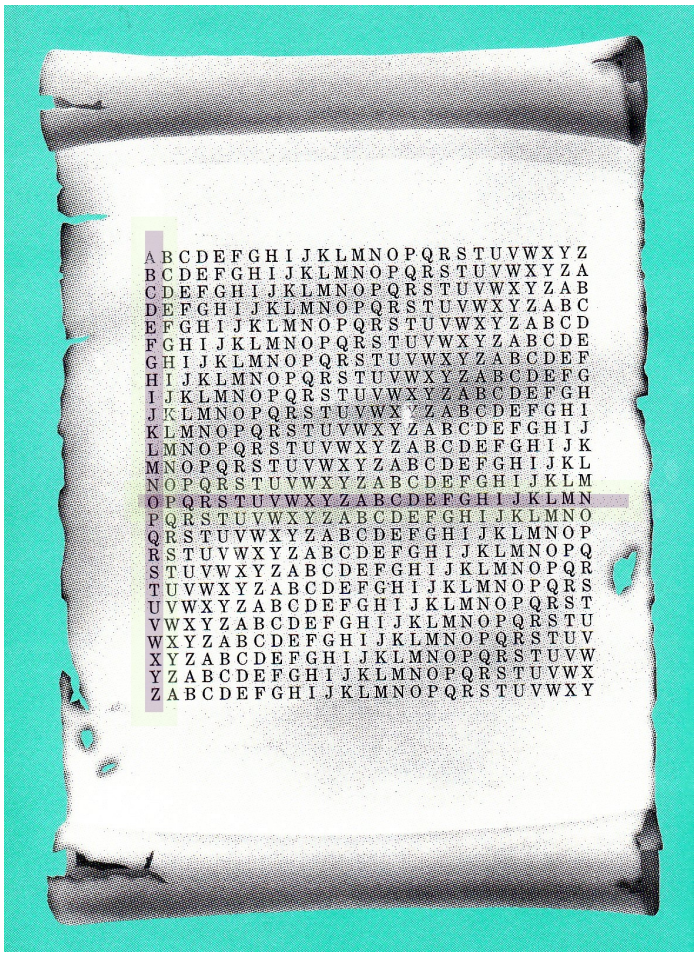
| P | A | R | I | S | V | A | U | T | B | I | E | N | U | N | E | M | E | S | S | E |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| L | O | U | P | L | O | U | P | L | O | U | P | L | O | U | P | L | O | U | P | L |



# Cifrari a sostituzione polialfabetica

## Cifrazione

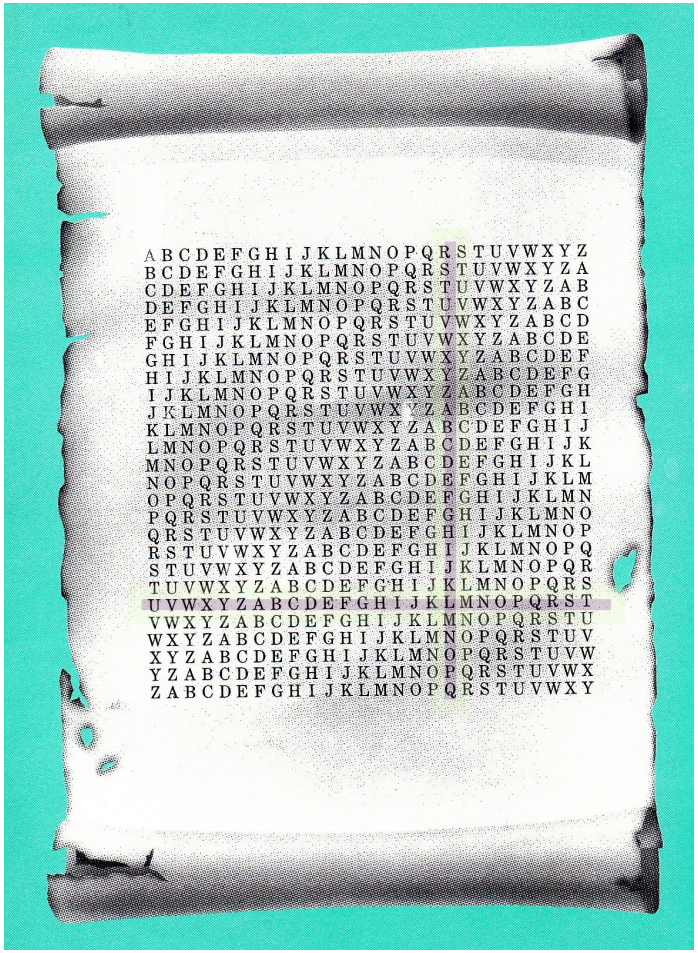
| P | A | R | I | S | V | A | U | T | B | I | E | N | U | N | E | M | E | S | S | E |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| L | O | U | P | L | O | U | P | L | O | U | P | L | O | U | P | L | O | U | P | L |



# Cifrari a sostituzione polialfabetica

## Cifrazione

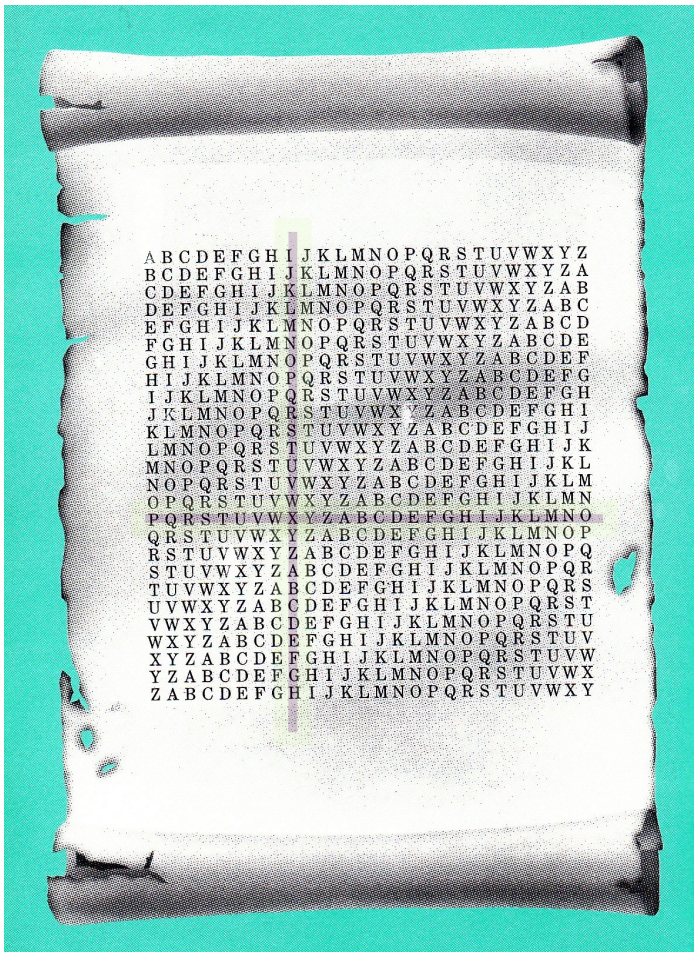
| P | A | R | I | S | V | A | U | T | B | I | E | N | U | N | E | M | E | S | S | E |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| L | O | U | P | L | O | U | P | L | O | U | P | L | O | U | P | L | O | U | P | L |



# Cifrari a sostituzione polialfabetica

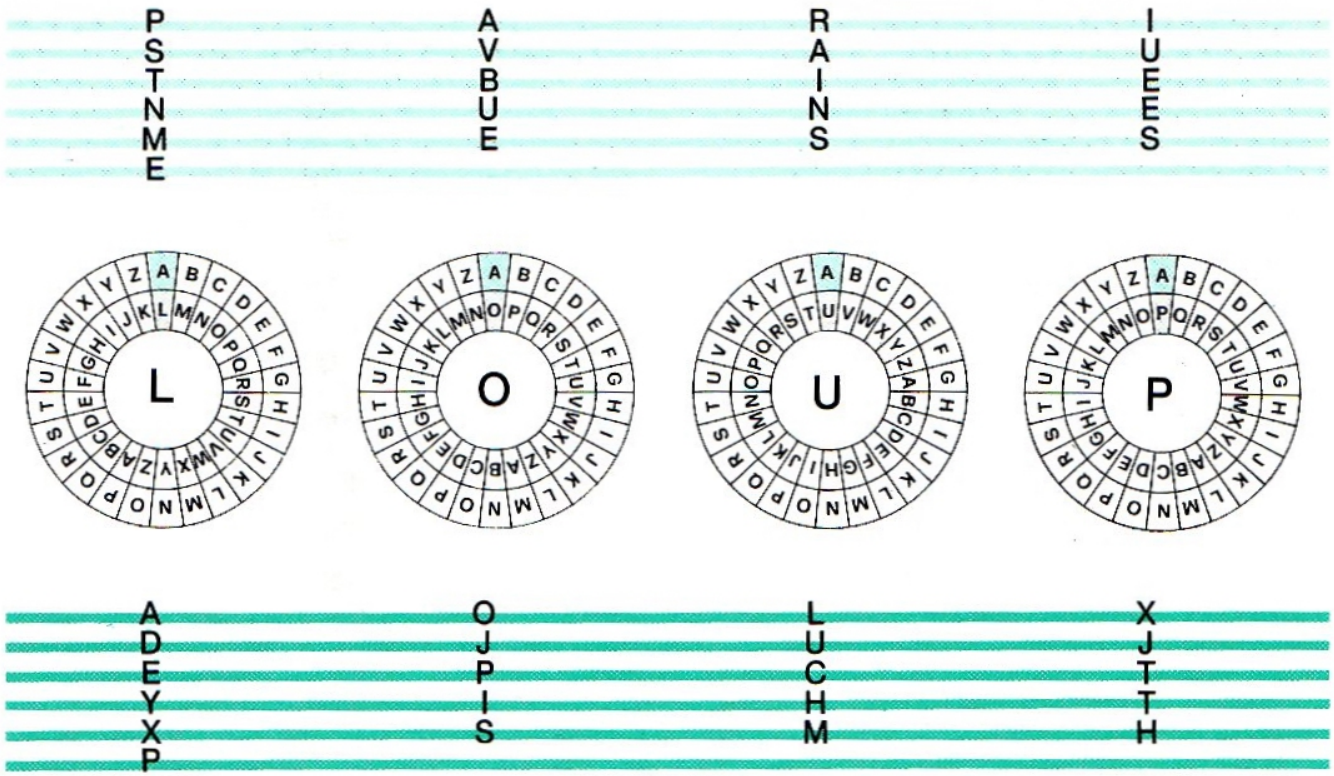
## Cifrazione

| P | A | R | I | S | V | A | U | T | B | I | E | N | U | N | E | M | E | S | S | E |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| L | O | U | P | L | O | U | P | L | O | U | P | L | O | U | P | L | O | U | P | L |



# Cifrari a sostituzione polialfabetica

## Cifrazione



# Cifrari a sostituzione polialfabetica

- E' come se ci fossero più cifrari monoalfabetici del tipo di cesare, tanti quanti la lunghezza della chiave.
- Se la chiave è lunga $n$, in fondo è come avere una funzione biiettiva

$$f : \{A, \ldots, Z\}^n \longrightarrow \{A, \ldots, Z\}^n$$

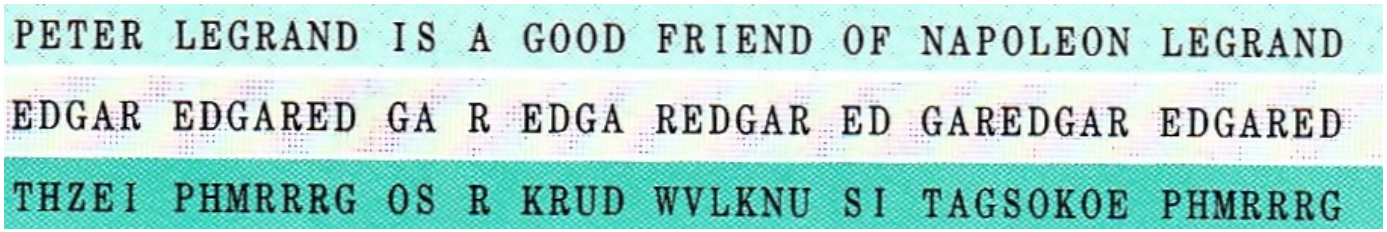
- Anche se su ogni lettera della chiave ci sono solo 21 scelte, in tutto ce ne sono ben $21^n$.
- Inoltre la statistica sembra ingannata.
- E la spia non conosce nemmeno $n$.

# Cifrari a sostituzione polialfabetica

## Friedrich Kasiski (1805–1881): decrittatura (Babbage?)

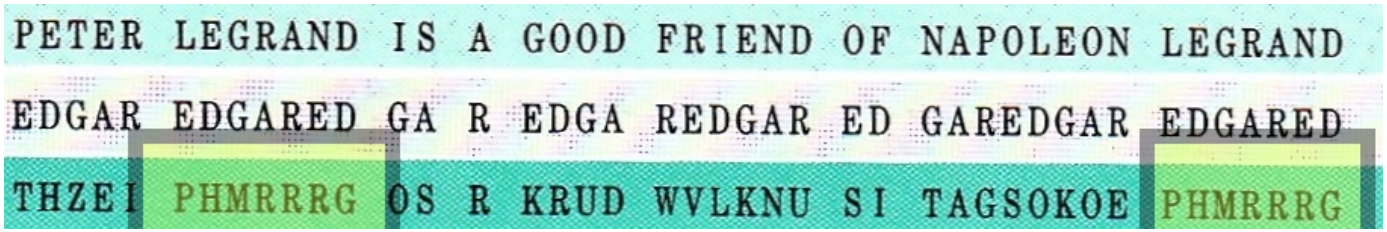
# Cifrari a sostituzione polialfabetica

## Friedrich Kasiski (1805–1881): decrittatura (Babbage?)



# Cifrari a sostituzione polialfabetica

## Friedrich Kasiski (1805–1881): decrittatura (Babbage?)



# Cifrari a sostituzione polialfabetica

## Metodo più generale

tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp

# Cifrari a sostituzione polialfabetica

## Metodo più generale

tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp

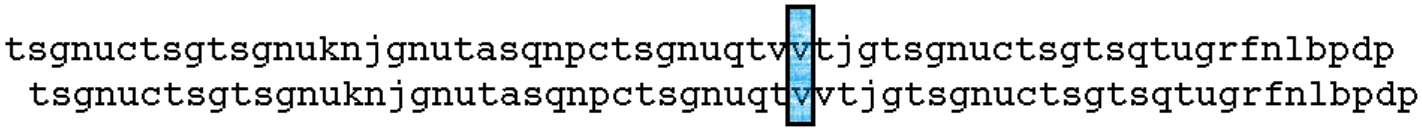
# Cifrari a sostituzione polialfabetica

## Metodo più generale

```
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
 tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
```

# Cifrari a sostituzione polialfabetica

## Metodo più generale



# Cifrari a sostituzione polialfabetica

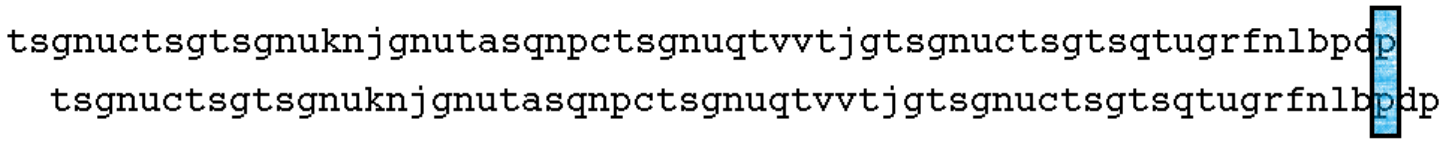
## Metodo più generale

tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp

tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp

# Cifrari a sostituzione polialfabetica

## Metodo più generale



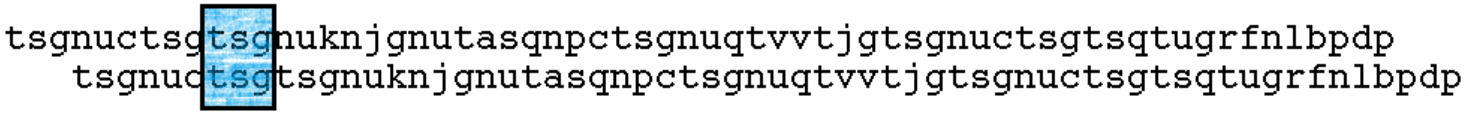
# Cifrari a sostituzione polialfabetica

## Metodo più generale

```
tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
   tsgnuctsgtsgnuknjgnutasqnpctsgnuqtvvtjgtsgnuctsgtsqtugrfnlbpdp
```

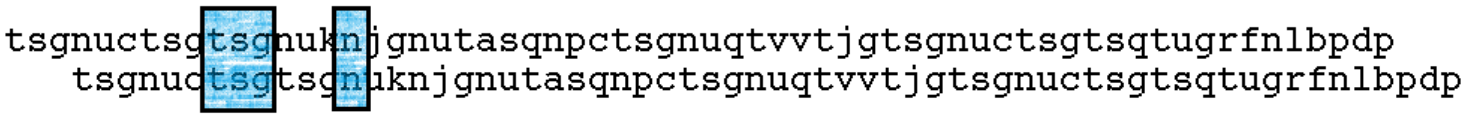
# Cifrari a sostituzione polialfabetica

## Metodo più generale



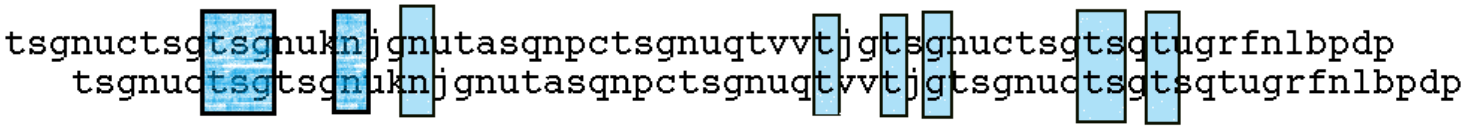
# Cifrari a sostituzione polialfabetica

## Metodo più generale



# Cifrari a sostituzione polialfabetica

## Metodo più generale



# Cifrari a sostituzione polialfabetica

## Decrittazione e limiti

- Con l'allineamento visto, si determina la lunghezza della parola chiave.
- Congetturata la lunghezza, si partiziona il testo in $n$ sottotesti e si cercano le $n$ chiavi con la la statistica.

# Cifrari a sostituzione polialfabetica

## Decrittazione

Proviamo con Peter Legrand etc. (Edgar)

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| t h z e i | p h m r r | r g o s r | k r u d w | v l k n u | s i t a g | s o k o e | p h m r r | r g | |
| | t h z e i | p h m r r | r g o s r | k r u d w | v l k n u | s i t a g | s o k o e | p h m r r | r g |
| | * | * | | | | * | | | |

Non molto evidente, ma il testo è corto per manifestare proprietà statistiche.

# Cifrari a sostituzione polialfabetica

## Decrittazione

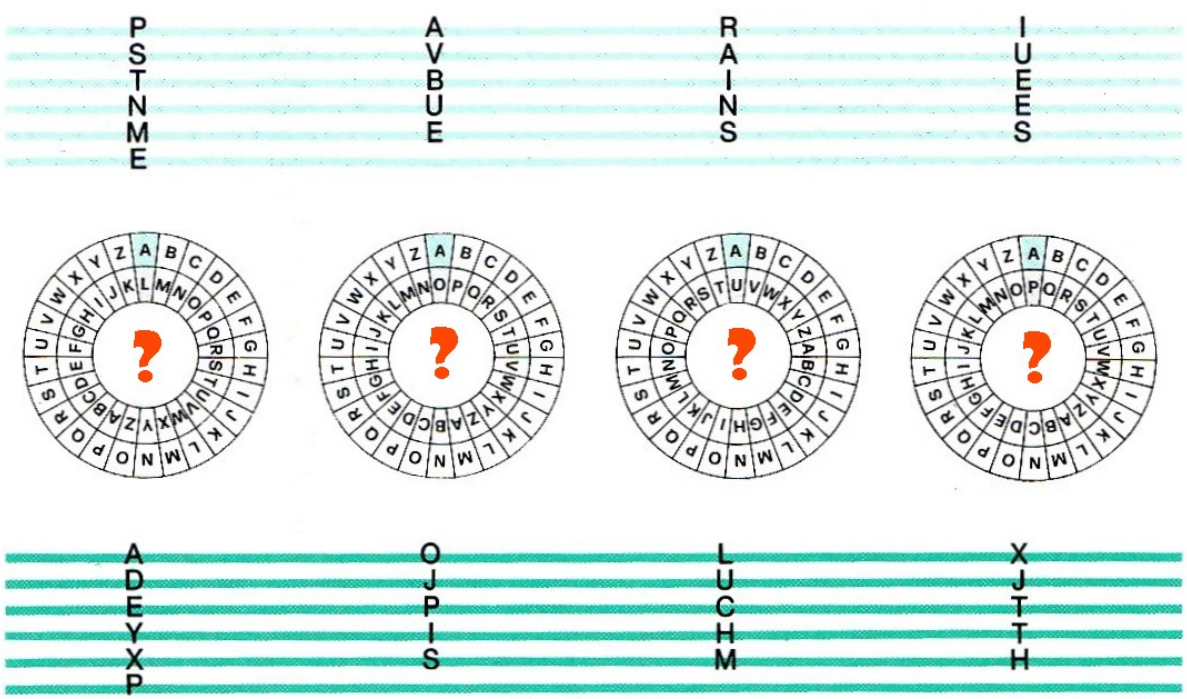
Proviamo con Peter Legrand etc. (Edgar)

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| thzei | phmrr | rgosr | krudw | vlknu | sitag | sokoe | phmrr | rg | |
| | thzei | phmrr | rgosr | krudw | vlknu | sitag | sokoe | phmrr | rg |
| | * | * | | | | * | | | |

Non molto evidente, ma il testo è corto per manifestare proprietà statistiche.

# Cifrari a sostituzione polialfabetica

## Decrittazione




Partiziono il testo usando la lunghezza della chiave e applico la statistica ad ogni partizione.

# Cifrari a sostituzione polialfabetica

## Decrittazione e limiti

- Questo sarà il vostro esercizio di programmazione: implementare l'algoritmo di decrittazione del Vigenère.
- La cifratura polialfabetica non è praticamente decifrabile se la parola chiave è lunga quanto il testo (e non viene più utilizzata per alti testi). Se inoltre non ha senso compiuto (è scelta lanciando una moneta) diventa dimostrabilmente indecifrabile (cifrario perfetto Vernam)
- In generale, se la chiave (il periodo) è molto lungo rispetto al testo la decodifica statistica non è effettiva.

# Cifrari a sostituzione polialfabetica

## Decrittazione e limiti

- Questo sarà il vostro esercizio di programmazione: implementare l'algoritmo di decrittazione del Vigenère.
- La cifratura polialfabetica non è praticamente decifrabile se la parola chiave è lunga quanto il testo (e non viene più utilizzata per alti testi). Se inoltre non ha senso compiuto (è scelta lanciando una moneta) diventa dimostrabilmente indecifrabile (cifrario perfetto Vernam)
- In generale, se la chiave (il periodo) è molto lungo rispetto al testo la decodifica statistica non è effettiva.

# Algebrizzazione del Vigenére

## Sostituzione polialfabetica algebrica (in $\mathbb{Z}_{26}$)

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Parola chiave: UDINE (=20,3,8,13,4). Testo in chiaro: Oggi la lezione è noiosa.

| O | G | G | I | L | A | L | E | Z | I | O | N | E | E | N | O | I | O | S | A |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 14 | 6 | 6 | 8 | 11 | 1 | 11 | 4 | 25 | 8 | 14 | 13 | 4 | 4 | 13 | 14 | 8 | 14 | 18 | 1 |
| 20 | 3 | 8 | 13 | 4 | 20 | 3 | 8 | 13 | 4 | 20 | 3 | 8 | 13 | 4 | 20 | 3 | 8 | 13 | 4 |
| 8 | 9 | 14 | 21 | 15 | 21 | 14 | 12 | 12 | 12 | 8 | 16 | 12 | 17 | 17 | 8 | 11 | 22 | 5 | 5 |
| I | J | O | V | P | V | O | M | M | M | I | Q | M | R | R | I | L | W | F | F |

Testo in cifra: IJOVPVOMMMIQMRRILWFF
(ovviamente non usiamo gli accenti!)

# Algebrizzazione del Vigenére

## Sostituzione polialfabetica algebrica (in $\mathbb{Z}_2$)

| A B C D E | F G H I J | K L M N O | P Q R S T | U V W X Y | Z ♣ ◇ ♡ ♠ | ♭ ♯ |
|---|---|---|---|---|---|---|
| 0 1 2 3 4 | 5 6 7 8 9 | 10 11 12 13 14 | 15 16 17 18 19 | 20 21 22 23 24 | 25 26 27 28 29 | 30 31 |

Chiave: UDINE= 20,3,8,13,4 = 10100, 00011, 01000, 01101, 00100

Testo in chiaro: Oggi la lezione è noiosa.

| O | G | G | I | L | A | L | E | Z | I |
|---|---|---|---|---|---|---|---|---|---|
| 01110 | 00110 | 00110 | 01000 | 01011 | 00000 | 01011 | 00100 | 11001 | 01000 |
| 10100 | 00011 | 01000 | 01101 | 00100 | 10100 | 00011 | 01000 | 01101 | 00100 |
| 11010 | 00101 | 01110 | 00101 | 01111 | 10100 | 01000 | 01100 | 10100 | 01100 |
| ♣ | F | O | F | P | U | Q | M | U | M |

| O | N | E | E | N | O | I | O | S | A |
|---|---|---|---|---|---|---|---|---|---|
| 01110 | 01110 | 00100 | 00100 | 01101 | 01110 | 01000 | 01110 | 01010 | 00000 |
| 10100 | 00011 | 01000 | 01101 | 00100 | 10100 | 00011 | 01000 | 01101 | 00100 |
| 11010 | 01101 | 01100 | 01001 | 01001 | 11010 | 01011 | 00110 | 00111 | 00100 |
| ♣ | N | M | J | J | ♣ | L | G | H | E |

Testo in cifra: ♣ FOFP UQMUM ♣ NMJJ ♣ LGHE

# Il cifrario perfetto

## Gilbert Vernam (1890–1960): one-time-pad

- Ogni bit usato per cifrare viene generato da un lancio di moneta.
- La chiave è lunga quanto il testo e
- Non viene più riutilizzata
- Sembra indecifrabile.
- Lo è (Shannon)
- Come comunichiamo la chiave?

# Il cifrario perfetto

## Gilbert Vernam (1890–1960): one-time-pad

- Ogni bit usato per cifrare viene generato da un lancio di moneta.
- La chiave è lunga quanto il testo e
- Non viene più riutilizzata
- Sembra indecifrabile.
- Lo è (Shannon)
- Come comunichiamo la chiave?

# Il cifrario perfetto

## Gilbert Vernam (1890–1960): one-time-pad

- Ogni bit usato per cifrare viene generato da un lancio di moneta.
- La chiave è lunga quanto il testo e
- Non viene più riutilizzata
- Sembra indecifrabile.
- Lo è (Shannon)
- Come comunichiamo la chiave?

# Il cifrario perfetto

## La linea rossa

Il cifrario one-time-pad fu usato nelle comunicazioni USA–URSS durante la guerra fredda.




Ci dev'essere stato un piccolo esercito di lanciatori di monete.

# Il cifrario perfetto

## La linea rossa

Il cifrario one-time-pad fu usato nelle comunicazioni USA–URSS durante la guerra fredda.




Ci dev'essere stato un piccolo esercito di lanciatori di monete.

# Il cifrario perfetto

## Numbers Station

- Le numbers stations sono stazioni radio in onde corte che trasmettono informazioni criptate.
- La codifica può essere effettuata in vari modi (che includono modulazione dell'audio). One-time-pad è uno di questi.
- La/le spie concordano il codice one-time-pad assieme. Poi si spostano con la loro radio.
- Ricevendo il segnale con una radio e non si è tracciabili.
- Nel 1995–1998 c'è stato il caso della stazione cubana Atención e dell'arresto delle spie cubane denominate Wasp.

# Il cifrario perfetto

## Numbers Station

- Le numbers stations sono stazioni radio in onde corte che trasmettono informazioni criptate.
- La codifica può essere effettuata in vari modi (che includono modulazione dell'audio). One-time-pad è uno di questi.
- La/le spie concordano il codice one-time-pad assieme. Poi si spostano con la loro radio.
- Ricevendo il segnale con una radio e non si è tracciabili.
- Nel 1995–1998 c'è stato il caso della stazione cubana Atención e dell'arresto delle spie cubane denominate Wasp.

# Conclusioni

- Per oggi è tutto.
- In laboratorio potrete implementare dapprima i cifrari monoalfabetici (Cesare) e poi i polialfabetici (Vigenere)
- Potrete dunque usarli per scrivervi degli sms cifrati!
- Poi implementrerete la tecnica brevemente descritta per forzare il cifrario di Vigenére
- Dovrete scoprire cosa si nasconde in testi (abbastanza lunghi) scritti dai vostri compagni!
- Nella prossima lezione vedremo l'automazione della crittografia, in particolare parleremo dell'ENIGMA.

# Conclusioni

- Per oggi è tutto.
- In laboratorio potrete implementare dapprima i cifrari monoalfabetici (Cesare) e poi i polialfabetici (Vigenere)
- Potrete dunque usarli per scrivervi degli sms cifrati!
- Poi implementrerete la tecnica brevemente descritta per forzare il cifrario di Vigenére
- Dovrete scoprire cosa si nasconde in testi (abbastanza lunghi) scritti dai vostri compagni!
- Nella prossima lezione vedremo l'automazione della crittografia, in particolare parleremo dell'ENIGMA.

# Conclusioni

- Per oggi è tutto.
- In laboratorio potrete implementare dapprima i cifrari monoalfabetici (Cesare) e poi i polialfabetici (Vigenere)
- Potrete dunque usarli per scrivervi degli sms cifrati!
- Poi implementrerete la tecnica brevemente descritta per forzare il cifrario di Vigenére
- Dovrete scoprire cosa si nasconde in testi (abbastanza lunghi) scritti dai vostri compagni!
- Nella prossima lezione vedremo l'automazione della crittografia, in particolare parleremo dell'ENIGMA.

# Conclusioni

- Per oggi è tutto.
- In laboratorio potrete implementare dapprima i cifrari monoalfabetici (Cesare) e poi i polialfabetici (Vigenere)
- Potrete dunque usarli per scrivervi degli sms cifrati!
- Poi implementrerete la tecnica brevemente descritta per forzare il cifrario di Vigenére
- Dovrete scoprire cosa si nasconde in testi (abbastanza lunghi) scritti dai vostri compagni!
- Nella prossima lezione vedremo l'automazione della crittografia, in particolare parleremo dell'ENIGMA.

# Conclusioni

- Per oggi è tutto.
- In laboratorio potrete implementare dapprima i cifrari monoalfabetici (Cesare) e poi i polialfabetici (Vigenere)
- Potrete dunque usarli per scrivervi degli sms cifrati!
- Poi implementrerete la tecnica brevemente descritta per forzare il cifrario di Vigenére
- Dovrete scoprire cosa si nasconde in testi (abbastanza lunghi) scritti dai vostri compagni!
- Nella prossima lezione vedremo l'automazione della crittografia, in particolare parleremo dell'ENIGMA.