# Laboratorio di Crittografia

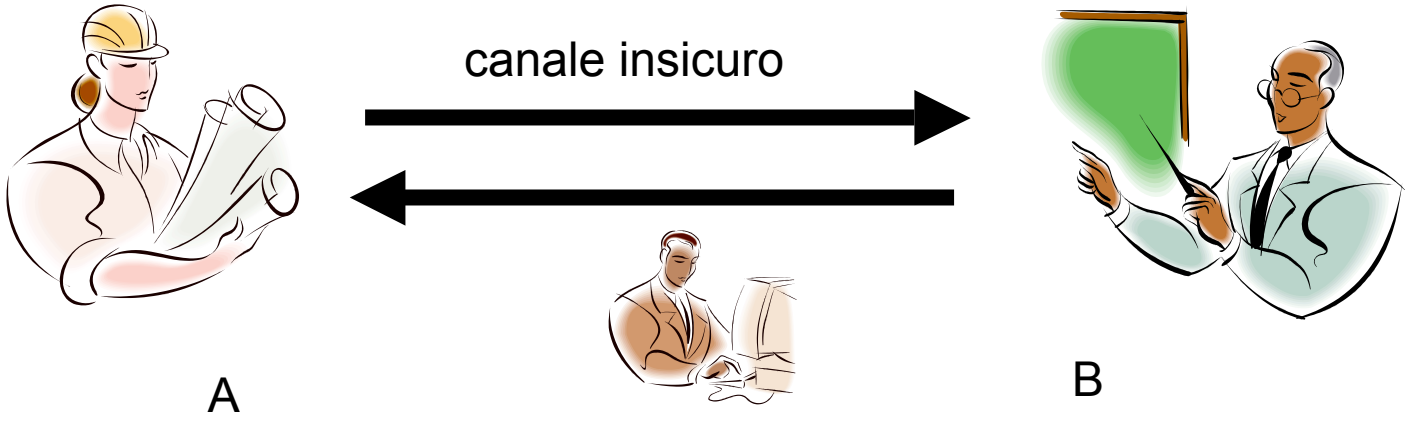
Prima Lezione

# Schema della lezione

- Crittografia e crittoanalisi: presentazione, definizioni e utilizzo
- La crittografia nella storia: la scacchiera di Polibio
- Il crittosistema di Cesare
- Sostituzione monoalfabetica e analisi delle frequenze
- Utilizzo di matematica e informatica

# Che cos’è la crittografia

E’ la scienza che studia come rendere segreta e sicura la comunicazione tra due persone o entità nascondendo il significato del messaggio



- Supponiamo che A voglia mandare a B un messaggio segreto *m*
- A **cifra** il messaggio *m* ottenendo un messaggio *c* che invia a B
- B riceve *c* e lo **decifra** riottenendo il messaggio *m*
- *m* si dice **messaggio in chiaro**, *c* **messaggio cifrato**

- Il processo di cifratura deve essere biunivoco, in modo permettere un processo inverso che ritrovi il messaggio originale
- Chi riceve il messaggio *c* deve essere in grado di interpretare ("decifrare") *c*
- A e B si devono essere messi d'accordo prima su come "cifrare" e "decifrare" e scegliere un metodo efficace in modo che per gli altri sia sostanzialmente impossibile cifrare e decifrare un messaggio

- La crittografia fornisce metodi effettivi per effettuare cifratura e decifratura dei messaggi
- Il processo di trasformazione dal messaggio in chiaro al messaggio cifrato e viceversa è spesso noto, ma si basa su una informazione specifica (detta “chiave”), senza la quale non si è in grado di operare
- I metodi di cifratura si sono estremamente evoluti nell’arco della storia

# La crittografia nella storia

- Erodoto (libro VII delle Storie):
  - Demarato per avvisare gli Spartani del prossimo attacco del re persiano Serse alla Grecia *prese una tavoletta doppia, ne raschiò la* cera e *poi sul legno della tavoletta scrisse il piano del re. Fatto ciò versò di nuovo* cera *liquefatta sullo scritto, in modo che, venendo portata vuota, la tavoletta non procurasse nessun fastidio da parte dei custodi delle strade*

(prima della battaglia di Salamina, 480 a.C.)

# La crittografia nella storia

- Ancora Erodoto narra (libro V delle Storie)
  - Istieo voleva dare ad Aristagora l'ordine di ribellarsi, non aveva alcun altro modo per annunziarglielo con sicurezza, essendo le strade sorvegliate, ***fatta rasare la testa al più fido degli schiavi, vi impresse dei segni,*** **e** ***aspettò che ricrescessero*** **i** ***capelli.*** *Non appena ricrebbero, lo spedì a Mileto, non comandandogli null'altro se non che, quando giungesse a Mileto, dicesse ad Aristagora di fargli radere* i *capelli* e *di guardare la sua testa: i segni impressi ordinavano, come già prima ho detto, la rivolta.*

# La crittografia nella storia

- Questi primi due esempi riguardano in realtà la “steganografia” (viene nascosto il messaggio e non il significato)
- Tra i primi esempi di scrittura segreta vera e propria si citano i geroglifici egiziani crittografati
- Possono essere trattati come esempi di crittografia anche le lingue morte (o, da un punto di vista personale, qualunque linguaggio o modalità di scrittura che non ci sia noto)

# La crittografia nella storia

- Un altro esempio è la scitala (skytale) con cui gli spartani cifravano e decifravano messaggi segreti
  (Plutarco, Vite parallele)
- I messaggi erano scritti su un nastro (spesso una striscia di papiro) avvolto su un bastone (la scitala), solo con un bastone identico il messaggio poteva essere riletto

# La scacchiera di Polibio

Nel libro X delle Storie, (circa 200-118 a. C.) Polibio attribuisce ai suoi contemporanei Cleoxeno e Democleito l'introduzione di un sistema di telecomunicazione (telegrafo ottico trasmesso con due gruppi di 5 torce) qui adattato all'alfabeto italiano, con l'aggiunta dei principali segni di interpunzione

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

La scacchiera di Polibio è la base per un cifrario a colpi. Ogni lettera è rappresentata dalla coppia di numeri che indica la sua posizione nella scacchiera, cominciando dalla prima riga:

B è 12, P è 34, V è 45

Il messaggio viene battuto lasciando una pausa più breve tra i due numeri che si riferiscono ad una lettera e una pausa più lunga tra una lettera e l'altra.

DOMANI PIOVE

1433311132243424334515

(cf anche (con una scacchiera differente):
http://www.liceofoscarini.it/studenti/crittografia/critto/js/polibio.html)

Sito completo:

http://www.liceofoscarini.it/studenti/crittografia/

Abbiamo usato:

- Alfabeto del messaggio in chiaro
- Alfabeto per il messaggio cifrato
- Una corrispondenza biunivoca tra i due alfabeti, definita dalla forma della scacchiera e dalla distribuzione dell'alfabeto in essa. (tale scelta è detta "chiave")

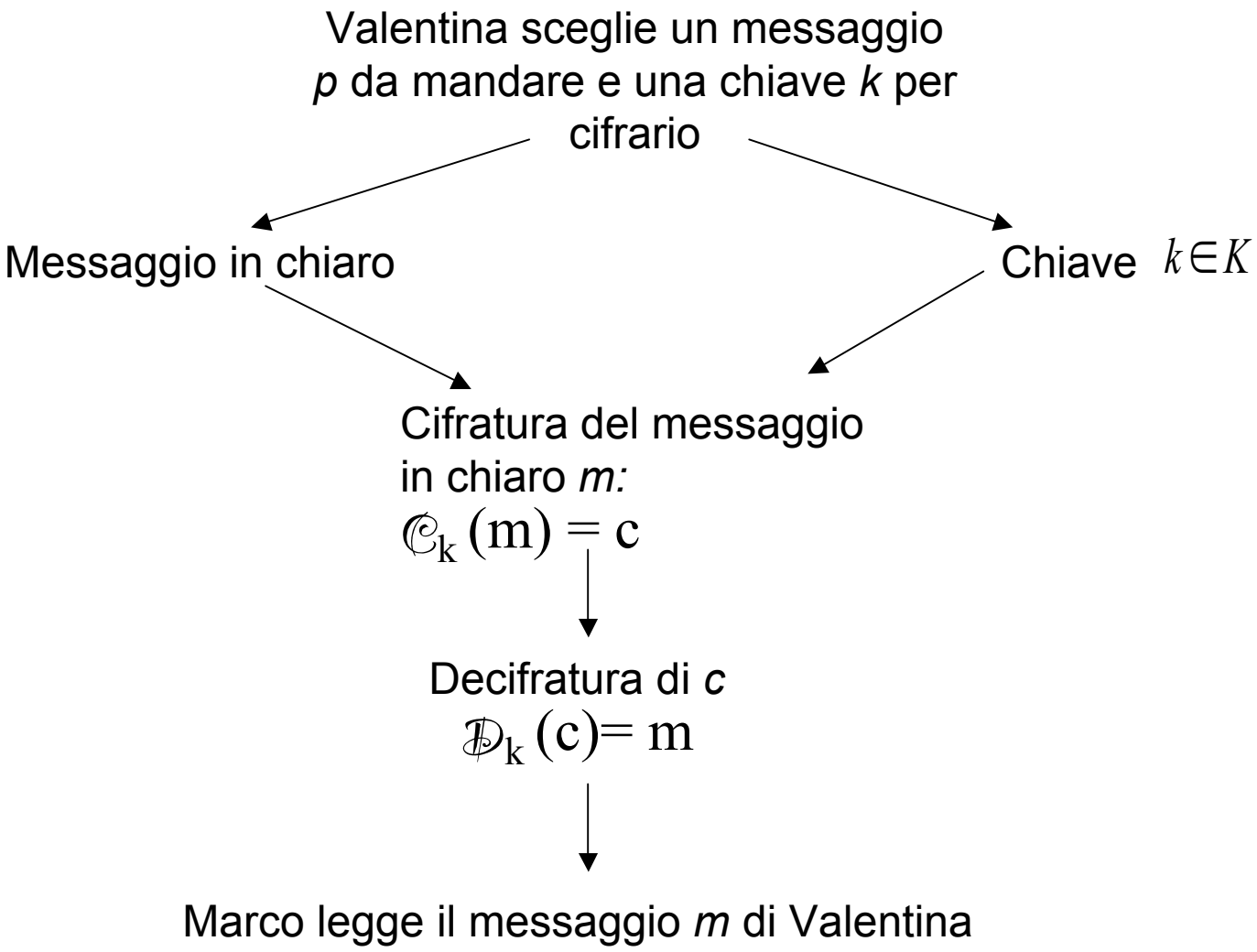
Caratteristiche:

- Una lettera viene cifrata sempre allo stesso modo (cifrario monoalfabetico)
- La regola che mi permette di cifrare mi spiega anche come decifrare (e viceversa)

# Crittosistema

Un crittosistema è costituito da:

- l'insieme dei messaggi in chiaro *M* di cui indichiamo gli elementi con la lettera m;
- l'insieme delle chiavi *K* in cui ogni elemento k determina una trasformazione di cifratura $\mathcal{C}_k$ e una trasformazione di decifratura $\mathcal{D}_k$ che sono una l'inversa dell'altra;
- l'insieme dei messaggi cifrati *C* i cui elementi sono indicati con la lettera c.


Valentina sceglie un messaggio
*p* da mandare e una chiave *k* per
cifrario
Messaggio in chiaro
Chiave $k \in K$
Cifratura del messaggio
in chiaro *m:*
$\mathcal{E}_k(m) = c$
Decifratura di *c*
$\mathcal{D}_k(c) = m$
Marco legge il messaggio *m* di Valentina

# La crittoanalisi

- La crittoanalisi invece studia come decifrare un messaggio senza esserne “autorizzati”
- La crittoanalisi ha il ruolo fondamentale di far capire quanto un sistema di cifratura/decifratura sia sicuro

La crittoanalisi nasce sostanzialmente durante l'VIII e il IX secolo d. C., quando gli arabi si dedicarono allo studio approfondito della lingua scritta e, tra l'altro, stabilirono le frequenza delle varie lettere. In particolare, scoprirono che le lettere più usate erano sostanzialmente le stesse in qualsiasi testo, purchè abbastanza esteso. Non è noto quando queste conoscenze furono applicate alla crittografia.

# Che cos'è la crittografia : obiettivi

- Segretezza

  Il messaggio non deve essere leggibile a terzi.

- Autenticazione

  Il destinatario deve poter essere sicuro del mittente.

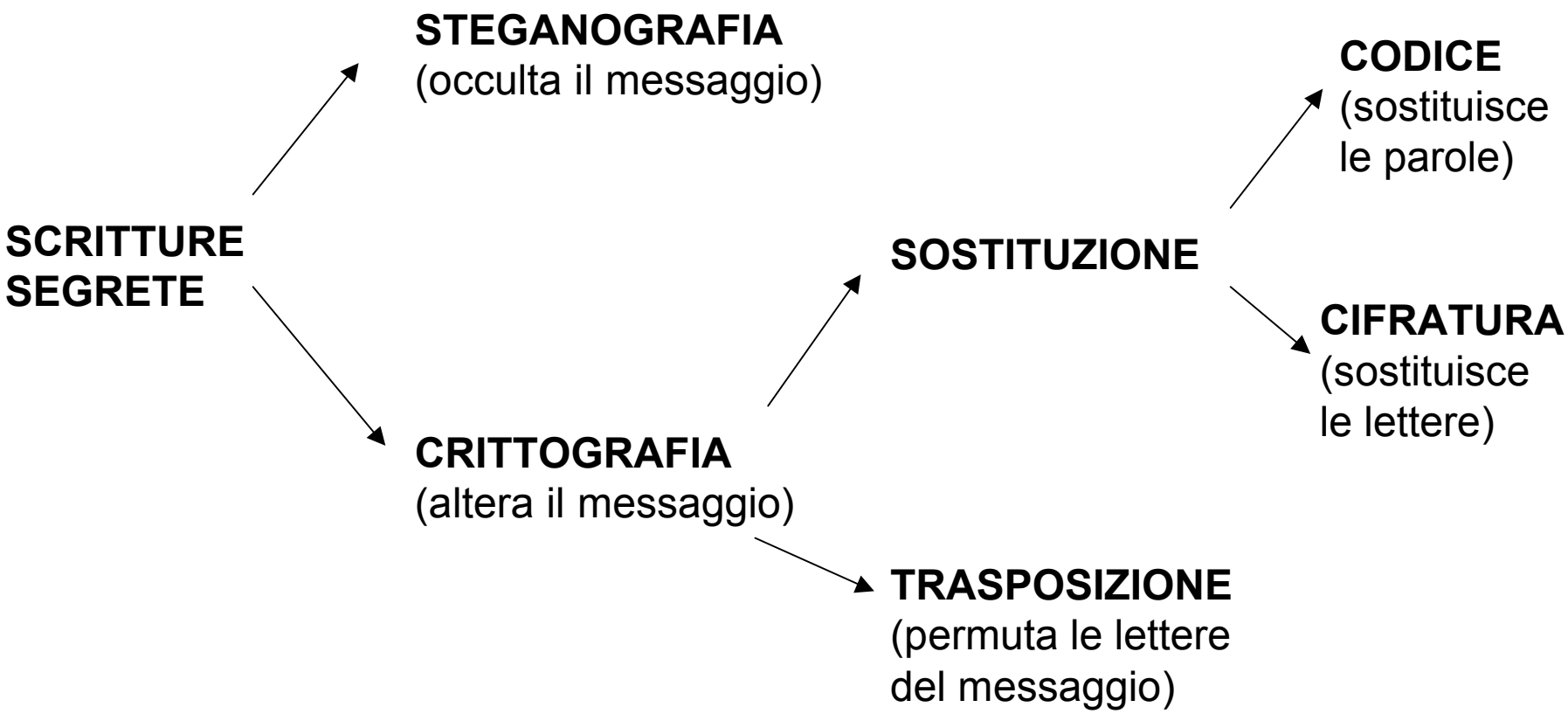
- Integrità

  Il destinatario deve poter essere sicuro che il messaggio non sia stato modificato.

- Attendibilità

  Il mittente non deve poter negare di aver inviato il messaggio.

# Che cos'è la crittografia



# Discipline affini alla crittografia

Oltre alla crittografia, anche le seguenti discipline alterano i messaggi

- **teoria dei codici**, altera il messaggio per rilevare ed eventualmente correggere errori in fase di trasmissione
- **compressione dati**, altera il messaggio per ridurne la grandezza in modo da risparmiare memoria e tempo di trasmissione

# Utilizzo tradizionale della crittografia

- Gli usi tradizionali riguardavano quasi esclusivamente gli ambiti militari e di spionaggio/controspionaggio
- Sono riportati numerossimi esempi di uso di sistemi crittografici nel corso di guerre, battaglie, rivoluzioni, cospirazioni, complotti, ...

# Utilizzi moderni della crittografia

- L'uso più importante della crittografia in ambito "civile" è quella della sicurezza delle comunicazioni in rete
- Più in particolare le applicazioni di commercio elettronico sono quelle in cui maggiormente è sentita la necessità della sicurezza e della segretezza (scambio di dati sensibili, quali il numero di carta di credito, numero di conti bancari, ecc.)

# Utilizzi moderni della crittografia

- Un altro utilizzo importante è quello della firma digitale e dell'autenticazione dei documenti, che ha applicazioni nella pubblica amministrazione (e-government) e in generale negli aspetti burocratici (contratti, domande, moduli, vari documenti ufficiali, ecc.)

# Strumenti per la crittografia tradizionale

- La crittografia “tradizionale” ha lavorato molto sulle tecniche di cifratura per sostituzione monoalfabetica e polialfabetica
- Si usavano anche “classificatori” per codificare parole e frasi
- Le tecniche erano pensate per l’uomo o per strumenti meccanici più o meno semplici

# Strumenti per la crittografia moderna

- La crittografia moderna è stata fortemente influenzata dall'informatica e dalla matematica
- L'informatica
  - pone nuove sfide rendendo possibile decifrare in modo semplice cifrari ritenuti impossibili
  - chiede nuove applicazioni e nuove tecniche: ad esempio lo scambio di chiavi, la crittografia a chiave pubblica, la firma digitale, ...
  - fornisce hardware e soprattutto software per la crittografia

# Strumenti per la crittografia moderna

- La matematica è lo strumento fondamentale per la crittografia
  - fornisce metodi per cifrare, decifrare, firmare e controllare messaggi
  - garantisce la sicurezza della crittografia
  - studia (unitamente all'informatica) come svolgere velocemente le operazioni crittografiche

# Il crittosistema di Cesare

Svetonio, nella Vita dei dodici Cesari, racconta che Giulio Cesare utilizzava un sistama di cifrazione molto semplice: ogni lettera va sostituita con quella che si trova tre posti dopo

| ·a | ·b | ·c | ·d | ·e | ·f | ·g | ·h | ·i | ·l | ·m | ·n | ·o | ·p | ·q | ·r | ·s | ·t | ·u | ·v | ·z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ·D | ·E | ·F | ·G | ·H | ·I | ·L | ·M | ·N | ·O | ·P | ·Q | ·R | ·S | ·T | ·U | ·V | ·Z | ·A | ·B | ·C |

Ad esempio la frase
**domani attaccheremo** (testo in chiaro),
diventerà
**GRPDQN DZZDFFMHUHPRI** (testo cifrato).

# Il crittosistema di Cesare

- La decifrazione è altrettanto semplice, basta sostituire ogni lettera quella che si trova tre posti prima

| ·A | ·B | ·C | ·D | ·E | ·F | ·G | ·H | ·I | ·L | ·M | ·N | ·O | ·P | ·Q | ·R | ·S | ·T | ·U | ·V | ·Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ·u | ·v | ·z | ·a | ·b | ·c | ·d | ·e | ·f | ·g | ·h | ·i | ·l | ·m | ·n | ·o | ·p | ·q | ·r | ·s | ·t |

# Generalizzazione

- E’ possibile generalizzare il sistema di Cesare usando uno spostamento di k posti, anzichè di 3.
- k deve essere un numero compreso tra 1 e 20
- Ad esempio con k=7

| ·a | ·b | ·c | ·d | ·e | ·f | ·g | ·h | ·i | ·l | ·m | ·n | ·o | ·p | ·q | ·r | ·s | ·t | ·u | ·v | ·z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ·H | ·I | ·L | ·M | ·N | ·O | ·P | ·Q | ·R | ·S | ·T | ·U | ·V | ·Z | ·A | ·B | ·C | ·D | ·E | ·F | ·G |

La frase dell’esempio precedente diventa
**MVTHUR HDDHLLQNBNTV**

# Sostituzione monoalfabetica

- In generale il crittosistema di Cesare è un cifrario in cui la stessa lettera è codificata sempre con la stessa lettera
- Ad esempio la lettera ‘a’ è sempre codificata con la lettera ‘D’, la ‘b’ è codificata con ‘E’, ...

# Sostituzione monoalfabetica

- Il caso più generale è quello in cui l'alfabeto cifrato è una permutazione di quello in chiaro
- Un modo semplice per ricordare la permutazione è quello di usare una frase

| ·a | ·b | ·c | ·d | ·e | ·f | ·g | ·h | ·i | ·l | ·m | ·n | ·o | ·p | ·q | ·r | ·s | ·t | ·u | ·v | ·z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ·N | ·E | ·L | ·M | ·Z | ·O | ·D | ·C | ·A | ·I | ·S | ·T | ·R | ·V | ·B | ·F | ·G | ·H | ·P | ·Q | ·U |

in questo esempio la frase è

NEL MEZZO DEL CAMMIN DI NOSTRA VITA

- Ad esempio la frase **domani attaccheremo** diventa

**MRSNTA NHHNLLCZFZSR**

# Sostituzione monoalfabetica

- Esistono 21!=**51090942171709440000** permutazioni possibili, cioè circa $51 \cdot 10^{18}$, ossia più di *cinquanta miliardi di miliardi*
- Una ricerca esaustiva per trovare la permutazione giusta è praticamente impossibile
- Eppure questo codice è tutt'altro che sicuro...

# Come decifrare un codice monoalfabetico

- Usare simboli diversi al posto delle lettere non aumenta la difficoltà di decifratura
- Si confronti ad esempio il codice
  **MRSNTA NHHNLLCZFZSR**
  con il codice
  11-16-17-12-18-01-00-12-08-08-12-10-10-03-21-06-21-17-16
- La debolezza del codice sta nelle ripetizioni di simboli

# Frequenza delle lettere in italiano

| •Lettera | •% | •Lettera | •% | •Lettera | •% |
|---|---|---|---|---|---|
| •a | •11,74 | •h | •1,54 | •q | •0,51 |
| •b | •0,92 | •i | •11,28 | •r | •6,38 |
| •c | •4,50 | •l | •6,51 | •s | •4,98 |
| •d | •3,73 | •m | •2,52 | •t | •5,63 |
| •e | •11,79 | •n | •6,88 | •u | •3,02 |
| •f | •0,95 | •o | •9,83 | •v | •2,10 |
| •g | •1,65 | •p | •3,05 | •z | •0,49 |

# Come decifrare un codice monoalfabetico

- Sapendo che il testo è in italiano,è facile che l'ultima lettera di ciascuna parola sia una vocale. (questa osservazione non è essenziale per il metodo, ma lo rende più breve)
- Si cercano i simboli più frequenti nel testo cifrato
- Si provano a sostituire con le lettere più frequenti in italiano
- Si cerca di vedere se si riesce a "intravedere" delle parti di parole
- Qualche tentativo può portare a parole improbabili, in tal caso si deve rivedere alcune scelte

# Esempio

**TRT QRDIAR NTMNFZ N GLPRIN**

| •Lettera | •Occor-renze | •Lettera | •Occor-renze | •Lettera | •Occor-renze |
|---|---|---|---|---|---|
| •A | •1 | •H | •0 | •Q | •1 |
| •B | •0 | •I | •2 | •R | •4 |
| •C | •0 | •L | •1 | •S | •0 |
| •D | •1 | •M | •1 | •T | •3 |
| •E | •0 | •N | •4 | •U | •0 |
| •F | •1 | •O | •0 | •V | •0 |
| •G | •1 | •P | •1 | •Z | •1 |

# Esempio: **TRT QRDIAR NTMNFZ N GLPRIN**

- Primo tentativo*:* inizio dalle lettere terminali di una parola e associando loro le vocali, in ordine di frequenza: **R = e, N = a , T = i, Z = o,**
- si ottiene **iei QeDIAe aiMNFZ a GLPeIa**
- Rivediamo alcune scelte (la prima parola non ha senso) **T = n**, (è la seconda consonante per frequenza: la prima è L che non sembra adatta), **R = o, Z = e,**
- Otteniamo **non QoDIAo anMaFe a GLPoIa**
- Ora introduciamo le consonanti più frequenti ancora mancanti (**l**, **r**,**t**,**s**,**c**) e reintroduciamo la **i**. Proviamo con **I = l**, **A = i**, **D = t**, **F = r, G = s** , **L=c:**

  **non Qotlio anMare a scPola**

  Posso modificare ancora **D = g** e continuare...

# Sostituzione polialfabetica

- Un crittosistema per sostituzione polialfabetica non usa sempre lo stesso simbolo per la stessa lettera
- Per ogni posizione del messaggio in chiaro viene usato un alfabeto diverso
- Così si supera (parzialmente…) il problema della debolezza visto per i crittosistemi monoalfabetici
- Infatti ha “meno” senso contare le frequenze di simboli, non essendoci più corrispondenza tra lettere in chiaro e simboli cifrati