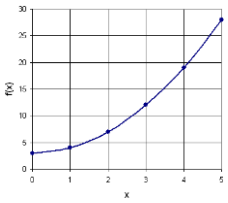
Laboratorio matematica Data:

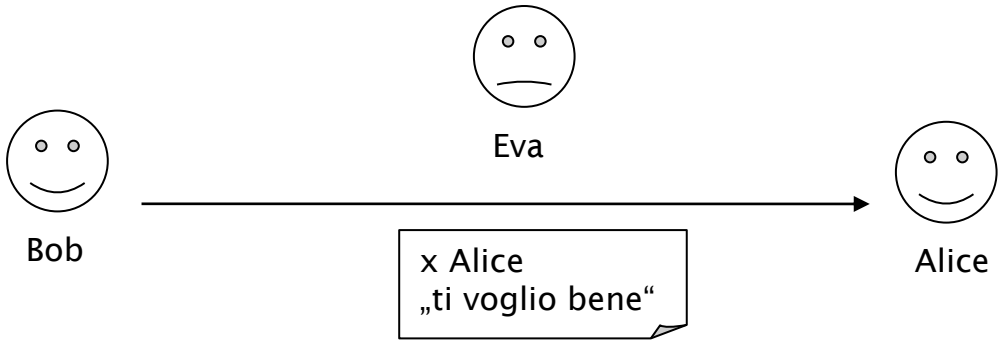


Il messaggio segreto

La crittografia

Usando la crittografia è possibile codificare un messaggio in modo che risulti illeggibile a chi lo legge senza possedere determinate conoscenze.

Un esempio:



Bob vuole scrivere un messaggio a Alice. Lo scrive su un bigliettino e lo passa tra i banchi con la scritta “x Alice”. Il biglietto passa in mano ad Eva, la quale per curiosità lo apre e lo legge.

Come potrebbe fare Bob per rendere il messaggio illeggibile a Eva?

Il cifrario di Cesare

Un metodo molto antico è il cosiddetto “cifrario di Cesare”, usato dall’imperatore romano Giulio Cesare per i suoi messaggi segreti.
Si tratta di sostituire ogni lettera del testo con la lettera che viene dopo un certo numero di posizioni (useremo un alfabeto comprensivo anche delle lettere j,k,w,x e y - in fondo al foglio lo trovi elencato con l’ordinamento corretto.).

Nel caso dello spostamento di una posizione (cifrario di Cesare con chiave 1) abbiamo la seguente situazione:

```
ti voglio bene      (questo si chiama "testo in chiaro")
↓↓ ↓↓↓↓↓↓ ↓↓↓↓
uj wphmjp cfof      (questo si chiama "testo cifrato")
```

In questo caso Eva legge il messaggio “uj wphmjp cfof” e non capisce, mentre Alice, che conosce il modo usato da Bob per codificare il messaggio, può ricostruire il messaggio originale, sostituendo ogni lettera con quella che la precede.

Attività 1
Codifica i seguenti messaggi con il cifrario di Cesare con chiave 1.

Messaggio 1: “Io mi chiamo Cesare”

……

Messaggio 2: “Come la mettiamo con Zorro?”

……

Attività 2
Decodifica i seguenti messaggi, che sono stati crittati con il cifrario di Cesare con chiave 1.

Messaggio 1: “jp bnp mb nbufnbujdb”

……

Messaggio 2: “b dbsofwbmf nj wftujsp eb apssp”

……

Attività 3
Ora pensa tu una piccola frase, codificala con il cifrario di Cesare in chiave 1, e prova a farla scoprire al tuo compagno di banco.

Testo cifrato: ……

Ora tutti i tuoi compagni sanno come funziona questo metodo. Hai qualche idea su come potresti fare in modo che i tuoi compagni non possano leggere i tuoi messaggi?

Laboratorio matematica Data:

Il cifrario di Cesare con chiave "n"

Invece di sostituire una lettera con quella seguente, si può sostituirla con quella che viene dopo due, tre (questo era il metodo usato da Giulio Cesare), quattro, cinque o più posizioni. Si dice che si usa il cifrario di Cesare in chiave "n", dove n è il numero di posizioni di cui si sposta una lettera.

Esempio: usando la chiave 5 la parola "casa" diventa "hfxf" (verificalo!).

Attività 4
Codifica i seguenti messaggi con il cifrario di Cesare con chiave 3.

Messaggio 1: "Sono o non sono il capitano Uncino?"

……

Messaggio 2: "Houston, we have a problem."

……

Attività 5
Decodifica il seguente messaggio, crittato con il cifrario di Cesare con chiave 3

Messaggio 1: "rjjl id eho whpsr"

……

Decodifica il seguente messaggio, crittato con il cifrario di Cesare con chiave 10.

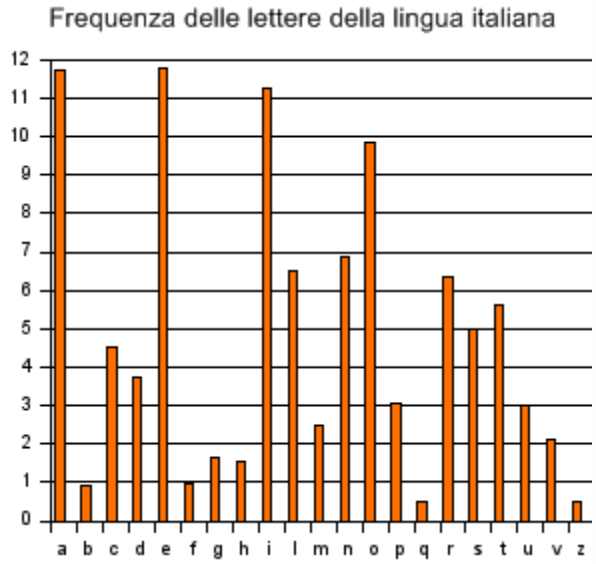
Messaggio 2: "Ommy cfovkdy sv wocckqqsy"

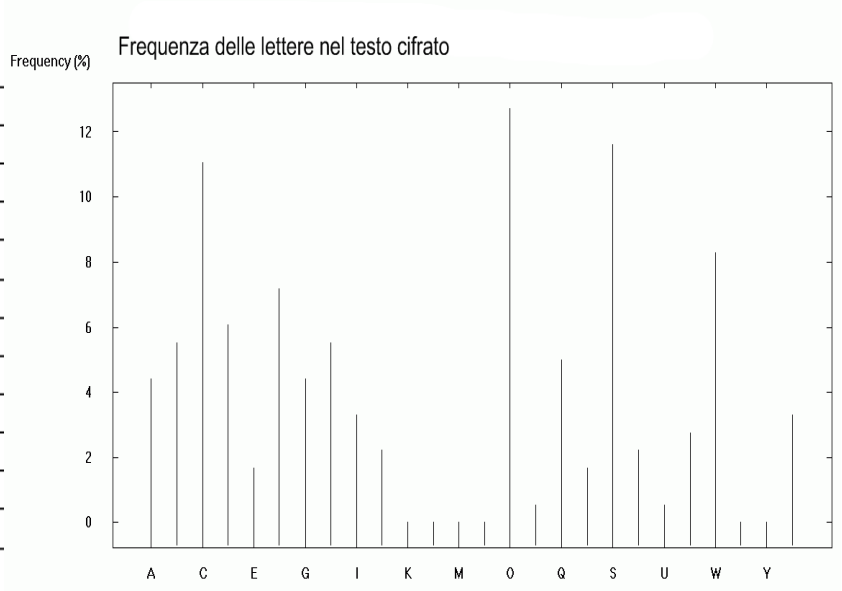
……

Attività 6

Qui sotto trovi un breve testo codificato mediante il cifrario di Cesare.
Non sappiamo però quale chiave è stata usata.
Hai qualche idea su come recuperare il messaggio originale?

“Ti qcgw qvs qcawbqwow o qodwfs qvs bcb gw dofzo gczoasbhs dsf dofzofs, dsf rwfs 'vc tohhc eisghc' 'vc tohhc eiszzc' 'vc aobuwohc s psjihc', ao gw dofzo dsf tofgw ib'wrso, dsf qodwfs qcas jo eisghc acbrc. Bcb qw ojsjc aow dsbgohc dfwao.”





Per approfondire:

http://it.wikipedia.org/wiki/Crittologia
http://it.wikipedia.org/wiki/Cifrario_di_Cesare
http://it.wikipedia.org/wiki/ROT13
http://it.wikipedia.org/wiki/Cifrario_di_Vigen%C3%A8re
http://it.wikipedia.org/wiki/Enigma_(crittografia)
http://www.cryptool.de/