MESSAGGI SEGRETI

di Massimo Iuliani

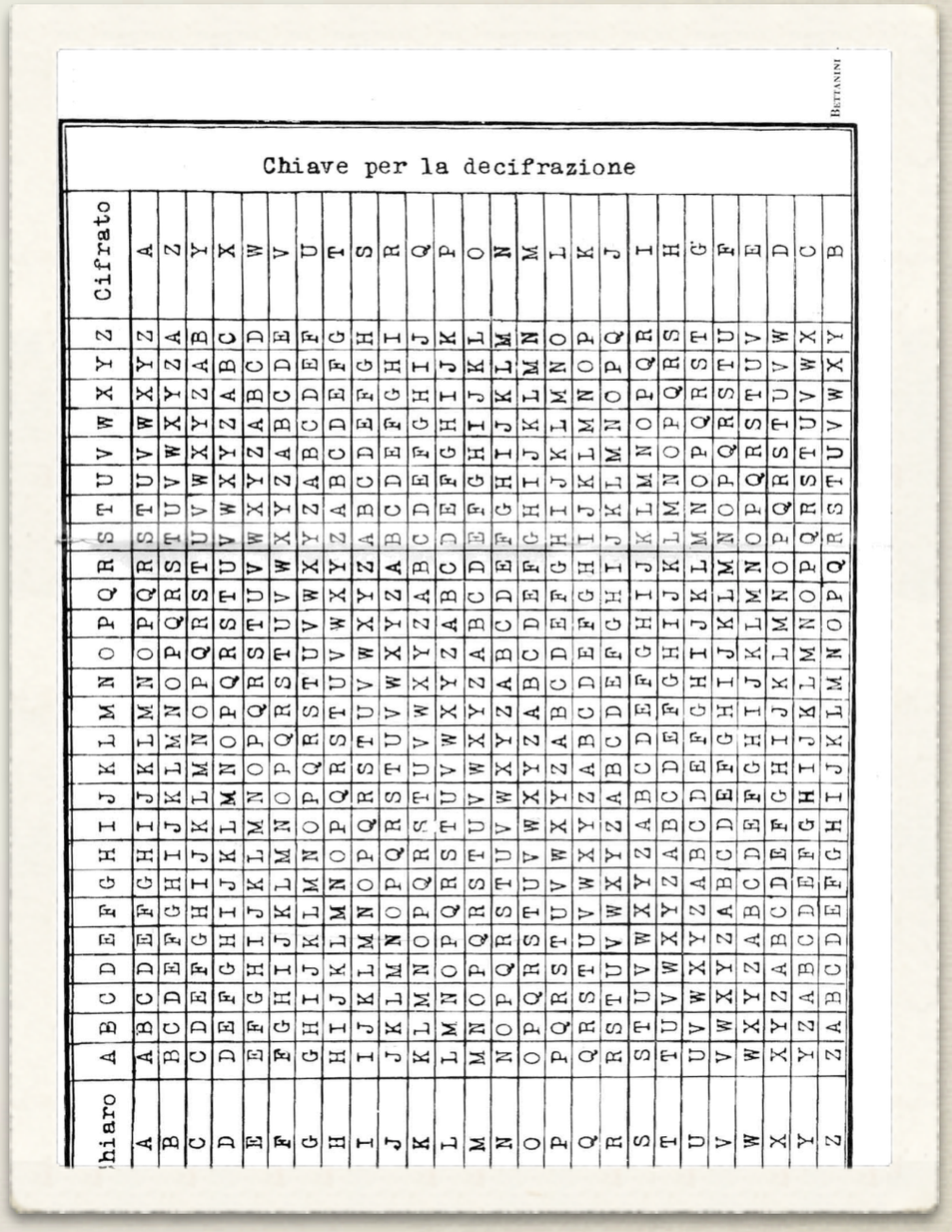
DESCRIZIONE ESPERIENZA

Ho presentato una lezione di Crittografia a classi diverse del liceo scientifico di Pistoia rivolgendomi in particolare a due categorie: una 4° e una 5° del corso normale ed una 4° e una 5° del corso PNI (curriculum scientifico).

Ho presentato la Crittografia secondo un percorso cronologico in modo da poter analizzare con gli studenti alcuni dei più importanti sistemi di cifratura della storia per comprenderne i punti forza e i limiti.

PERCORSO

- Cifratura di Cesare;
- Cifratura per permutazione;
- One Time Pad;
- Il problema dello scambio di chiavi.



Bettanini

Chiave per la decifrazione

Chiaro	Cifrato
A	A
B	Z
C	Y
D	X
E	W
F	V
G	U
H	T
I	S
J	R
K	Q
L	P
M	O
N	N
O	M
P	L
Q	K
R	J
S	I
T	H
U	G
V	F
W	E
X	D
Y	C
Z	B

Esempio con cifratura di Cesare

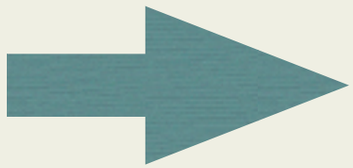
S'BVTV UVU WBV LZZLYL
WHYYALJPWL KLSSH
MLSPJPAH HSAYBP MPU
AHUAV JOL UVU ZP
ZLUAL LNSP ZALZZV
ZVKKPZMHAAV.

Esempio con cifratura di Cesare

S'BVTV UVU WBV LZZLYL
WHYALJPWL KLSSH
MLSPJPAH HSAYBP MPU
AHUAV JOL UVU ZP
ZLUAL LNSP ZALZZV
ZVKKPZMHAAV.

Esempio con cifratura di Cesare

S'BVTV UVU WBV LZZLYL
WHYALJPWL KLSSH
MLSPJPAH HSAYBP MPU
AHUAV JOL UVU ZP
ZLUAL LNSP ZALZZV
ZVKKPZMHAAV.



L'uomo non può essere partecipe della felicità altrui fin tanto che non si sente egli stesso soddisfatto.

Immanuel Kant

Problemi evidenti:

- Si attacca facilmente;
- Chiavi insufficienti.

Possibili soluzioni:

- Usare come cifrario non una traslazione delle lettere bensì una permutazione;
- Usare una diversa chiave a seconda della posizione della lettera: ad esempio crittando le lettere di posizione pari con una chiave e quelle di posizione dispari con un'altra.

Cifratura per permutazione

Usando una permutazione dell'alfabeto come chiave, il numero di cifrature diverse ottenibili da uno stesso testo in chiaro aumenta drasticamente, infatti posso cifrare:

Cifratura per permutazione

Usando una permutazione dell'alfabeto come chiave, il numero di cifrature diverse ottenibili da uno stesso testo in chiaro aumenta drasticamente, infatti posso cifrare:

* A in 26 modi diversi;
* B in 25 modi diversi;
* C in 24 modi diversi;
* ...
* Y in 2 modi diversi;
* Z con l'unica lettera rimasta

Cifratura per permutazione

Usando una permutazione dell'alfabeto come chiave, il numero di cifrature diverse ottenibili da uno stesso testo in chiaro aumenta drasticamente, infatti posso cifrare:

* A in 26 modi diversi;
* B in 25 modi diversi;
* C in 24 modi diversi;
* ...
* Y in 2 modi diversi;
* Z con l'unica lettera rimasta

per un totale di 26! permutazioni.

Cifratura per permutazione

Usando una permutazione dell'alfabeto come chiave, il numero di cifrature diverse ottenibili da uno stesso testo in chiaro aumenta drasticamente, infatti posso cifrare:

* A in 26 modi diversi;
* B in 25 modi diversi;
* C in 24 modi diversi;
* ...
* Y in 2 modi diversi;
* Z con l'unica lettera rimasta

per un totale di 26! permutazioni.

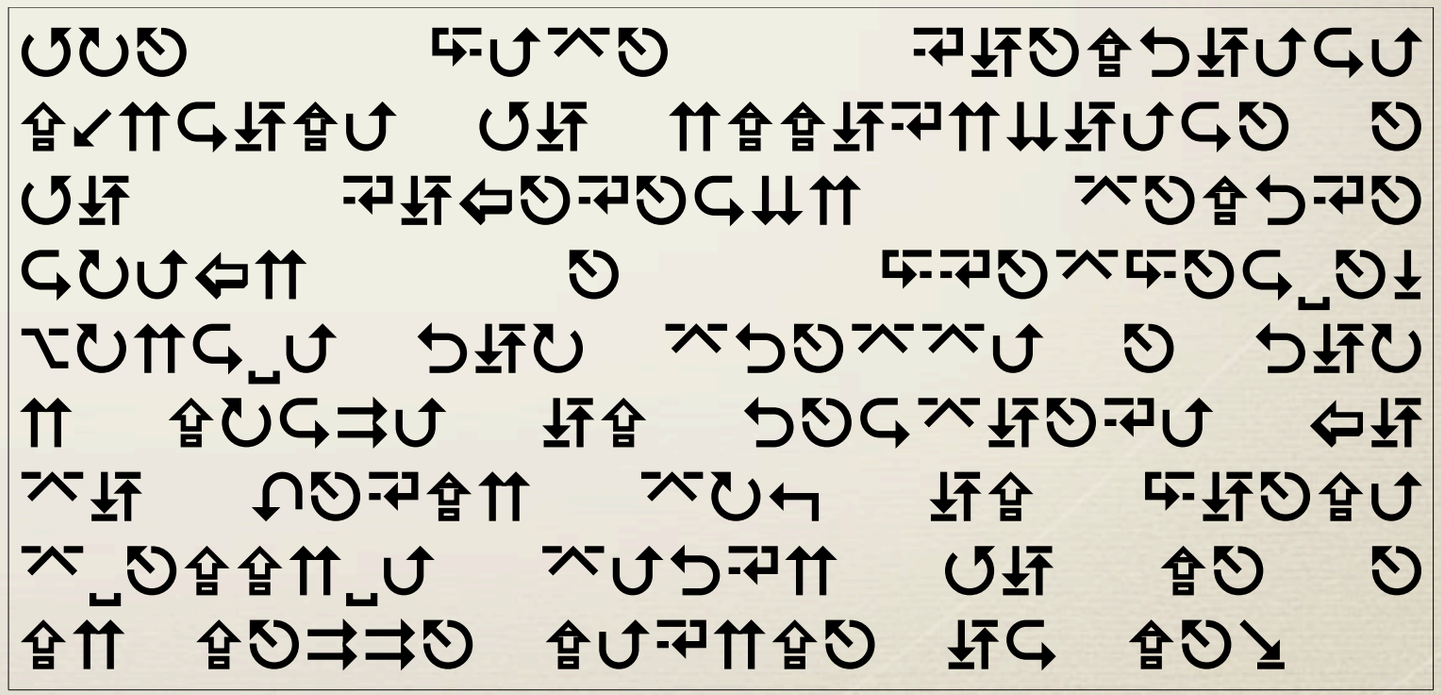
(26! > 5.000.000.000.000.000.000.000.000.000)

ESEMPIO:

QPR CMSR BGRYOGMNM X'JNGYM QG JYYGBJKGMNR R QG BGZRBRNKJ SRYOBR NPMZJ R CBRSCRNVR, UPJNVM OGP SORSSM R OGP J XPNIM GX ORNSGRBM ZG SG LRBYJ SP: GX CGRXM SVRXXJVM SMOBJ QG YR R XJ XRIIR YMBJXR GN YR.

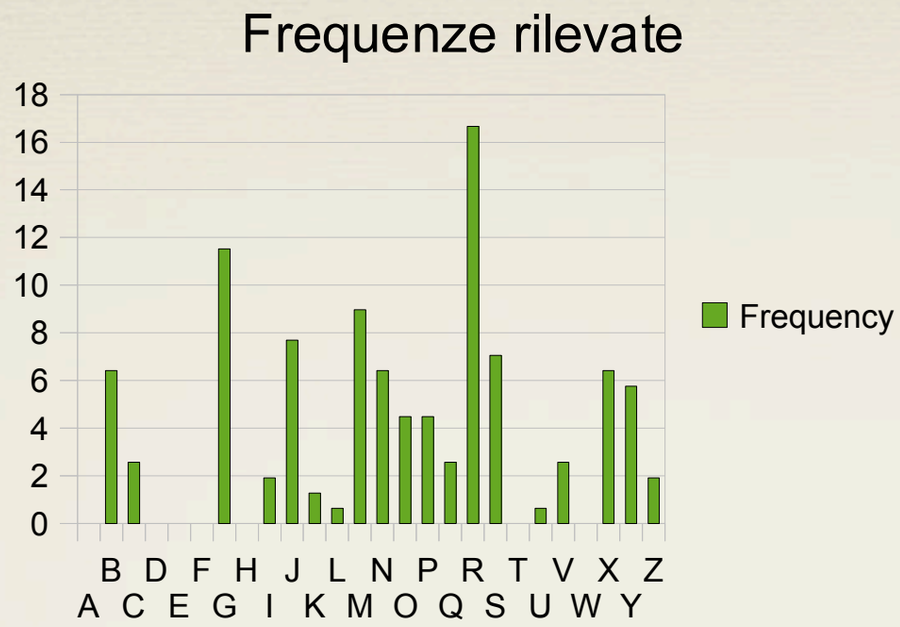
In questo caso è impossibile effettuare un attacco per tentativi (anche analizzando un caso al secondo potrebbero volerci anche 16 milioni di miliardi di anni).

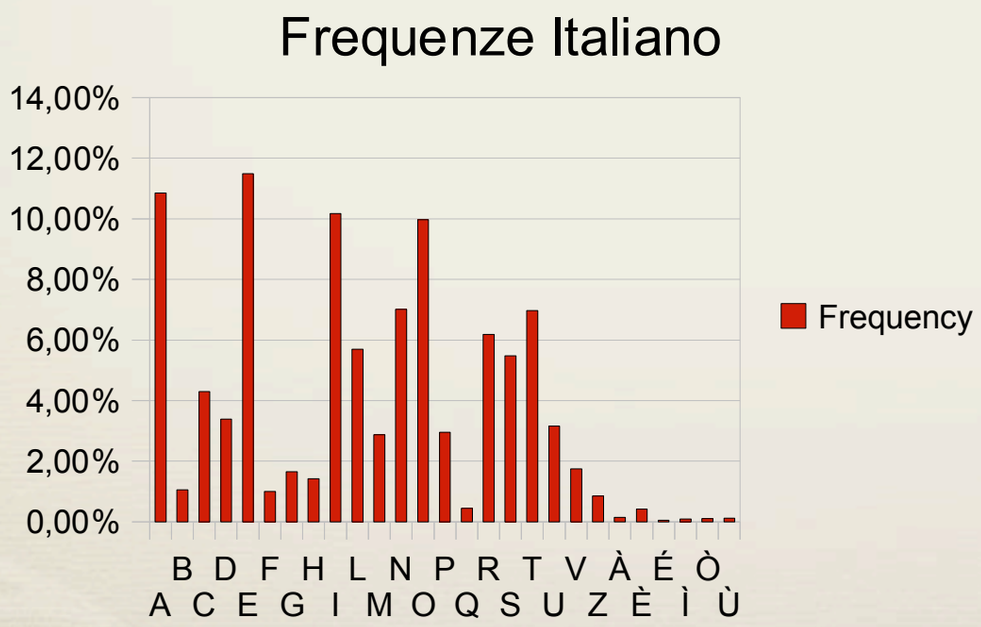
Si può comunque decifrare il codice analizzando la frequenza delle lettere/simboli e confrontandola con quella delle lettere nella lingua italiana:



ANALISI FREQUENZE

RILEV EMPIRICO		
Character		Number
A	↳	0
B	⇄	6,41
C	↳	2,56
D	⇆	0
E	↓↑	0
F	↳	0
G	↓↑	11,53
H	⇇	0
I	⇉	1,92
J	↑↑	7,69
K	↓↓	1,28
L	↶	0,64
M	↺	8,97
N	↳	6,41
O	↩	4,48
P	↻	4,48
Q	↺	2,56
R	↻	16,66
S	⌥	7,05
T	^	0
U	⌥	0,64
V	␣	2,56
W	␣	0
X	⇪	6,41
Y	⇪	5,76
Z	⇦	1,92



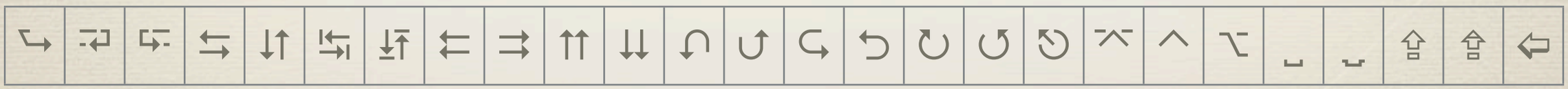


FREQ EMPIRICHE		
Character		Emp Freq.
R	↻	16,66
G	↓↑	11,53
M	↺	8,97
J	↑↑	7,69
S	⌥	7,05
B	⇄	6,41
N	↳	6,41
X	⇪	6,41
Y	⇪	5,76
O	↩	4,48
P	↻	4,48
C	↳	2,56
Q	↺	2,56
V	␣	2,56
I	⇉	1,92
Z	⇦	1,92
K	↓↓	1,28
L	↶	0,64
U	⌥	0,64
A	↳	0
D	⇆	0
E	↓↑	0
F	↳	0
H	⇇	0
T	^	0
W	␣	0

FREQ ITALIANO	
Character	Frequency
E	11,49%
A	10,85%
I	10,18%
O	9,97%
N	7,02%
T	6,97%
R	6,19%
L	5,70%
S	5,48%
C	4,30%
D	3,39%
U	3,16%
P	2,96%
M	2,87%
V	1,75%
G	1,65%
H	1,43%
B	1,05%
F	1,01%
Z	0,85%
Q	0,45%
È	0,42%
À	0,15%
Ù	0,12%
Ò	0,11%
Ì	0,09%
É	0,06%

Tentando sostituzioni tra lettere con frequenza simile si può effettuare un attacco per tentativi “guidato” e ricavare la permutazione risolvente in tempi ragionevoli:

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

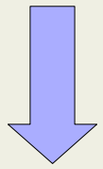


Sostituendo si ricava la celebre frase di Kant:

QPR CMSR BGRYOGMNM X'JNGYM QG
JYYGBJKGMNR R QG BGZRBRNKJ SRYOBR
NPMZJ R CBRSCRNVR, UPJNVM OGP SORSSM R
OGP J XPNIM GX ORNSGRBM ZG SG LRBYJ SP:
GX CGRXM SVRXXJVM SMOBJ QG YR R XJ XRIIR
YMBJXR GN YR.

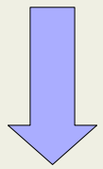
Sostituendo si ricava la celebre frase di Kant:

QPR CMSR BGRYOGMNM X'JNGYM QG
JYYGBJKGMNR R QG BGZRBRNKJ SRYOBR
NPMZJ R CBRSCRNVR, UPJNVM OGP SORSSM R
OGP J XPNIM GX ORNSGRBM ZG SG LRBYJ SP:
GX CGRXM SVRXXJVM SMOBJ QG YR R XJ XRIIR
YMBJXR GN YR.



Sostituendo si ricava la celebre frase di Kant:

QPR CMSR BGRYOGMNM X'JNGYM QG
JYYGBJKGMNR R QG BGZRBRNKJ SRYOBR
NPMZJ R CBRSCRNVR, UPJNVM OGP SORSSM R
OGP J XPNIM GX ORNSGRBM ZG SG LRBYJ SP:
GX CGRXM SVRXXJVM SMOBJ QG YR R XJ XRIIR
YMBJXR GN YR.

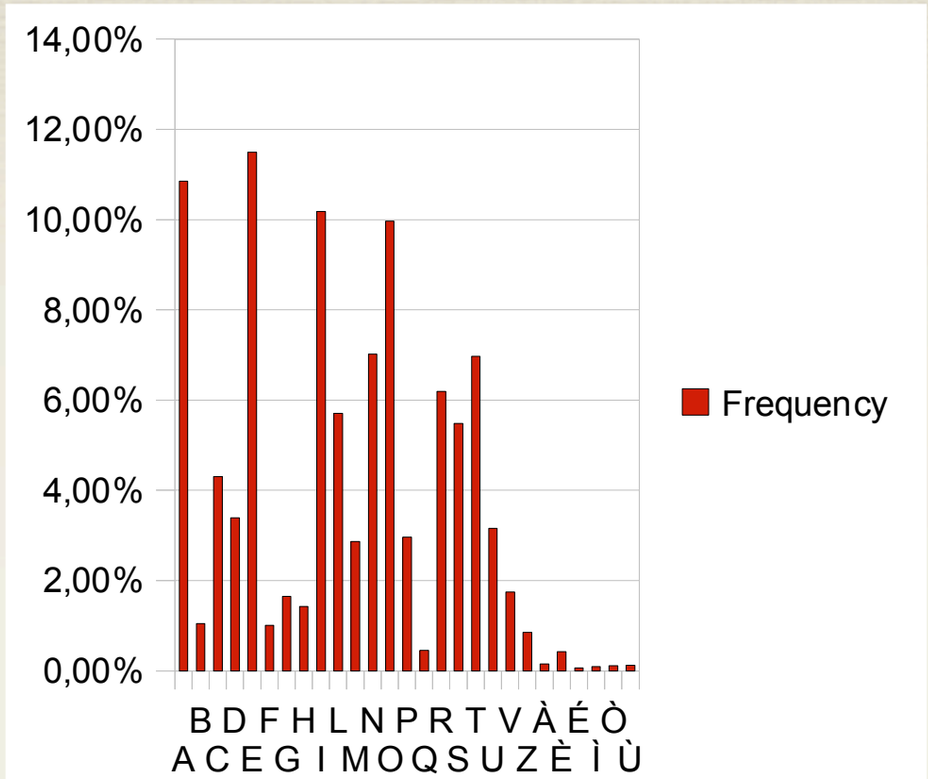


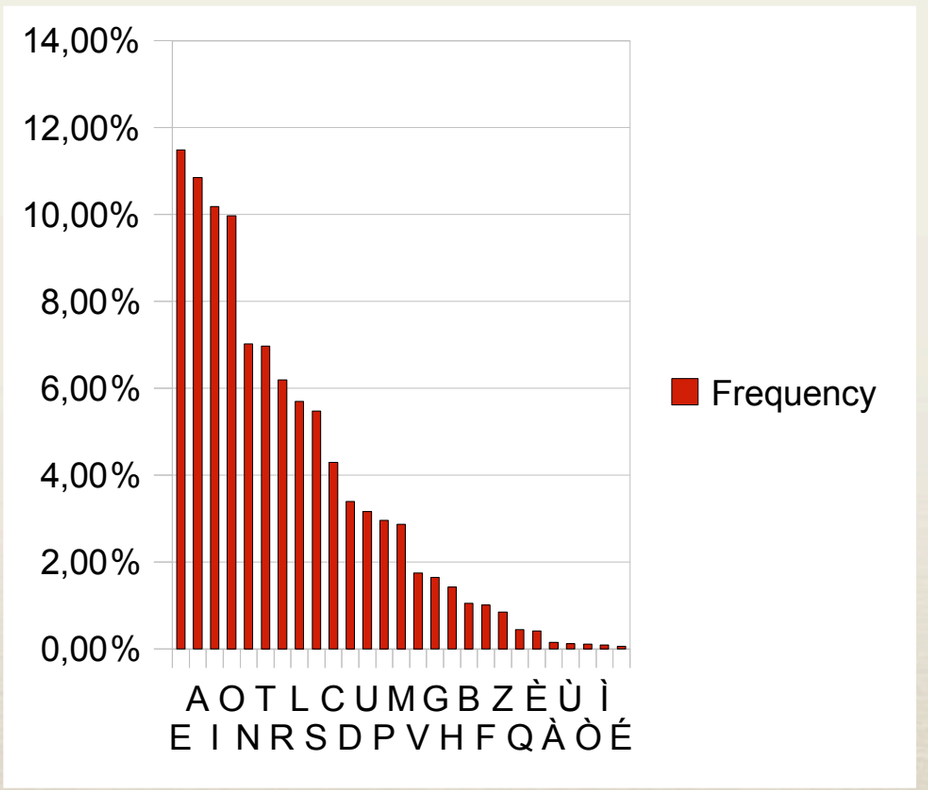
Due cose riempiono l'animo di ammirazione e di riverenza sempre nuova e crescente, quanto più spesso e più a lungo il pensiero vi si ferma su: il cielo stellato sopra di me e la legge morale in me.

Immanuel Kant

FREQUENZE ITALIANO

Character	Frequency
A	10,85%
B	1,05%
C	4,30%
D	3,39%
E	11,49%
F	1,01%
G	1,65%
H	1,43%
I	10,18%
L	5,70%
M	2,87%
N	7,02%
O	9,97%
P	2,96%
Q	0,45%
R	6,19%
S	5,48%
T	6,97%
U	3,16%
V	1,75%
Z	0,85%
À	0,15%
È	0,42%
É	0,06%
Ì	0,09%
Ò	0,11%
Ù	0,12%

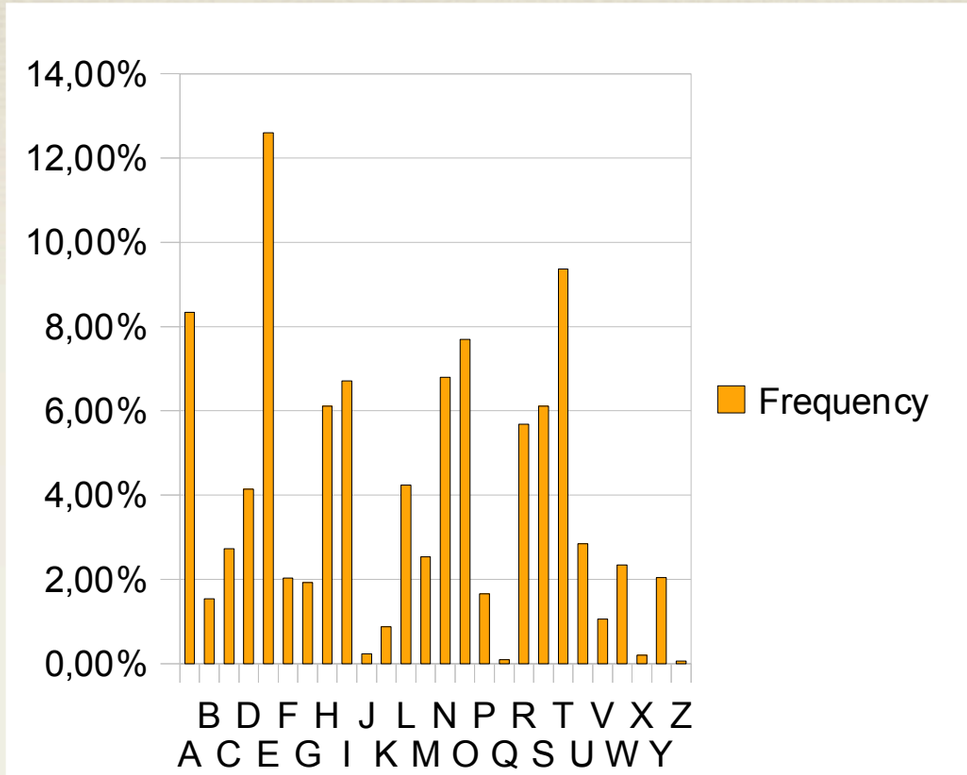


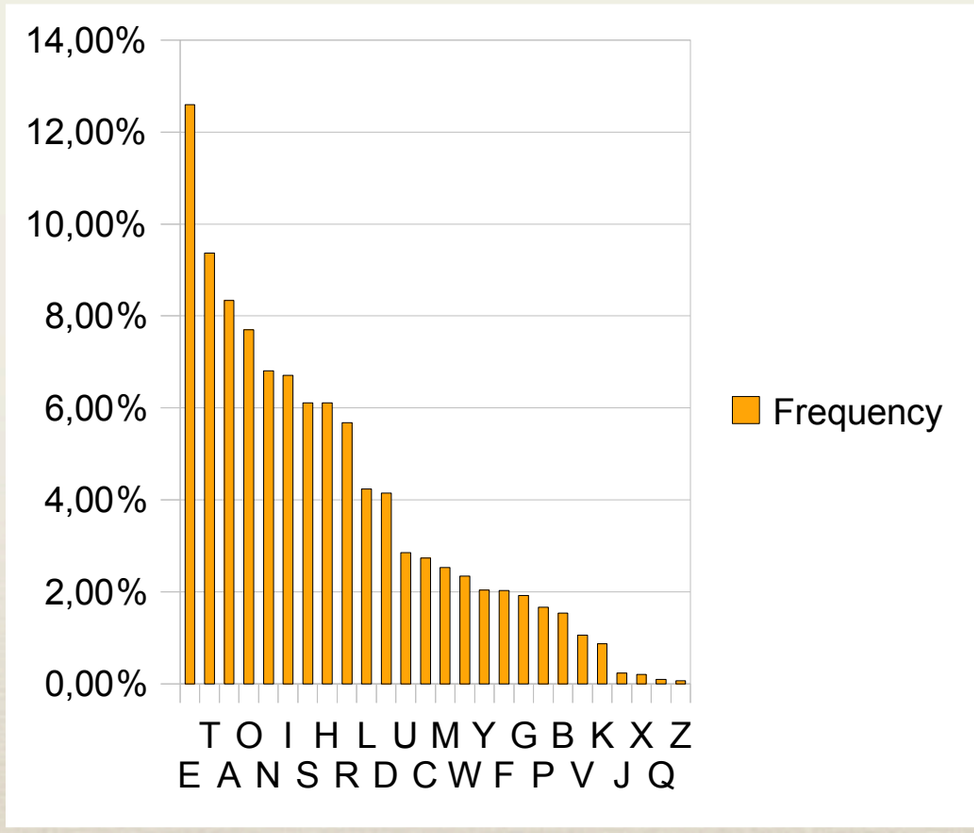


Character	Frequency
E	11,49%
A	10,85%
I	10,18%
O	9,97%
N	7,02%
T	6,97%
R	6,19%
L	5,70%
S	5,48%
C	4,30%
D	3,39%
U	3,16%
P	2,96%
M	2,87%
V	1,75%
G	1,65%
H	1,43%
B	1,05%
F	1,01%
Z	0,85%
Q	0,45%
È	0,42%
À	0,15%
Ù	0,12%
Ò	0,11%
Ì	0,09%
É	0,06%

FREQUENZE INGLESE

Character	Frequency
A	8,34%
B	1,54%
C	2,73%
D	4,14%
E	12,60%
F	2,03%
G	1,92%
H	6,11%
I	6,71%
J	0,23%
K	0,87%
L	4,24%
M	2,53%
N	6,80%
O	7,70%
P	1,66%
Q	0,09%
R	5,68%
S	6,11%
T	9,37%
U	2,85%
V	1,06%
W	2,34%
X	0,20%
Y	2,04%
Z	0,06%

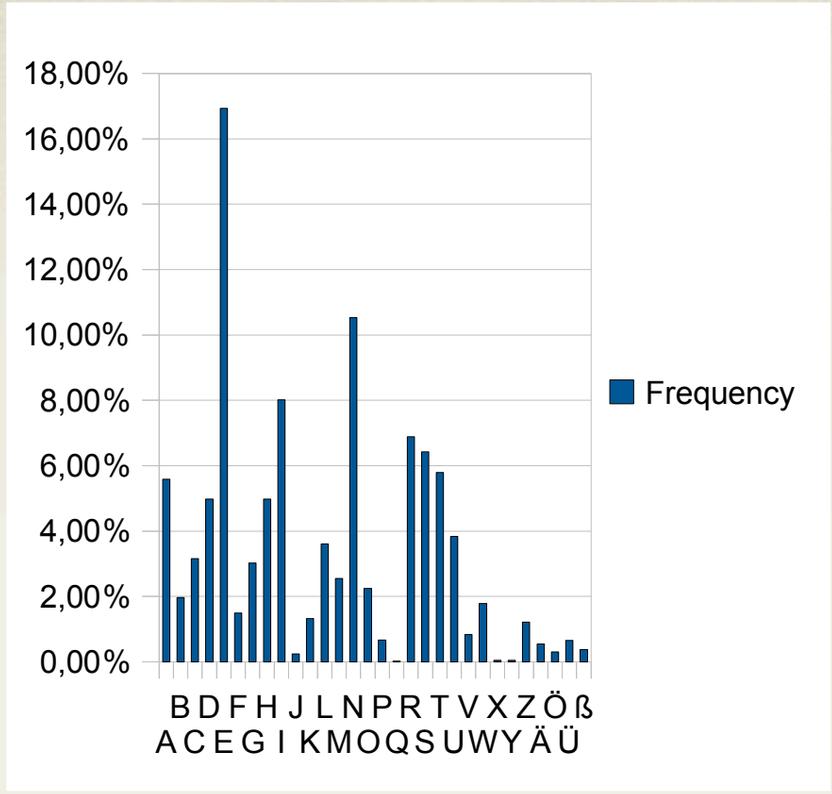


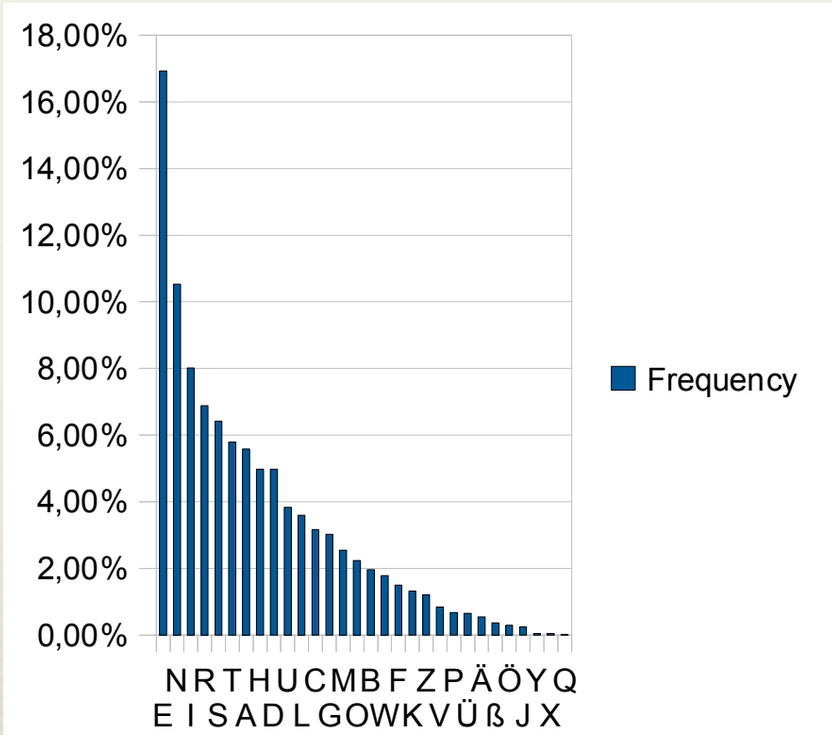


Character	Frequency
E	12,60%
T	9,37%
A	8,34%
O	7,70%
N	6,80%
I	6,71%
S	6,11%
H	6,11%
R	5,68%
L	4,24%
D	4,14%
U	2,85%
C	2,73%
M	2,53%
W	2,34%
Y	2,04%
F	2,03%
G	1,92%
P	1,66%
B	1,54%
V	1,06%
K	0,87%
J	0,23%
X	0,20%
Q	0,09%
Z	0,06%

FREQUENZE TEDESCO

Character	Frequency
A	5,58%
B	1,96%
C	3,16%
D	4,98%
E	16,93%
F	1,49%
G	3,02%
H	4,98%
I	8,02%
J	0,24%
K	1,32%
L	3,60%
M	2,55%
N	10,53%
O	2,24%
P	0,67%
Q	0,02%
R	6,89%
S	6,42%
T	5,79%
U	3,83%
V	0,84%
W	1,78%
X	0,05%
Y	0,05%
Z	1,21%
Ä	0,54%
Ö	0,30%
Ü	0,65%
ß	0,37%





Character	Frequency
E	16,93%
N	10,53%
I	8,02%
R	6,89%
S	6,42%
T	5,79%
A	5,58%
H	4,98%
D	4,98%
U	3,83%
L	3,60%
C	3,16%
G	3,02%
M	2,55%
O	2,24%
B	1,96%
W	1,78%
F	1,49%
K	1,32%
Z	1,21%
V	0,84%
P	0,67%
Ü	0,65%
Ä	0,54%
ß	0,37%
Ö	0,30%
J	0,24%
Y	0,05%
X	0,05%
Q	0,02%

Problemi della cifratura per permutazioni:

- Suscettibile ad un attacco delle frequenze;
- La struttura del linguaggio offre informazioni sul testo in chiaro.

Possibili soluzioni:

- Eliminare la struttura del linguaggio (per quanto possibile) nel testo cifrato.
- Usare una diversa chiave a seconda della posizione della lettera.

One Time Pad

(semplificato)

Si genera una lista casuale di lettere (numeri) lunga quanto il messaggio da trasmettere, si affianca al messaggio e si cifra ogni lettera del messaggio in chiaro con la cifratura di Cesare corrispondente:

Esempio:

```
Testo in chiaro: C  I  A  O
Chiave:          A  J  R  F
                (0  9 18  5)
-------------------------------
Testo cifrato:   C  R  R  T
```

Osservazioni:

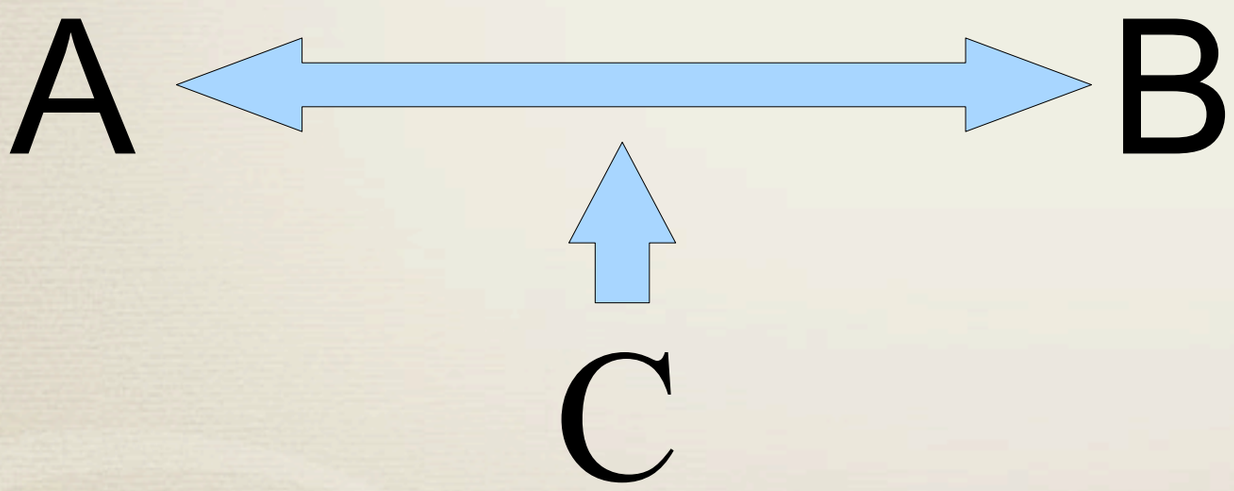
- Indecifrabile: il testo cifrato non dà nessuna informazione sul testo in chiaro.

Problemi e limiti:

- Scomodissimo dal punto di vista pratico;
- Difficoltà di generare sequenze casuali;
- Bisogna trovare un percorso sicuro su cui scambiare la chiave ogni volta che finiamo la sequenza.

Un grosso problema: lo scambio di chiavi

In tutti i casi precedenti sussisteva il problema dello scambio della chiave che doveva avvenire in precedenza o attraverso un percorso sicuro alternativo (che di solito non c'è visto se abbiamo la necessità di crittare dei messaggi).



E' plausibile quindi pensare che C possa intercettare la chiave che viene scambiata su un percorso tecnicamente non sicuro.

Metodo del doppio lucchetto

Alice e Bob vogliono trasmettersi in maniera sicura una chiave K per comunicare su un percorso non sicuro. Data allora una opportuna funzione di cifratura (one-way) ciascuno dei due sceglie individualmente una chiave (lucchetto) da usare. A questo punto procedono come segue:

* A mette il suo lucchetto alla chiave K e la spedisce a B;
* B mette il suo lucchetto e spedisce il risultato a A;
* A toglie il suo lucchetto e rispedisce il risultato a B;
* B toglie il suo lucchetto e finalmente ritrova K.

Avendo scelto le chiavi individualmente nessuno dei due sa togliere il lucchetto dell'altro e, un eventuale C che intercettasse la comunicazione, si troverebbe di fronte sempre ad un messaggio con almeno un lucchetto e mai alla chiave K.

Questo metodo, per quanto sicuro, è pesante dal punto di vista computazionale perciò conviene usarlo solo per trasmettersi la chiave che poi verrà usata per comunicare per un più lungo tempo sul percorso non sicuro.

OBIETTIVI

- Stimolare curiosità;
- Utilizzare le conoscenze acquisite e il ragionamento per affrontare una problematica;
- Integrare l'analisi matematica con una visione d'insieme;
- Indurre gli studenti ad usare l'intuizione libera come base di riflessione

DIFFICOLTA' ATTESA

Mi aspettavo che gli studenti avessero difficoltà ad inventarsi soluzioni basate semplicemente sulla propria intuizione e a presentarle senza timore visto che la paura di fare domande stupide è abbastanza diffusa.

Mi aspettavo una ulteriore difficoltà per quegli studenti che ancora non concepivano la matematica come un mezzo per affrontare delle problematiche.

DIFFICOLTA' RISCONTRATE

Classi Normali:

gli studenti hanno partecipato in maniera attiva pur non riuscendo quasi mai a rispondere correttamente alle domande indotte dalla lezione.

Classi PNI:

interventi meno densi ma decisamente più coerenti e costruttivi; in alcuni casi ho avuto io difficoltà a rispondere alle idee di alcuni studenti.