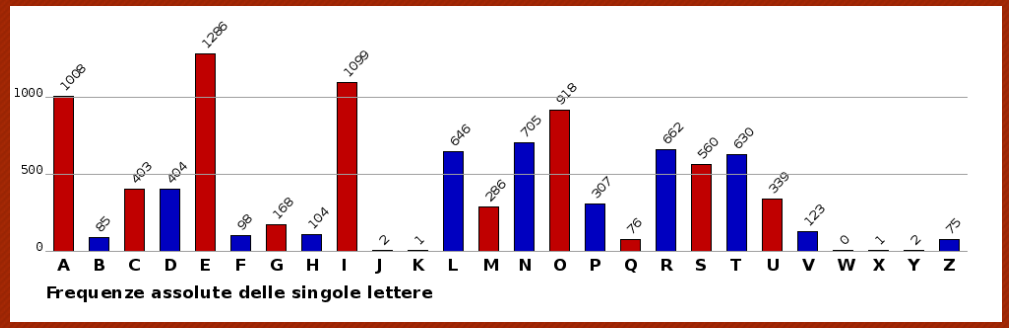
Mathesis Venezia

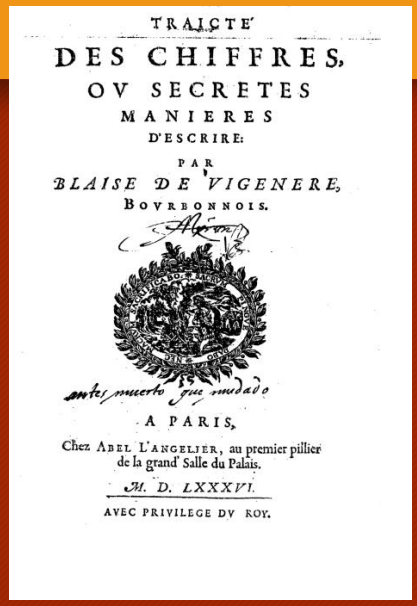
Convitto Nazionale Marco Foscarini Venezia



Crittografia a Venezia tra matematica e storia 2

La Crittografia come matematica applicata

La Crittografia come strumento di ricerca storica


TRAICTE'
DES CHIFFRES,
OV SECRETES
MANIERES
D'ESCRIRE:
PAR
BLAISE DE VIGENERE,
BOVRBONNOIS.
A PARIS,
Chez ABEL L'ANGELIER, au premier pillier de la grand' Salle du Palais.
M. D. LXXXVI.
AVEC PRIVILEGE DV ROY.

Classificazione dei cifrari

- Cifrari per **sostituzione**
- Cifrari per **trasposizione**

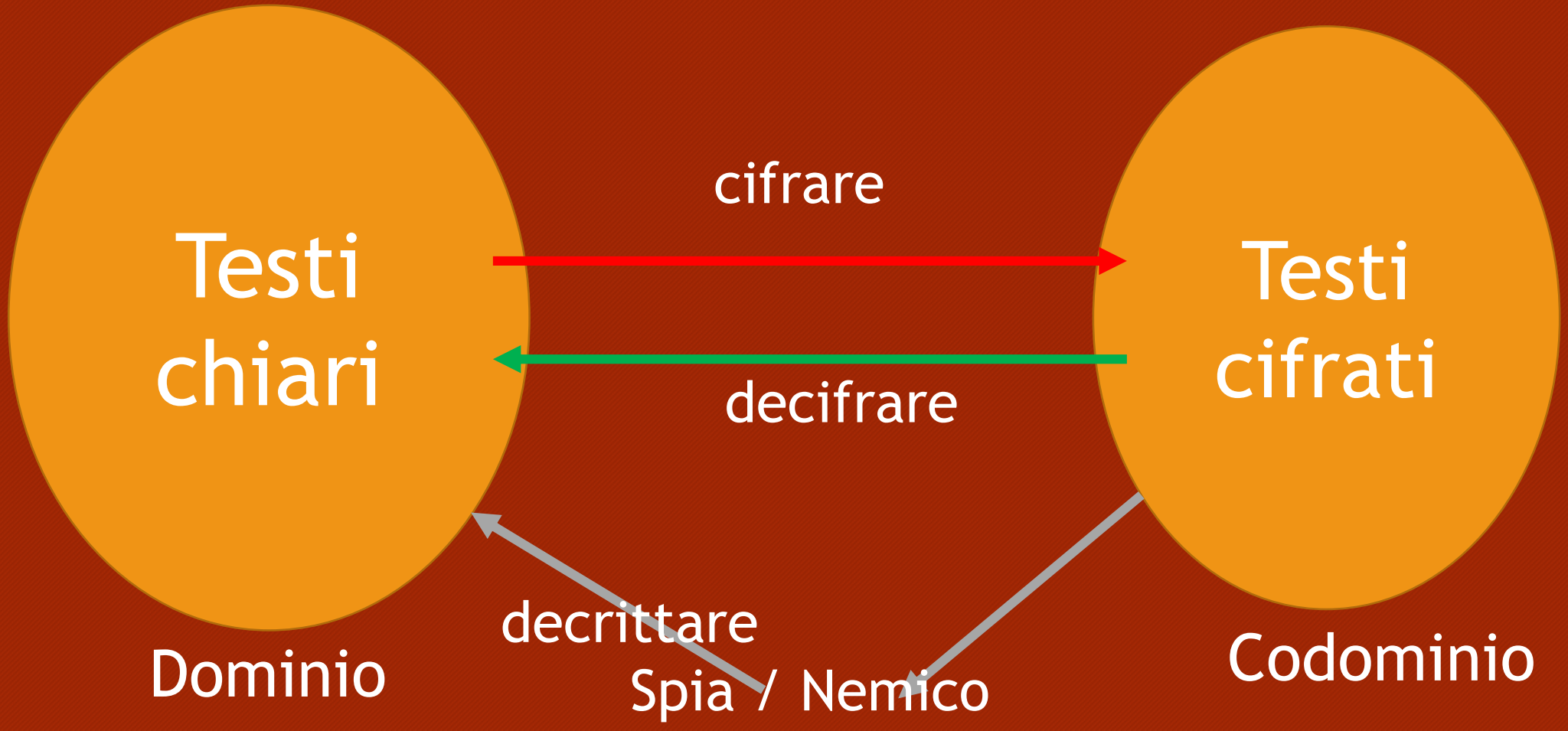
Il testo cifrato si ottiene sostituendo
Parti del testo **chiaro**
(lettere, sillabe, parole)
con
Segni cifranti
(lettere, numeri, segni di fantasia)

Il testo cifrato si ottiene sostituendo
Rimescolando
Il testo chiaro
Secondo una qualche regola
reversibile

Piccolo glossario

- **Chiave:** parola chiave, lista, tabella che permette di cifrare e decifrare.
- **Crittografia**: l'arte di scrivere in modo segreto.
- **Crittologia**: la scienza delle scritture segrete.
- **Crittoanalisi** : l'arte e i metodi per decrittare messaggi cifrati.
- **Cifra**: un metodo per scrivere in modo segreto.
- **Cifrario**: foglio, volume o altro dispositivo che realizza una cifra.
- **Cifrare**: scrivere in cifra, in modo segreto, usando un cifrario
- **Decifrare**: da un messaggio cifrato recuperare il testo chiaro in modo legittimo usando un cifrario.
- **Decrittare**: da un messaggio cifrato recuperare il testo chiaro senza conoscere il cifrario, usando i medodi della crittoanalisi.

Cifrari come relazioni



Crittografia, relazioni, funzioni

argomenti della "matematica di base" che potranno figurare nella prova scritta di matematica

11. Analizzare le proprietà di iniettività, suriettività, invertibilità di funzioni definite su insiemi qualsiasi. Riconoscere ed applicare la composizione di funzioni.

- I cifrari sono **funzioni** in generale **relazioni** tra l'insieme dei messaggi in chiaro (dominio) e l'insieme dei messaggi cifrati (codominio).
- In teoria ci aspetteremmo una corrispondenza biunivoca ma non sempre è così.
- Nella crittografia classica, come la precedente, la relazione chiaro-> cifrato raramente è biunivoca (monoalfabetica).

Crittografia: sempre funzioni?

- La relazione cifrante non è ovunque definita: spazi, segni di interpunzione non vengono cifrati.
- La relazione cifrante non è univoca; cifratura per ***omofoni***, una stessa lettera si può cifrare con segni diversi, per confondere la statistica.
- La funzione cifrante non è suriettiva, alcuni segni cifranti, detti ***nulle***, non hanno corrispondente in chiaro, sempre per confondere il nemico.
- La funzione cifrante non è iniettiva, alcuni segni cifranti, detti ***polifoni***, hanno più significati; da risolvere in base al contesto (raro)

Ovunque definita	**Solo maiuscole**
Univoca	**Omofoni**
Suriettiva	**Nulle**
Iniettiva	**Polifoni**

I cifrari più antichi : il bastone di Licurgo

CORD
IALI
SALV
TIXY

CIST OAAI RLLX DIVY

XY sono usate come riempitivo.
E' una buona idea usare X Y??

Questo è un esempio di **trasposizione semplice**.

I cifrari più antichi: Atbash e Cesare

ABCDEFGHIKLM
ZYXWVTSRQPON

ABCDEFGHIKLMNOPQRSTVX
DEFGHIKLMNOPQRSTVXABC

CORDIALISALVTI
XLHWQZOQGZOEFQ

CORDIALISALVTI
FRVGMDOMXDOBAM

Sono esempi di cifra monoalfabetica.

Decifrare e decrittare Cesare

Decifrare: *tradurre legittimamente un cifrato disponendo della chiave.*
Decrittare: *tradurre illegittimamente un cifrato ricostruendo la chiave.*

Ci sono 26 cifre di Cesare possibili.
Bastano 26 tentativi per decrittare.

```
ABCDEFGHIKLMNOPQRSTVX
BCDEFGHIKLMNOPQRSTVXA

ABCDEFGHIKLMNOPQRSTVX
CDEFGHIKLMNOPQRSTVXAB

ABCDEFGHIKLMNOPQRSTVX
DEFGHIKLMNOPQRSTVXABC

...
```

I cifrari monoalfabetici

ABCDEFGHIJKLMNOPQRSTUVWXYZ *Alfabeto Chiaro*
DUEIQRYGTJVXAFNKLWZMSOPHBC *Alfabeto Cifrante*

Cifra monoalfabetica: si cifra lettera per lettera.
Relazione **1:1**, biunivoca.
La chiave è la lista o alfabeto cifrante.
Metodo mnemonico (poco sicuro!!) con chiave **Montevideo**:

ABCDEFGHIJKLMNOPQRSTUVWXYZ *Alfabeto Chiaro*
MONTEVIDABCFGHJKLPQRSUWXYZ *Alfabeto Cifrante*

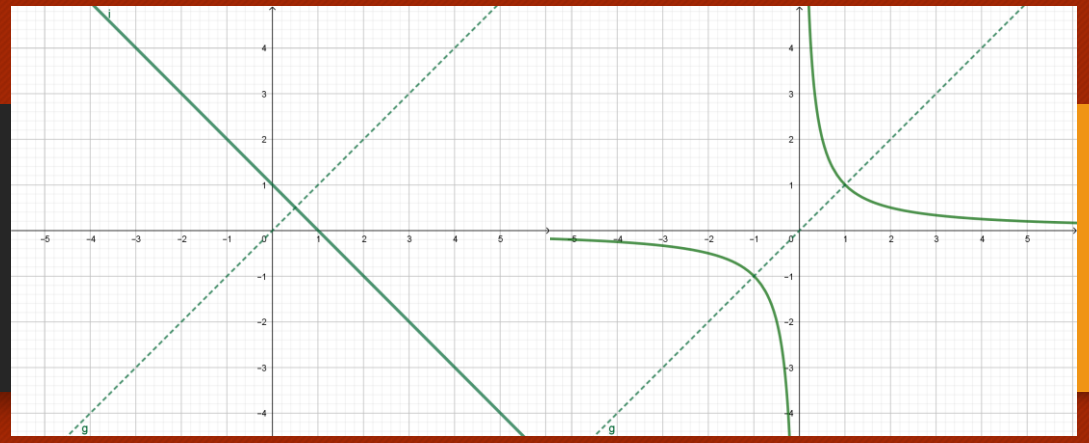
Quanti alfabeti cifranti sono possibili?

ABCDEFGHIJKLMNOPQRSTUVWX *Alfabeto Chiaro*
DUEIQRGTJVXAFNKLWMSOPHBC *Alfabeto Cifrante*

N = 26x25 x24 … x1 = 26! = *(fattoriale)*
403.291.461.126.605.635.584.000.000 **27 cifre!!!!**

Numero spaventoso, fuori portata per gli umani.
Quindi … questa cifra è inattaccabile!!

Liste involutorie o reciproche



ABCDEFGHIJKLM
NOPQRSTUVWXYZ
Lista ordinata

ABCDEFGHIJKLM
XQRYVTNZPSUOW
Lista disordinata

Da Atbash in poi le liste involutorie hanno goduto di una certa popolarità; godono della proprietà simmetrica, qui per esempio **A** si cifra con **N**, **N** si cifra con **A, ecc.ecc.**

Il grande vantaggio è che la funzione cifrante coincide con la funzione decifrante.

Funzioni involutorie esistono anche in matematica, tra insiemi numerici, per esempio:

$y = 1 - x$ retta, scritta in forma implicita $x + y = 1$

$y = \frac{1}{x}$ iperbole equilatera $xy = 1$

Matematicamente la funzione coincide con la sua inversa.

La cifra monoalfabetica è inattaccabile?

N = 26! = 403.291.461.126.605.635.584.000.000 = $4x10^{27}$

Numero spaventoso come già visto; molto meno spaventoso per le liste involutorie:

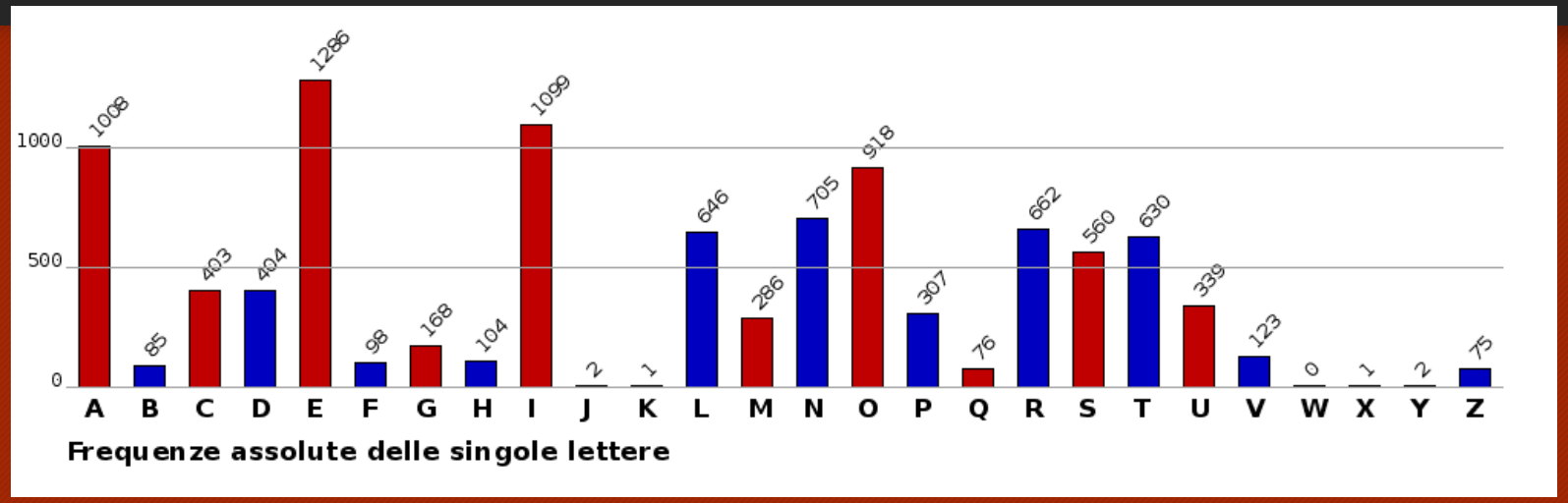
N = 13! = 6227020800

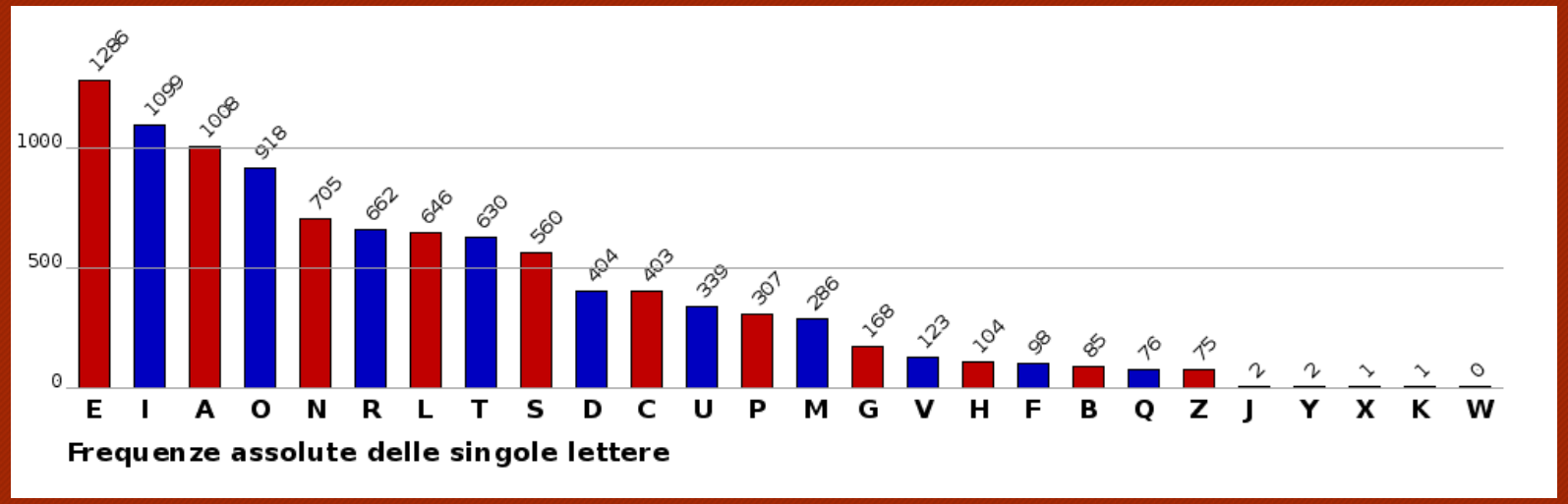
Ma questo numero misura solo il cosiddetto ***spazio delle chiavi*** che non è affatto una misura della sicurezza, infatti …

Esiste la statistica con i suoi metodi!

Strumento formidabile per il crittoanalista.

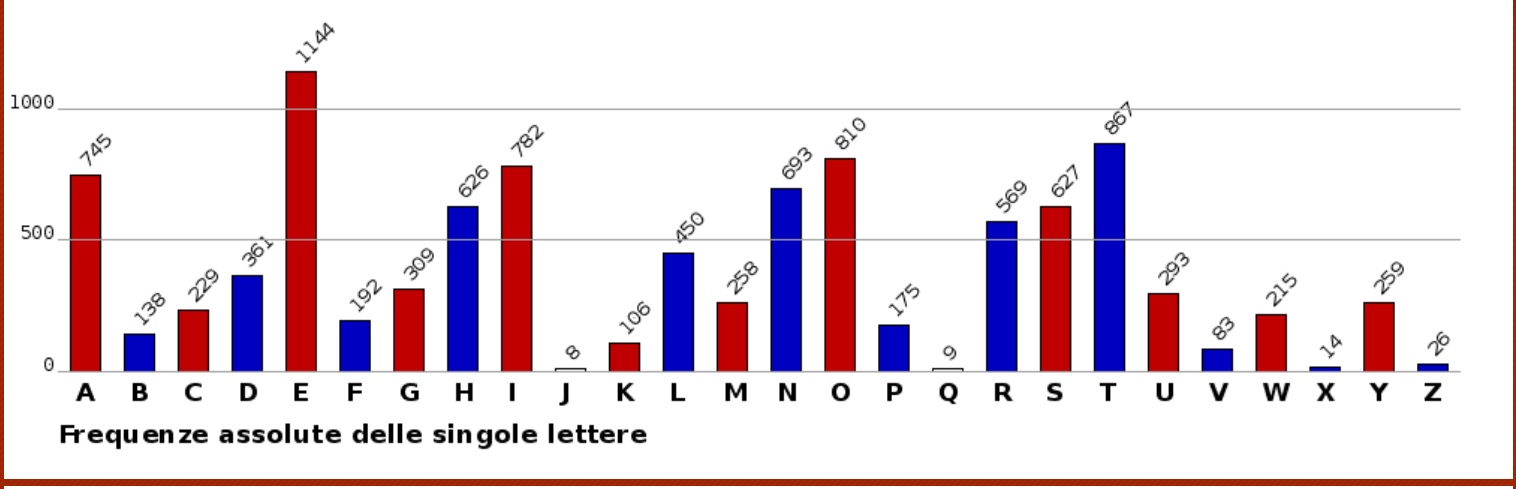
Crittografia e statistica

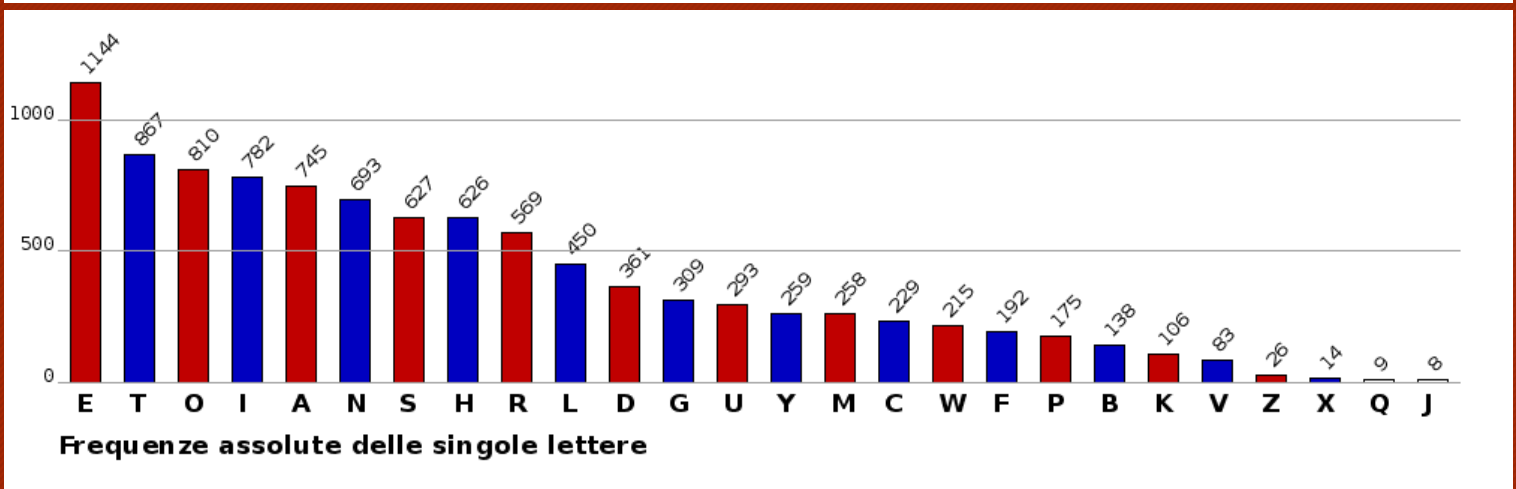




- Nella crittografia classica l'arma più potente per il crittoanalista è la statistica;
- Ogni lingua ha un distribuzione statistica caratteristica, quasi un'impronta digitale.
- Qui accanto quella della lingua italiana.
- Rare: J Y X K W
- Vocali A E I O U : 46%

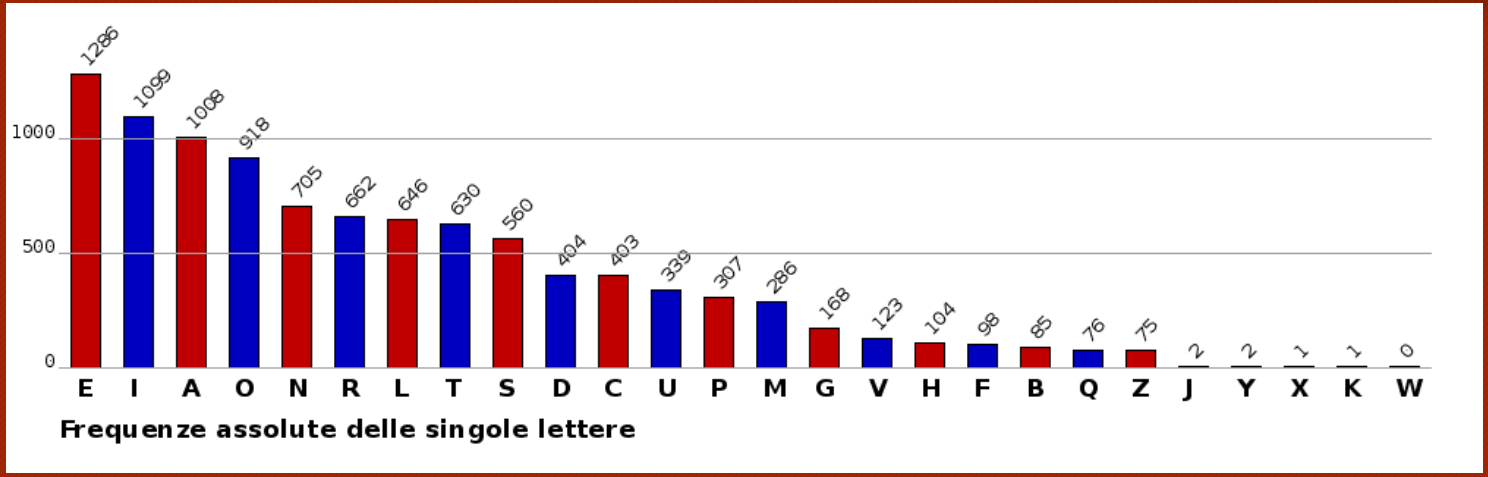
Crittografia e statistica: lingua inglese

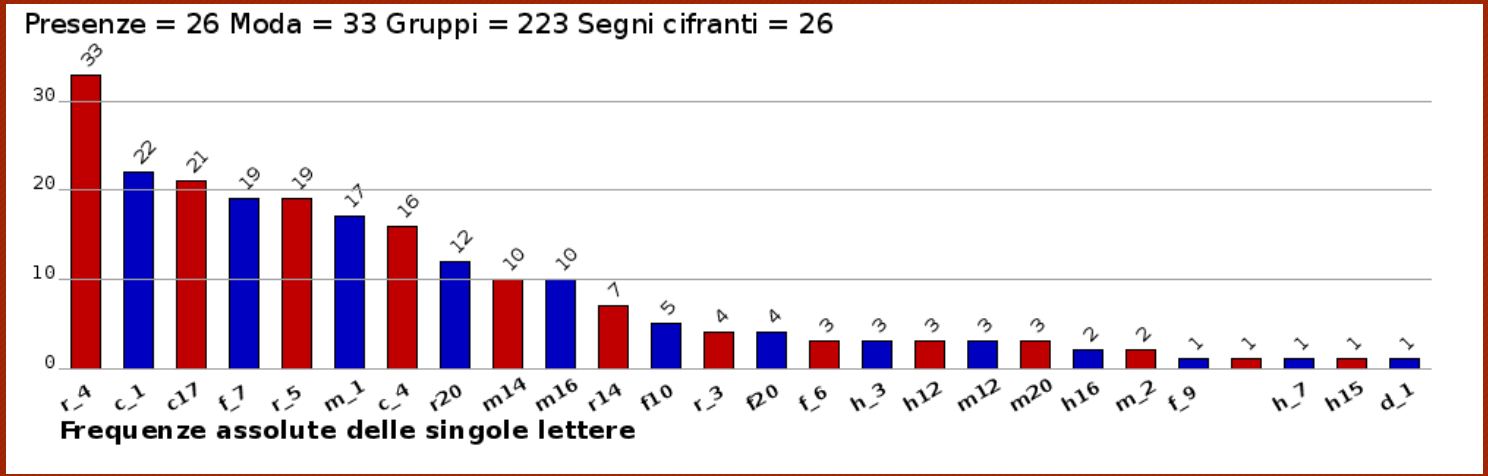




- Frequenze della lingua inglese, su 10000 lettere.
- La più frequente è sempre la E, come in molte lingue europee.
- Seconda la T (*the*, *this*, *that* …)
- Vocali un po’ meno che in italiano.
- Rare: Z X Q J
- Vocali AEIOUY 39%

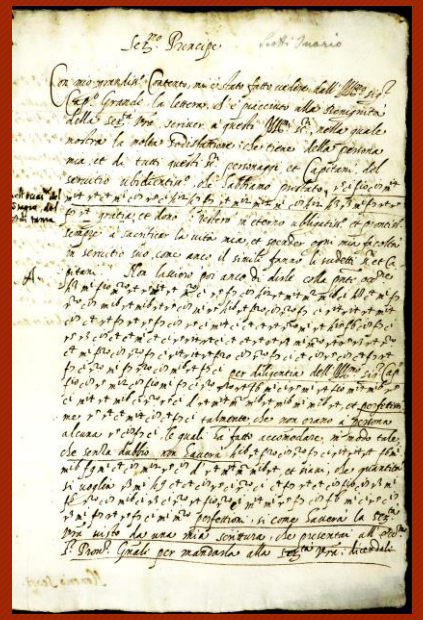
Confronto tra dati attesi e dati osservati





- Frequenze delle lettere nella lingua italiana, su 10000 lettere.
- Questi sono i dati attesi *(expected)*

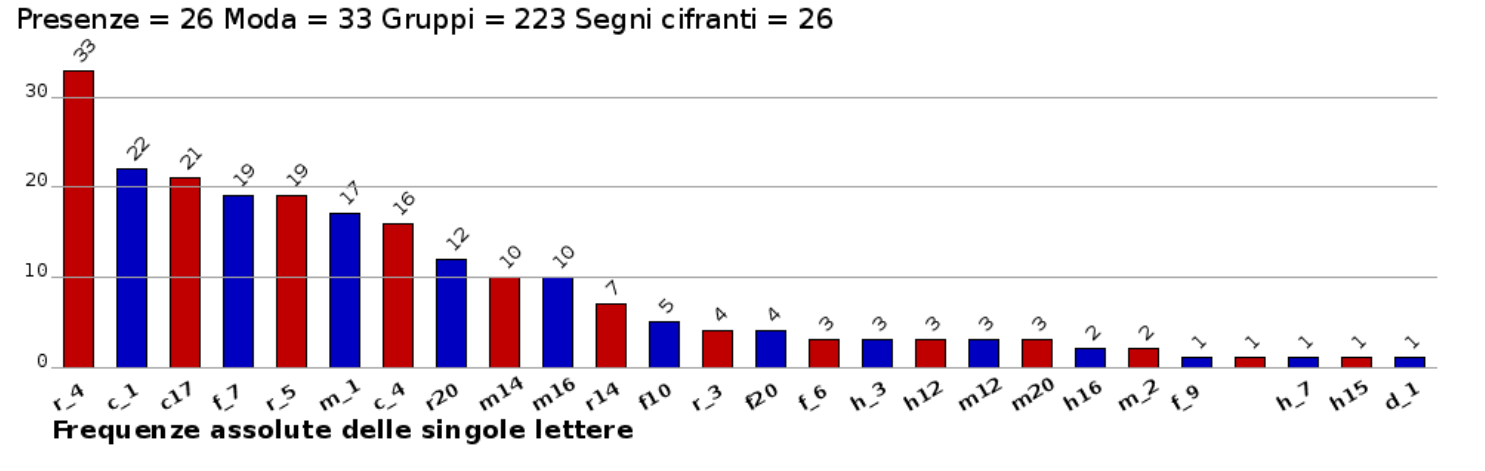
- Frequenze osservate nel dispaccio da Candia del 1590
- Questi sono i dati osservati *(observed)*



Confronto tra dati attesi e dati osservati

ALFABETO																		
a	b	c	d	e	f	g	i	l	m	n	o	p	q	r	s	t	u	z
r_4	f_9	m14	r_3	c_1	f20	m12	m_1	f10	m20	r_5	c17	f_6	m_2	r20	c_4	f_7	m16	r14

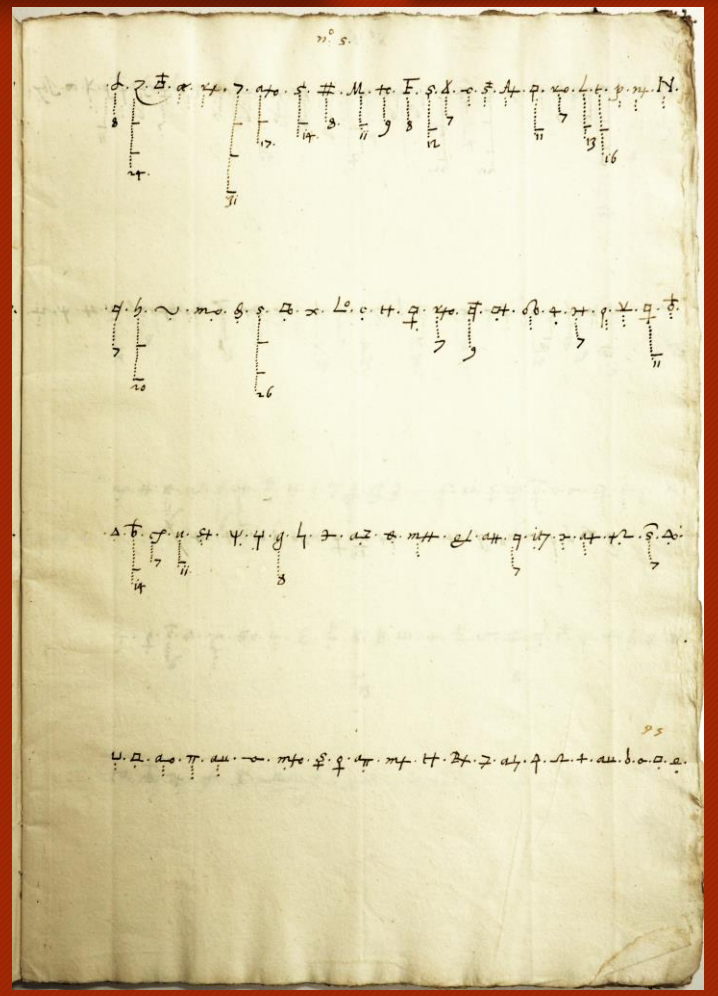
DIZIONARIO									
che	h_3	con	h_7	del	h12	non	h15	quel	h16



- Ecco il cifrario ricostruito per tentativi.
- Le più frequente qui risulta **A**, la cosa si spiega perché oltre alle lettere erano cifrate anche alcune parole, molte contenenti la **E**:
- *che, del, quel*

Crittografia e statistica: un esempio antico

- Lo studio delle frequenze era già praticato negli uffici cifra veneziani all'inizio del XVI secolo, come mostra questo registro con statistiche sulle frequenze di segni cifranti di qualche dispaccio intercettato.
- Ogni segno del messaggio viene riportato con un puntino nella colonna relativa.
- Alla fine viene segnato il totale per ogni segno.
- Capo dell'ufficio cifra veneziano era **Giovanni Soro**, che Kahn considera il padre della crittoanalisi occidentale.



Archivio di Stato di Venezia: Cifre, chiavi e scontri di cifra con studi successivi, sec. XVI – XVIII. 24. Liber secundus BAB.

Rimedio n.1: omofoni e nomenclatori

Rimedio n.1 alla crittoanalisi statistica?
Gli **omofoni** visti nella prima parte…
Le lettere più frequenti sono cifrate con diversi segni, e questo dovrebbe confondere le statistiche.
Però vanno usati correttamente … basta un addetto alla cifra pigro o frettoloso e la maggior sicurezza va persa.

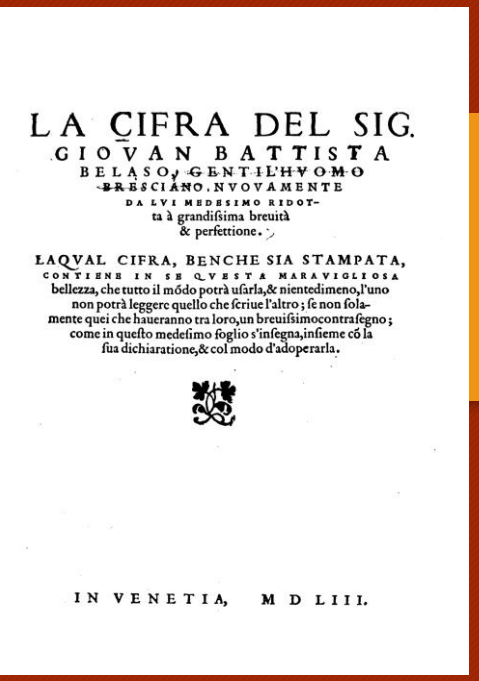
Ben più sicuri i **nomenclatori** visti nella prima parte, adottati a partire dal XV secolo.

Rimedio n.2 le cifre polialfabetiche

Rimedio n.2 alla crittoanalisi statistica?
La cifra **polialfabetica** …

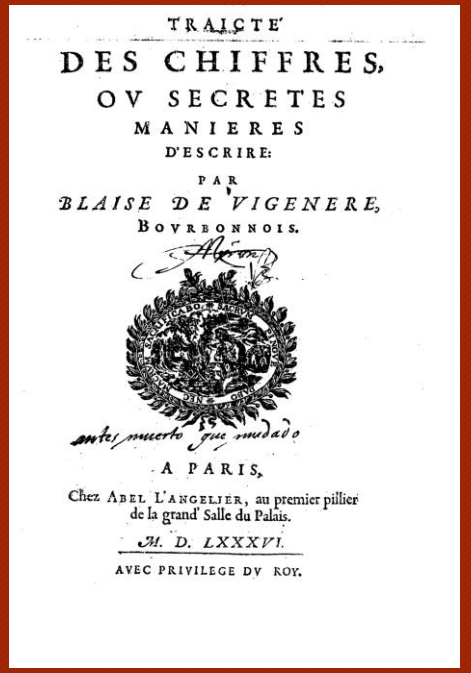
Prima il disco di **Leon Battista Alberti**,
rimasto segreto per un secolo.
Poi la tavola recta, 1507, dell'**abate Tritemio**.
Poi **la cifra di G.B. Bellaso**, Venezia 1553

In fine **il Traicté des chiffres** di Blaise de Vigenere, Parigi 1586, con la famosa tavola.

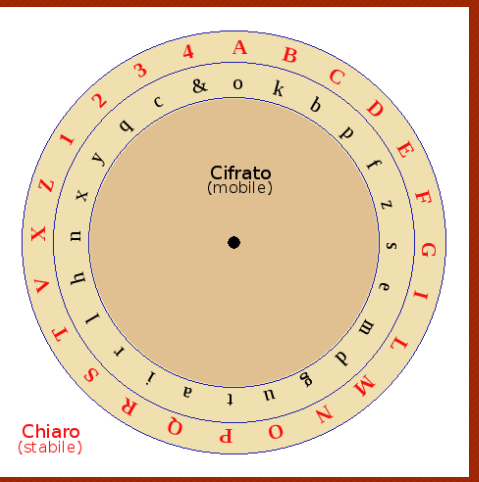

LA CIFRA DEL SIG.
GIOVAN BATTISTA
BELASO, GENTIL'HVOMO
BRESCIANO, NVOVAMENTE
DA LVI MEDESIMO RIDOT-
ta à grandissima breuità
& perfettione.

LAQVAL CIFRA, BENCHE SIA STAMPATA,
CONTIENE IN SE QVESTA MARAVIGLIOSA
bellezza, che tutto il módo potrà usarla, & nientedimeno, l'uno
non potrà leggere quello che scriue l'altro; se non sola-
mente quei che haueranno tra loro, un breuissimo contrasegno;
come in questo medesimo foglio s'insegna, insieme có la
sua dichiaratione, & col modo d'adoperarla.

IN VENETIA, M D LIII.


TRAICTE'
DES CHIFFRES,
OV SECRETES
MANIERES
D'ESCRIRE:
PAR
BLAISE DE VIGENERE,
BOVRBONNOIS.

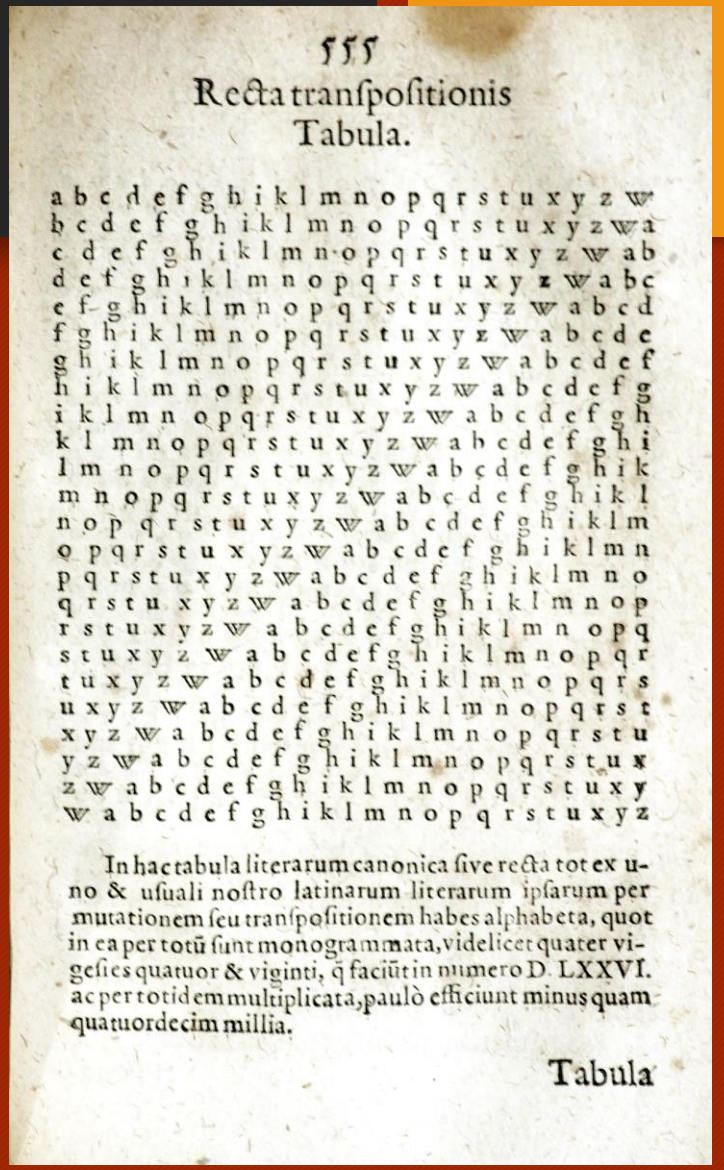
A PARIS,
Chez ABEL L'ANGELIER, au premier pillier de la grand' Salle du Palais.
M. D. LXXXVI.
AVEC PRIVILEGE DV ROY.



Disco di
L. B. Alberti

La tabula recta di Iohannes Tritemius

L'abate tedesco Iohannes Heidelberg meglio noto come Tritemius o (Trithemius) scrisse di stregoneria, arti magiche e di crittografia.
Alla fine del suo libro *Polygraphia* presenta una serie di alfabeti e tavole per uso crittografico e prima di tutto la *tabula recta* che precorre quella di Vigenére. Le istruzioni suggeriscono di usare ogni riga come alfabeto cifrante cambiandola ad ogni lettera. Non si parla di un verme o contrasegno come quelli di Vigenére e Bellaso.



fff

Recta tranſpoſitionis Tabula.

a b c d e f g h i k l m n o p q r s t u x y z w
b c d e f g h i k l m n o p q r s t u x y z w a
c d e f g h i k l m n o p q r s t u x y z w a b
d e f g h i k l m n o p q r s t u x y z w a b c
e f g h i k l m n o p q r s t u x y z w a b c d
f g h i k l m n o p q r s t u x y z w a b c d e
g h i k l m n o p q r s t u x y z w a b c d e f
h i k l m n o p q r s t u x y z w a b c d e f g
i k l m n o p q r s t u x y z w a b c d e f g h
k l m n o p q r s t u x y z w a b c d e f g h i
l m n o p q r s t u x y z w a b c d e f g h i k
m n o p q r s t u x y z w a b c d e f g h i k l
n o p q r s t u x y z w a b c d e f g h i k l m
o p q r s t u x y z w a b c d e f g h i k l m n
p q r s t u x y z w a b c d e f g h i k l m n o
q r s t u x y z w a b c d e f g h i k l m n o p
r s t u x y z w a b c d e f g h i k l m n o p q
s t u x y z w a b c d e f g h i k l m n o p q r
t u x y z w a b c d e f g h i k l m n o p q r s
u x y z w a b c d e f g h i k l m n o p q r s t
x y z w a b c d e f g h i k l m n o p q r s t u
y z w a b c d e f g h i k l m n o p q r s t u x
z w a b c d e f g h i k l m n o p q r s t u x y
w a b c d e f g h i k l m n o p q r s t u x y z

In hac tabula literarum canonica ſive recta tot ex uno & uſuali noſtro latinarum literarum ipſarum permutationem ſeu tranſpoſitionem habes alphabeta, quot in ea per totũ ſunt monogrammata, videlicet quater vigeſies quatuor & viginti, q̃ faciũt in numero D. LXXVI. ac per totidem multiplicata, paulò efficiunt minus quam quatuordecim millia.

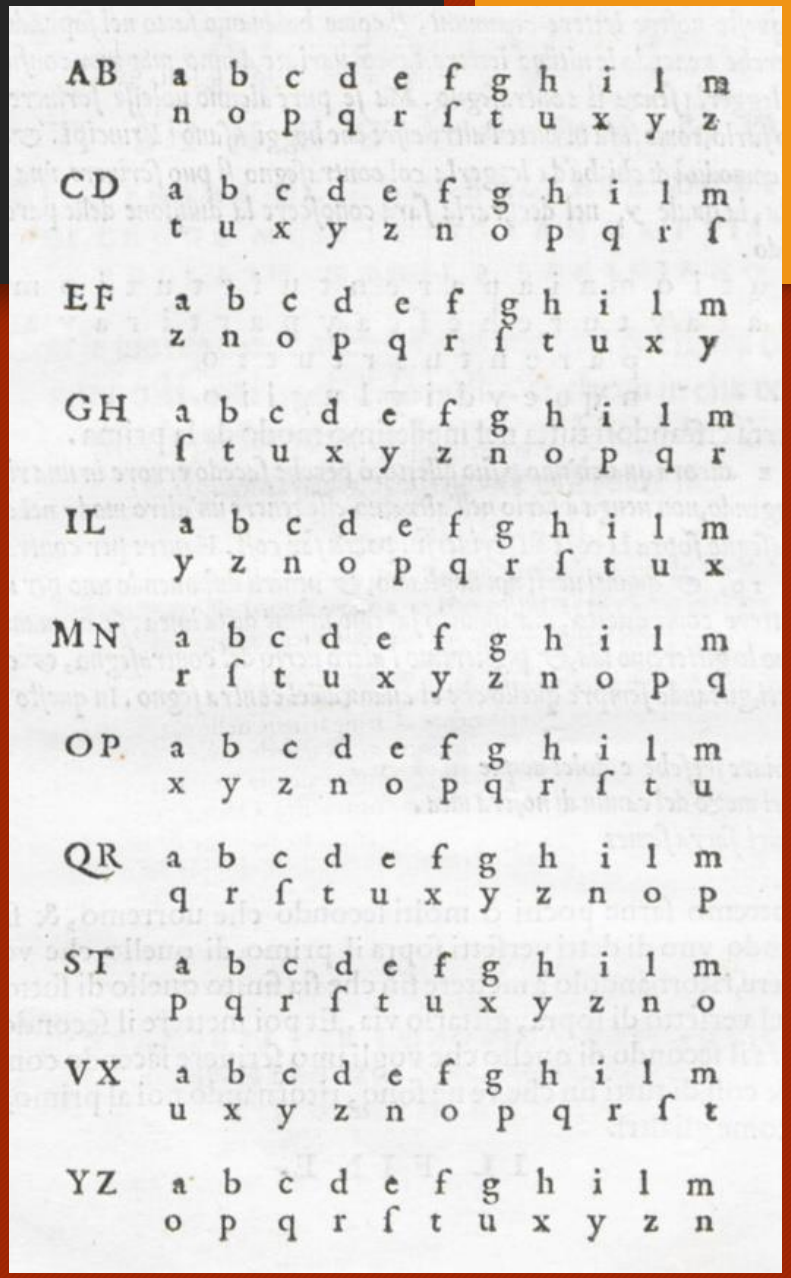
Tabula

Le cifre di G.B. Bellaso

Il bresciano G.B. Bellaso nel 1553 pubblica a Venezia una cifra polialfabetica basata su liste involutorie alternate in base alla lettera di un *contrassegno* (la moderna *password*)

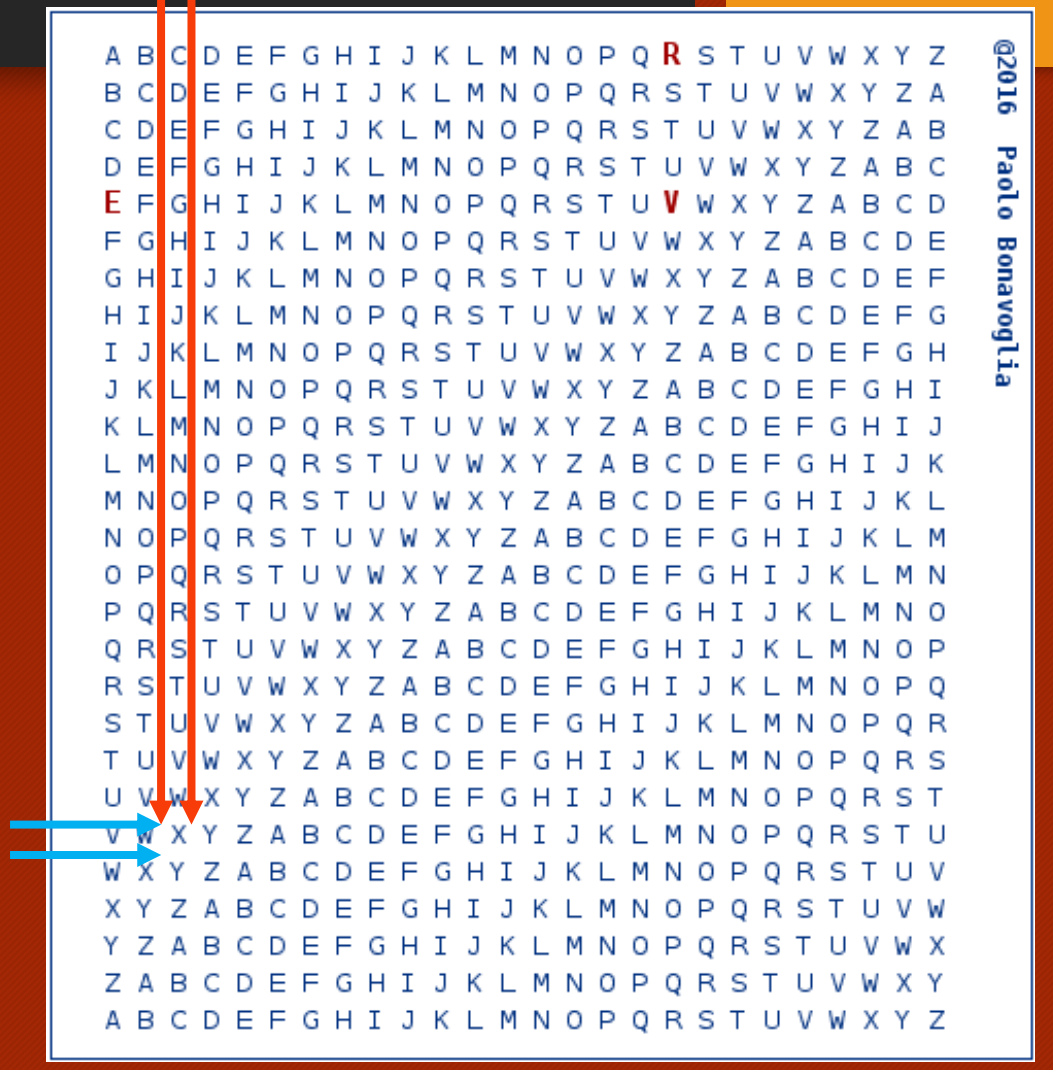
C.segno SEGNOSEGNOSEGN
Chiaro CORDIALISALVTI
Cifrato RCMVSPXPBXNIBO

La **I** viene cifrata come **S**, come **P** come **O**.
La crittoanalisi statistica è sconfitta?



La tavola di Vigenére

Chiaro C +
Verme V =
Cifra X



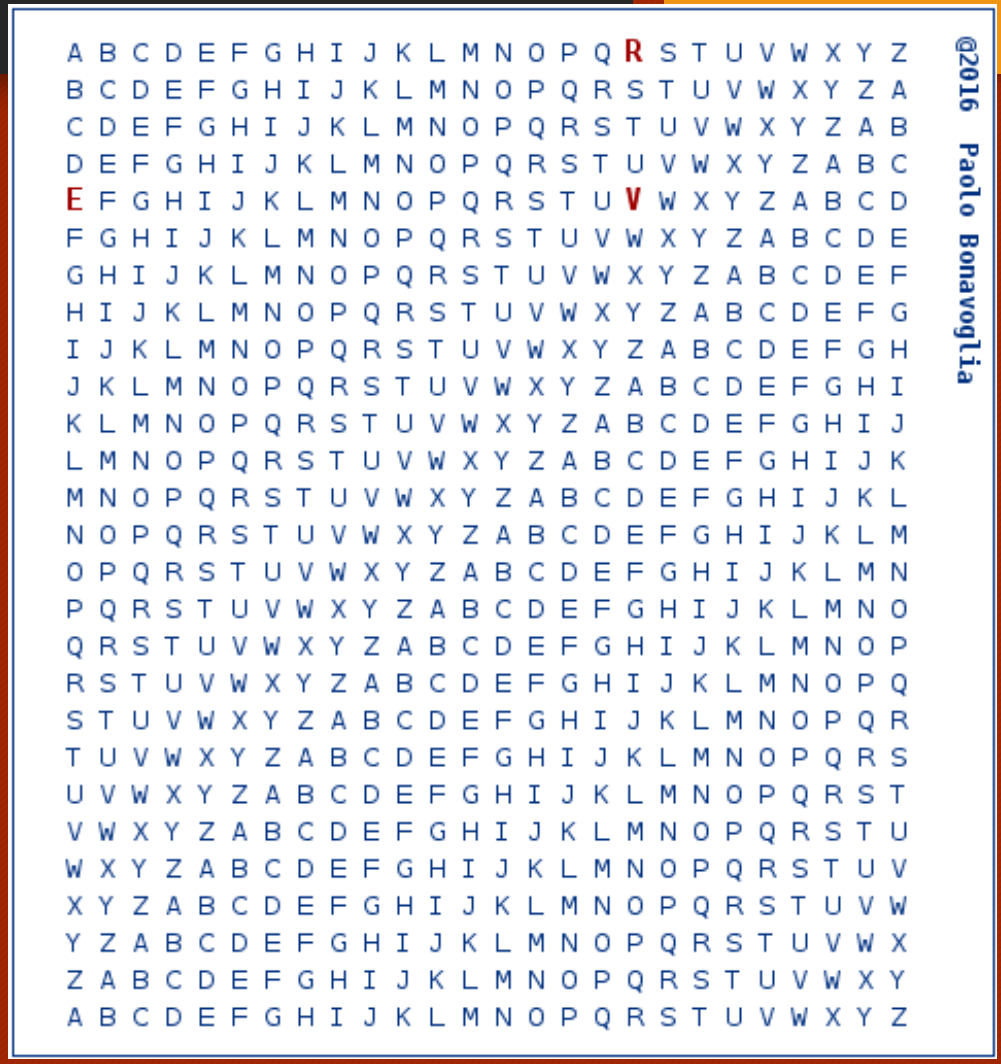
Il francese Blaise de Vigenére pubblica nel 1586 una cifra polialfabetica ancora più semplice.

Chiaro	CORDIALISALVTI
Verme	VERMEVERMEVERM
Cifrato	XSIPNVOZDEFYLT

La A è cifrata prima da V poi da E a seconda del verme.

La tavola di Vigenére è un’addizione modulo 26

Chiaro	CORDIALISALUTI
	02141703080010081800102019 08
Verme	VERMEVERMEVERM
	21041711042104171104210417 11
Cifrato	XSIPNVOZDEFYLT
	23180814122114250304052410 19



L’aritmetica modulo 26, esempio di aritmetica finita (o modulare)

Lo strano mondo dell’aritmetica finita. Qui esiste un numero limite, oltre il quale si ricomincia da zero.
Esempio ben noto: l’aritmetica dell’orologio; le ore vanno da 0 a 23; arrivati a 24 si ricomincia da 0; insomma in questa aritmetica 24 = 0! Questa è **un’aritmetica modulo 24.**
Simile l’aritmetica dell’alfabeto a 26 lettere; ponendo A =0; B = 1 … arrivati a 26 si ricomincia da 0 ! Questa è **un’aritmetica modulo 26.**

Esempi di aritmetica modulo 26:

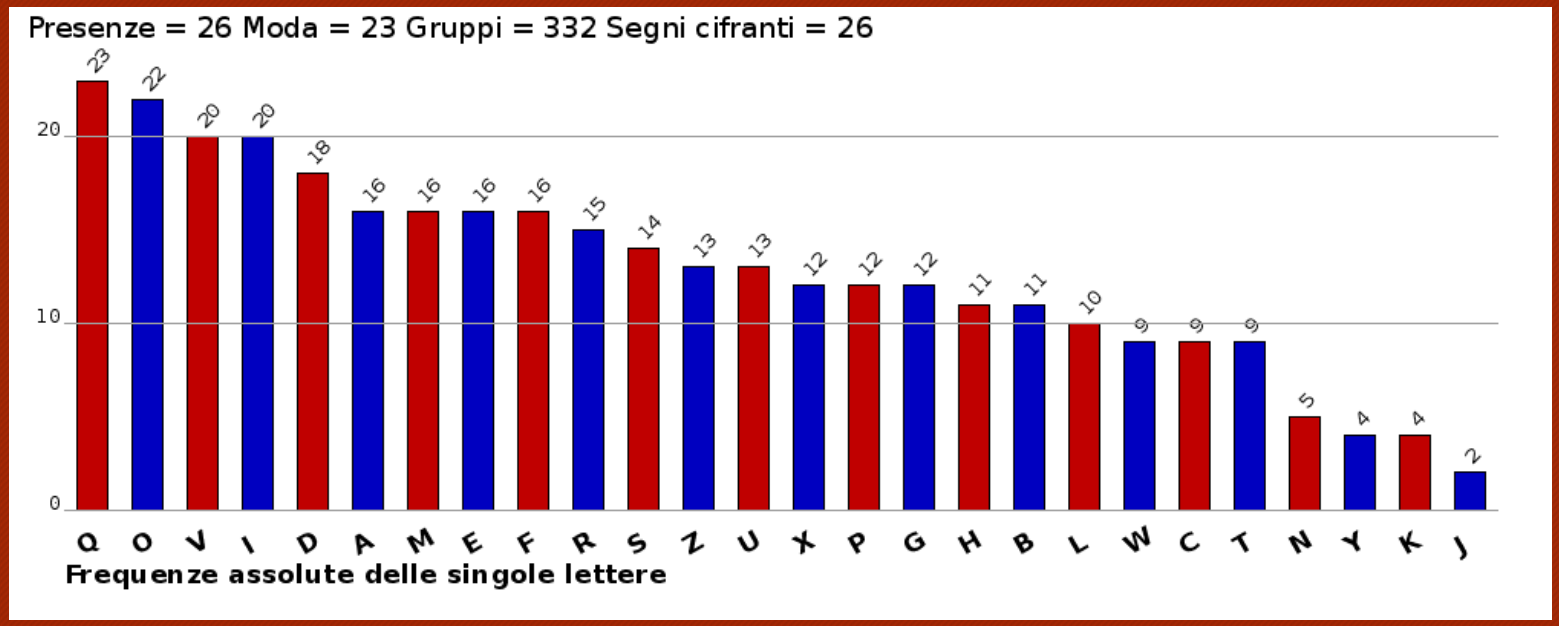
$13 + 22 = 9$ $13 - 22 = 17$ *Per fortuna nel Vigenere bastano queste due operazioni…*

$13 \times 2 = 0$ *cade la legge di annullamento del prodotto. Come evitarlo?*

$2^5 = 6$ $\log_2 6 = 5$ $3^3 = 1$ $\log_3 1 = 3$ $\sqrt[3]{1} = 3$

La statistica di un cifrato con Vigenére

PSXYICHOFSXOEPUIPRUZSVBRCJUFEPQRKHDAZDQPGFGZEVMLXOAEGXZAEVQXEGQRKHFMZ
LIETOEYEUZIVOQCYDVTQOPUUXILGFMQGRAAFIDMIVBAUSXHEVMLXOSSMDMAUDDMIIWRVS
OTIQMLRSZEMHZRKBZAZDTAROGDEWINVCQMQDZAEVQBSFWERWGYSUBEOOBQVSIRNODQHHT
BGBOTMRDIVFAHELLITCPQPOILVFQOSVMCJWAHLRACQFFQMRVOPGANIQZIFWDOSPQOXSZF
VDQTCBFQVDXIGBPUWRVNQOCGIOXUPHAOLHTAFWDUXWIVKOMNFDVDQBMU



La statistica appare più piatta di quella di un monoalfabetico e non si può dire nulla sulle più frequenti.
Dunque nulla da fare?
Sembra proprio di sì, e per secoli il Vigenére fu considerato inattaccabile e sicurissimo.

1863 : il colonnello prussiano Friedrich Kasiski scopre che in un Vigenére …

PSXYICHOFSXOEPUIPRUZSVBRCJUFEPQRKHDAZDQPGFGZEVMLXOAEGXZAEVQXEGQRKHFMZ
LIETOEYEUZIVOQCYDVTQOPUUXILGFMQGRAAFIDMIVBAUSXHEVMLXOSSMDMAUDDMIIWRVS
OTIQMLRSZEMHZRKBZAZDTAROGDEWINVCQMQDZAEVQBSFWERWGYSUBEOOBQVSIRNODQHHT
BGBOTMRDIVFAHELLITCPQPOILVFQOSVMCJWAHLRACQFFQMRVOPGANIQZIFWDOSPQOXSZF
VDQTCBFQVDXIGBPUWRVNQOCGIOXUPHAOLHTAFWDUXWIVKOMNFDVDQBMU

Il gruppo SX si ripete 8 posti avanti;
Il gruppo ML si ripete 24 posti avanti;
Più strano ancora:
QRKH si ripete tale e quale 32 posti avanti.

Potrebbe voler dire qualcosa?

Potrebbe essere che il verme …

PSXYICHOFSXOEPUIPRUZSVBRCJUFEPQRKHDAZDQPGFGZEVMLXOAEGXZAEVQXEGQRKHFMZ
LIETOEYEUZIVOQCYDVTQOPUUXILGFMQGRAAFIDMIVBAUSXHEVMLXOSSMDMAUDDMIIWRVS
OTIQMLRSZEMHZRKBZAZDTAROGDEWINVCQMQDZAEVQBSFWERWGYSUBEOOBQVSIRNODQHHT
BGBOTMRDIVFAHELLITCPQPOILVFQOSVMCJWAHLRACQFFQMRVOPGANIQZIFWDOSPQOXSZF
VDQTCBFQVDXIGBPUWRVNQOCGIOXUPHAOLHTAFWDUXWIVKOMNFDVDQBMU

Il gruppo SX si ripete 8 posti avanti;
Il gruppo ML si ripete 24 posti avanti;
Più strano ancora:
QRKH si ripete tale e quale 32 posti avanti.

Potrebbe voler dire qualcosa?

Potrebbe essere che il verme sia lungo 8 caratteri!!

Ma è importante la lunghezza del verme?

E’ importante la lunghezza del verme?

Importantissima!
Se la lunghezza è 8,
Il cifrato si riduce a 8 cifrari di Cesare, ben visibili se incolonniamo il testo per 8.

E per decrittare la cifra di Cesare bastano pochi tentativi.

Ci sono poi altri metodi più efficienti per trovare la lunghezza del verme.

Crittoanalisi automatica

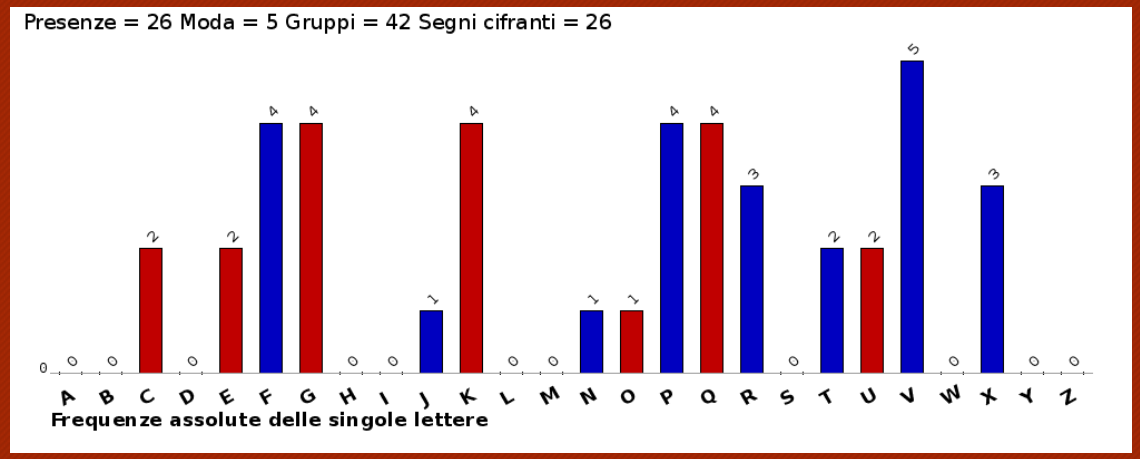
PSXYICHO VCQMQDZA
FSXOEPUI EVQBSFWE
PRUZSVBR RWGYSUBE
CJUFEPQR OOBQVSIR
KHDAZDQP NODQHHTB
GFGZEVML GBOTMRDI
XOAEGXZA VFAHELLI
EVQXEGQR TCPQPOIL
KHFMZLIE VFQOSVMC
TOEYEUZI JWAHLRAC
VOQCYDVT QFFQMRVO
QOPUUXIL PGANIQZI
GFMQGRAA FWDOSPQO
FIDMIVBA XSZFVDQT
USXHEVML CBFQVDXI
XOSSMDMA GBPUWRVN
UDDMIIWR QOCGIOXU
VSOTIQML PHAOLHTA
RSZEMHZR FWDUXWIV
KBZAZDTA KOMNFDVD
ROGDEWIN QBMU

Come risolvere Cesare a mano?

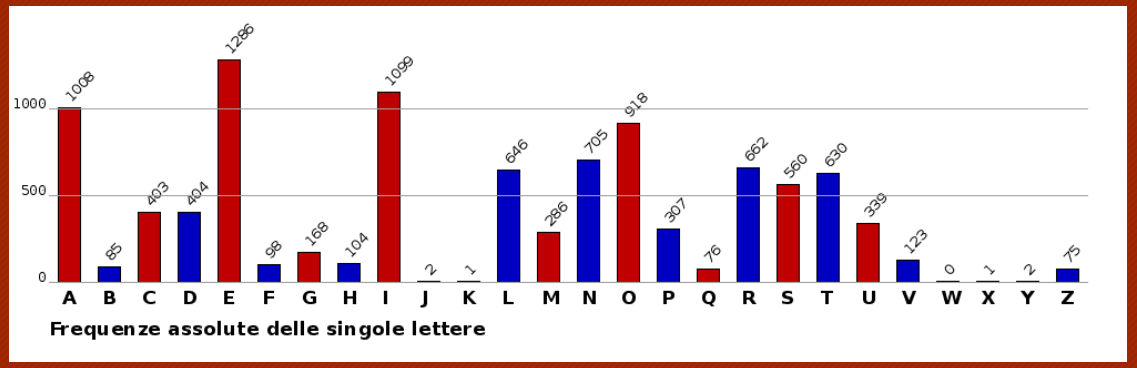
- Una caratteristica di un cifrario di Cesare è che le lettere più rare (in italiano JK WXY) saranno in una posizione riconoscibile.
- Anche le lettere più frequenti A E I O occupano una posizione riconoscibile
- Se invece la colonna è casuale, le frequenze saranno più appiattite, ci saranno meno differenze.

Crittoanalisi del Vigenere (o di Cesare?)

PFPCKGXEKTVQGFUXUVRKRVERONGVTVJQPFXCGQPFKQ



Prima colonna



Frequenze Lingua italiana

PSXYICHO VCQMQDZA
FSXOEPUI EVQBSFWE
PRUZSVBR RWGYSUBE
CJUFEPQR OOBQVSIR
KHDAZDQP NODQHHTB
GFGZEVML GBOTMRDI
XOAEGXZA VFAHELLI
EVQXEGQR TCPQPOIL
KHFMZLIE VFQOSVMC
TOEYEUZI JWAHLRAC
VOQCYDVT QFFQMRVO
QOPUUXIL PGANIQZI
GFMQGRAA FWDOSPQO
FIDMIVBA XSZFVDQT
USXHEVML CBFQVDXI
XOSSMDMA GBPUWRVN
UDDMIIWR QOCGIOXU
VSOTIQML PHAOLHTA
RSZEMHZR FWDUXWIV
KBZAZDTA KOMNFDVD
ROGDEWIN QBMU

E dell'ultima colonna, che dire?

Come risolvere Cesare auto-matematicamente?

- Come confrontare le frequenze osservate con quelle attese?
- Occorre un metodo per misurare quanto sono diverse, distanti due distribuzioni di frequenza.
- E’ un po’ come calcolare la distanza tra due punti.
- Che si fa usando un ben noto teorema …

Distanza geometrica e non solo …

- Distanza d tra due punti A, B nel piano? Nello spazio n dimensioni
- $d^2 = \Delta x^2 + \Delta y^2 + \ldots = (x_A - x_B)^2 + (y_A - x_B)^2 + (z_A - z_B)^2 + \cdots$
- Distanza d tra dati osservati $\boldsymbol{o}$ e dati attesi $\boldsymbol{e}$ in base a una data ipotesi
- $d^2 = (o_1 - e_1)^2 + (o_2 - e_2)^2 + (o_3 - e_3)^2 + \ldots$
- Chi quadrato tra dati osservati $\boldsymbol{o}$ e dati attesi $\boldsymbol{e}$ in base a una data ipotesi
- $\chi^2 = \frac{(o_1 - e_1)^2}{e_1} + \frac{(o_2 - e_2)^2}{e_2} + \frac{(o_3 - e_3)^2}{e_3} + \cdots$

Il test del chi quadrato χ^2 in questo caso

- $\chi^2 = \frac{(o_1 - e_1)^2}{e_1} + \frac{(o_2 - e_2)^2}{e_2} + \frac{(o_3 - e_3)^2}{e_3} + \cdots$

- Dove
- o_1= frequenza osservata della prima lettera e_1= frequenza attesa di A
- o_2= frequenza osservata della seconda lettera e_2= frequenza attesa di B
- ….
- Si calcola il χ^2 per 26 volte, spostando ogni volta le lettere a rotazione
- Ipotesi migliore quella con il χ^2 minore

Come trovare la lunghezza del verme?

- Come trovare la lunghezza del verme?
- Come trovare l’ipotesi migliore?
- Si possono provare tutte una per una da 1 a n e vedere ogni volta se le n colonne hanno le caratteristiche di un cifrario di Cesare.
- Ci serve un metodo per misurare quanto i dati osservati siano lontani da quelli attesi in base all’ipotesi.

Crittoanalisi automatica

Crittoanalisi automatica

Quindi Vigenére è molto debole.

Funziona solo se il testo è 10-20 volte più lungo del verme.
Più lungo il verme più difficile decrittare

Meglio un verme breve …
… o un verme lungo?

Un verme breve … si ricorda facilmente … ma è meno sicuro

Un verme lungo … è difficile da ricordare … ma è più sicuro

E se il verme avesse lunghezza infinita?

Il cifrario di Vernam

È questa l'idea proposta da Gilbert S. Vernam nel 1917 e brevettata nel 1919.
L’anno prossimo compie 100 anni!
Viene generata una chiave del tutto casuale, e dunque imprevedibile, lunga come il testo; a questo punto il chiaro e la chiave vengono "sommati" proprio come nel cifrario di Vigenere.
Ma come generare e scambiarsi una chiave infinita?
Ovviamente ci si deve limitare a una chiave molto lunga memorizzata su un nastro o simile. Un nastro *usa e butta*. Quando finisce occorre generarne uno nuovo e scambiarselo di nuovo.
In inglese ha anche il nome di ***One time pad.***
http://www.crittologia.eu/critto/vernam.html

Macchine [pseudo]Vernam

- L’idea di Vernam suggerì quella di costruire macchine in grado di generare sequenze casuali, in verità quasi sempre pseudo-casuali, avendo un periodo.
- La più famosa fu la macchina Lorenz usata dagli alti omandi tedeschi durante la II Guerra mondiale: una serie di rotori simulava un verme pseudo-casuale; gli inglesi riuscirono a decrittarla ma dovettero costruire il primo computer il Colossus per riuscirci in tempi brevi.
- Veramente casuale la macchina Hagelin RT basata su un nastro perforato (5 fori) con procedimenti chimici che dovrebbero essere *imprevedibili*. I nastri vanno rinnovati periodicamente.

La fine

Grazie per l’attenzione