La tavola di Vigenère

Un modo per rendere la sostituzione immune dall'analisi delle frequenze diverso da quelli visti finora fu introdotto nel Rinascimento da molti diversi crittografi, tra i quali Alberti, Bellaso, Della Porta e Vigenère. L'idea di base era di rendere il passaggio da un alfabeto cifrante all'altro continuo e sistematico, slegato da istruzioni e metasimboli presenti nel messaggio stesso. La chiave, considerata una lettera per volta, avrebbe indicato quale alfabeto cifrante usare e avrebbe al contempo determinato un continuo slittamento dello stesso.

Vediamo un esempio e supponiamo di disporre di 26 alfabeti cifranti diversi, ciascuno identificato da una lettera dell'alfabeto. Immaginando poi di utilizzare la chiave `CIAO`, possiamo ridurci a considerare 4 alfabeti cifranti $\boxed{A}$, $\boxed{C}$, $\boxed{I}$, $\boxed{O}$:

TABELLA DEL CIFRATORE (o *TABELLA DI CIFRATURA*)

Alfabeto CHIARO	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
Alfabeto CIFRANTE $\boxed{A}$	**X**	**A**	**Q**	**Y**	**P**	**B**	**M**	**C**	**L**	**D**	**W**	**Z**	**N**	**O**	**E**	**V**	**K**	**F**	**G**	**U**	**R**	**J**	**S**	**H**	**T**	**I**
Alfabeto CIFRANTE $\boxed{C}$	**Z**	**B**	**S**	**A**	**K**	**W**	**T**	**D**	**L**	**J**	**C**	**X**	**M**	**V**	**F**	**N**	**Y**	**E**	**O**	**I**	**G**	**H**	**R**	**Q**	**P**	**U**
Alfabeto CIFRANTE $\boxed{I}$	**Q**	**J**	**X**	**B**	**Y**	**F**	**N**	**P**	**D**	**H**	**S**	**L**	**V**	**Z**	**U**	**T**	**A**	**O**	**K**	**E**	**G**	**W**	**R**	**C**	**I**	**M**
Alfabeto CIFRANTE $\boxed{O}$	**F**	**W**	**I**	**L**	**E**	**U**	**K**	**A**	**S**	**X**	**R**	**G**	**B**	**O**	**T**	**M**	**Z**	**Y**	**N**	**J**	**V**	**Q**	**P**	**C**	**H**	**D**

Dobbiamo ora cifrare il messaggio "Nessun movimento a Nord" cioè "`NESSUNMOVIMENTOANORD`". Per questioni pratiche scriviamo la nostra chiave sopra il messaggio da crittare, ripetendola il numero di volte necessario ad eguagliare la lunghezza del messaggio:

CHIAVE	C	I	A	O	C	I	A	O	C	I	A	O	C	I	A	O	C	I	A	O
MESSAGGIO	N	E	S	S	U	N	M	O	V	I	M	E	N	T	O	A	N	O	R	D

A questo punto il gioco è fatto: per cifrare la `N` useremo l'alfabeto cifrante $\boxed{C}$, per cifrare la `E` l'alfabeto cifrante $\boxed{C}$ e così via. Si tratta di un lavoro durante il quale è facile sbagliare qualche assegnazione, conviene quindi ragionare nel seguente modo: mettiamo in evidenza l'alfabeto cifrante che ci interessa …

TABELLA DEL CIFRATORE (o *TABELLA DI CIFRATURA*)

Alfabeto CHIARO	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
Alfabeto CIFRANTE $\boxed{A}$	X	A	Q	Y	P	B	M	C	L	D	W	Z	N	O	E	V	K	F	G	U	R	J	S	H	T	I
Alfabeto CIFRANTE $\boxed{C}$	**Z**	**B**	**S**	**A**	**K**	**W**	**T**	**D**	**L**	**J**	**C**	**X**	**M**	**V**	**F**	**N**	**Y**	**E**	**O**	**I**	**G**	**H**	**R**	**Q**	**P**	**U**
Alfabeto CIFRANTE $\boxed{I}$	Q	J	X	B	Y	F	N	P	D	H	S	L	V	Z	U	T	A	O	K	E	G	W	R	C	I	M
Alfabeto CIFRANTE $\boxed{O}$	F	W	I	L	E	U	K	A	S	X	R	G	B	O	T	M	Z	Y	N	J	V	Q	P	C	H	D

… e operiamo tutte le sostituzioni che lo riguardano.

CHIAVE	C	I	A	O	C	I	A	O	C	I	A	O	C	I	A	O	C	I	A	O
MESSAGGIO	N	E	S	S	U	N	M	O	V	I	M	E	N	T	O	A	N	O	R	D
CIFRA	**V**				**G**				**H**				**S**				**V**			

Passiamo poi all'alfabeto cifrante successivo…

TABELLA DEL CIFRATORE (o *TABELLA DI CIFRATURA*)

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

…e continuiamo la sostituzione.

CHIAVE	C	I	A	O	C	I	A	O	C	I	A	O	C	I	A	O	C	I	A	O
MESSAGGIO	N	E	S	S	U	N	M	O	V	I	M	E	N	T	O	A	N	O	R	D
CIFRA	**V**	**Y**			**G**	**Z**			**H**	**D**			**S**	**E**			**V**	**U**		

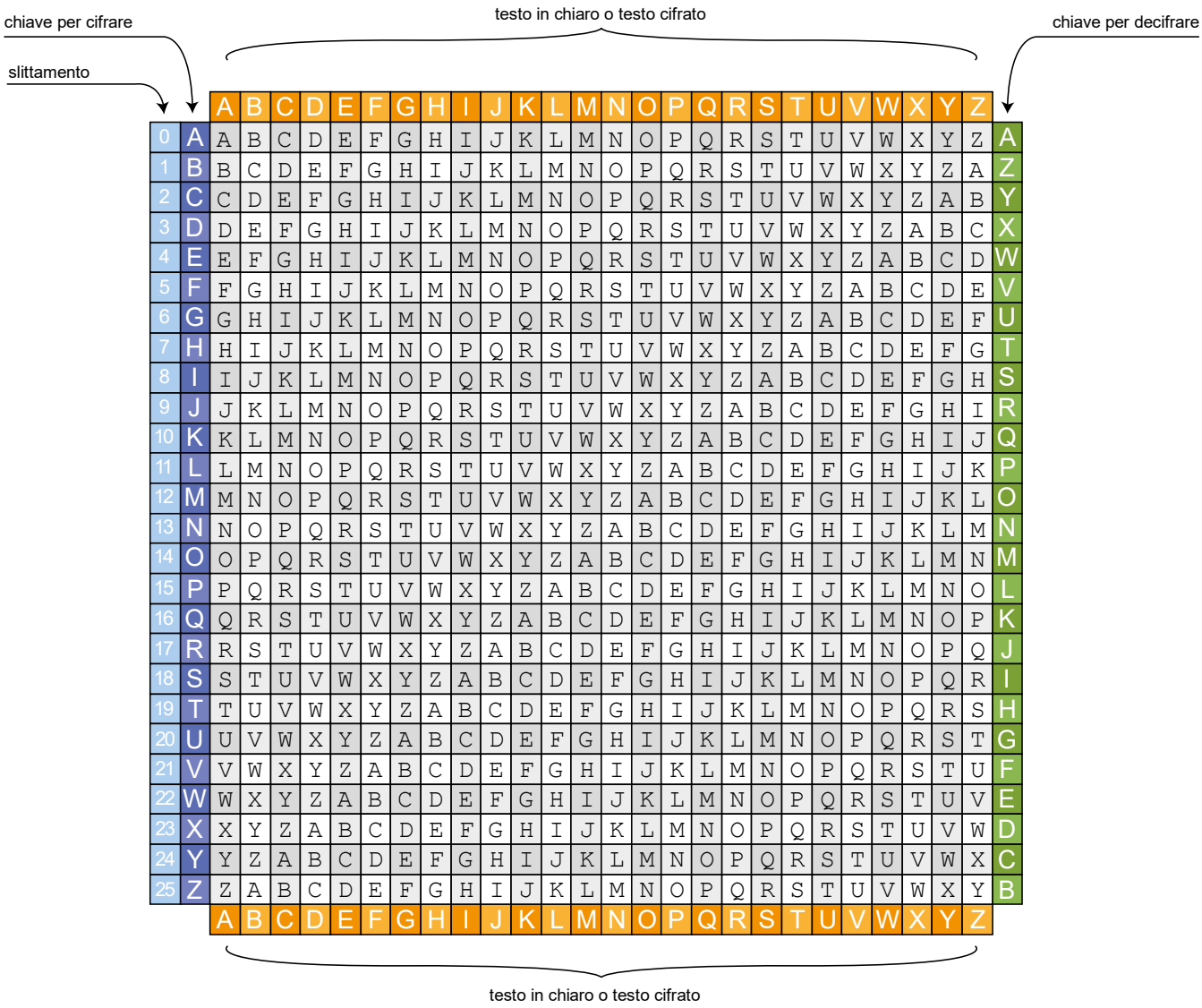
Continuando in questo modo si arriva presto a….

CIFRA	**V**	**Y**	**G**	**N**	**G**	**Z**	**N**	**T**	**H**	**D**	**N**	**E**	**S**	**E**	**E**	**F**	**V**	**U**	**F**	**L**

Per rendersi conto dell'efficacia del metodo notiamo per esempio che la doppia SS iniziale è stata tradotta in GN, mentre nel messaggio cifrato è apparsa la doppia EE in un punto nel quale il testo non ne preveda.

Un metodo del genere si chiama **sostituzione polialfabetica** (perché usa più alfabeti) e, in questo contesto, la chiave prende il nome di **verme**.

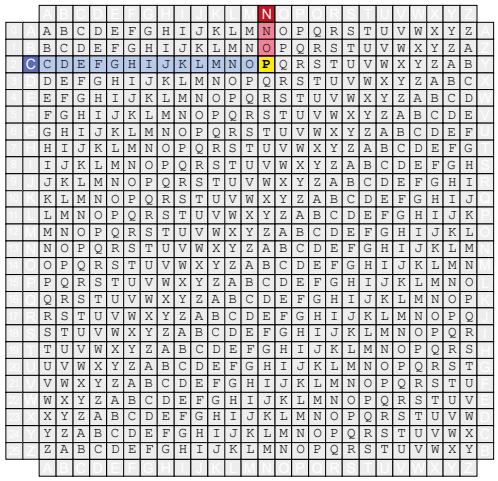
Il punto debole del metodo è il solito: tenere a mente 26 alfabeti cifranti diversi è un compito improbo! Furono proposte varie soluzioni a questo problema e una di esse soppiantò tutte le altre in virtù della sua maggiore semplicità (a scapito della segretezza, a dire il vero): si tratta della cosiddetta **tavola di Vigenère**. Il francese Vigenère riteneva che la robustezza del metodo potesse resistere ad una semplificazione degli alfabeti cifranti ed adottò per ogni lettera dell'alfabeto il cifrario di Cesare ad essa associato (l'associazione risulterà chiara osservando la tavola in basso).



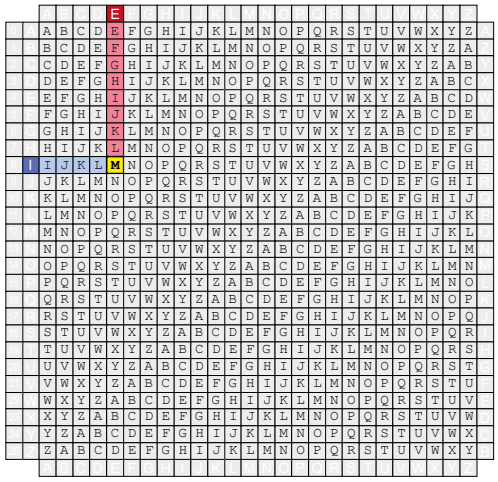
Grazie alla tavola di Vigenere, le codifiche possono essere svolte in modo abbastanza rapido, come mostra il solito esempio:

CHIAVE	C	I	A	O	C	I	A	O	C	I	A	O	C	I	A	O	C	I	A	O
MESSAGGIO	N	E	S	S	U	N	M	O	V	I	M	E	N	T	O	A	N	O	R	D

Iniziamo con la codifica della N attraverso la chiave $\boxed{C}$. Basterà cercare sulla tavola l'incrocio fra la colonna N e la riga C: si tratta della lettera **P** (da notare che si sarebbe trovata la stessa lettera anche invertendo colonna e riga).



La seconda lettera utilizza la tavola I per cifrare la lettera E. La lettera risultante è la **M**.



Nel caso in cui la riga individuata sia nella parte inferiore della tavola, si potrà usare l'ultima riga al posto della prima (si tratta di due copie). La prima e l'ultima colonna sono invece molto diverse fra loro e non possono assolutamente essere usate in questo modo.

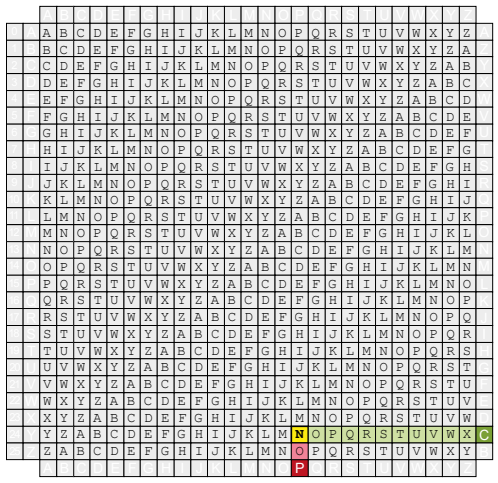
Proseguendo sempre in questo modo si arriva al seguente risultato:

CHIAVE	C	I	A	O	C	I	A	O	C	I	A	O	C	I	A	O	C	I	A	O
MESSAGGIO	N	E	S	S	U	N	M	O	V	I	M	E	N	T	O	A	N	O	R	D
CIFRA	**P**	**M**	**S**	**G**	**W**	**V**	**M**	**C**	**X**	**Q**	**M**	**S**	**P**	**B**	**O**	**O**	**P**	**W**	**R**	**R**

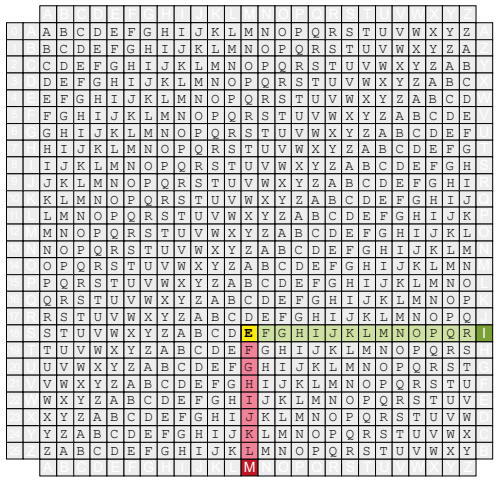
Per decifrare un messaggio crittato con la tavola di Vigenère si procede in modo quasi identico: stavolta però il "nome della riga" si trova nella colonna più a destra. Un'altra differenza è che stavolta righe e colonne non sono interscambiabili.

Nuovamente si tratta di vedere il "metodo all'opera":

Iniziamo con la decodifica della P attraverso la chiave C. Bisognerà ora individuare la riga corretta utilizzando le lettere della colonna di decodifica (si tratta di una delle ultime righe). Per la scelta della colonna si procederà invece facendo riferimento al "bordo" più vicino. Otteniamo così la **N**.



Procedendo allo stesso modo si ottiene velocemente la **E**.

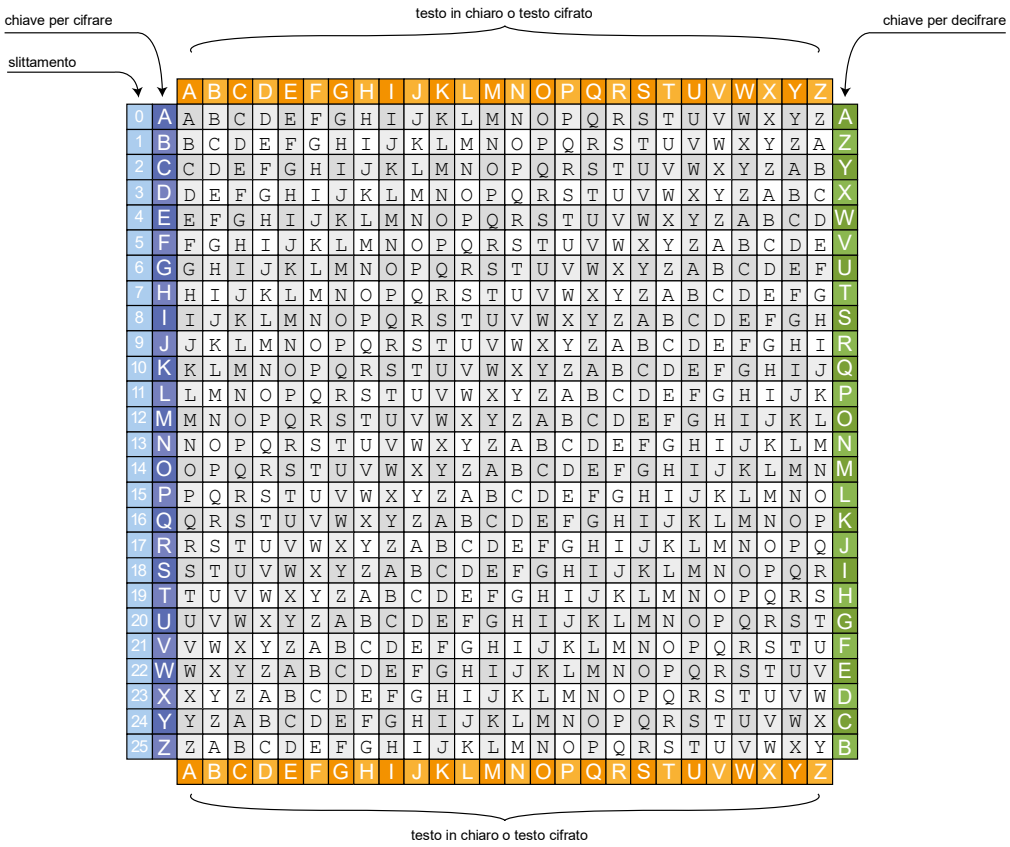


Si tratta in effetti delle prime due lettere del messaggio in chiaro NESSUNMOVIMENTOANORD.

Il modo migliorare per capire la tavola è provare ad usarla:

9.1) Utilizzando la tavola di Vigenère, codifica i seguenti messaggi con i vermi indicati.

	Messaggio	Verme
a)	Attacco	Verme
b)	Difendete la posizione	Vittorio Veneto
c)	Il mattino ha l'oro in bocca	Saggezza popolare
d)	California	Alabama



a)

CHIAVE	V	E	R	M	E		
MESSAGGIO	A	T	T	A	C	C	O
CIFRA							

b)

CHIAVE	V	I	T	T	O	R	I	O	V	E	N	E	T	O						
MESSAGGIO	D	I	F	E	N	D	E	T	E	L	A	P	O	S	I	Z	I	O	N	E
CIFRA																				

c)

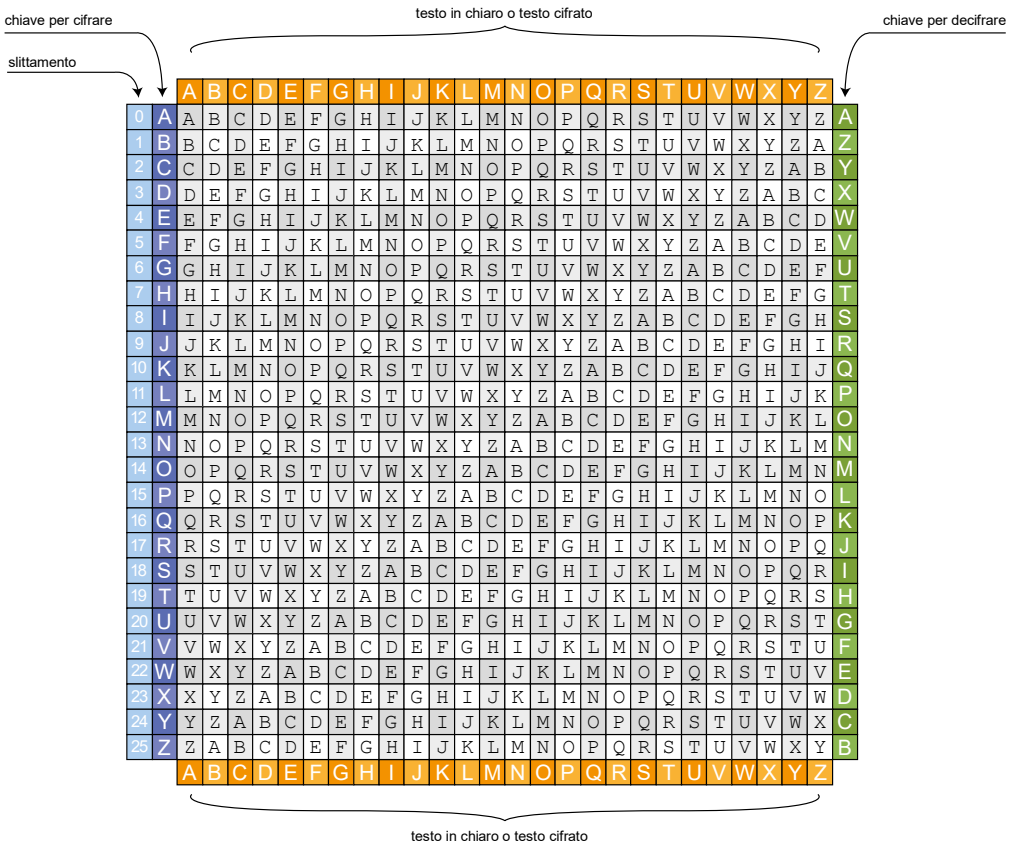
CHIAVE	S	A	G	G	E	Z	Z	A	P	O	P	O	L	A	R	E						
MESSAGGIO	I	L	M	A	T	T	I	N	O	H	A	L	O	R	O	I	N	B	O	C	C	A
CIFRA																						

d)

CHIAVE	A	L	A	B	A	M	A			
MESSAGGIO	C	A	L	I	F	O	R	N	I	A
CIFRA										

9.2) Utilizzando la tavola di Vigenère, decodifica i seguenti messaggi con i vermi indicati.

	Testo cifrato	Verme
a)	AADTZMSVILREU	PALERMO
b)	POZTBDNQVVVO	MANTOVA
c)	NRGIKWFHUFKXZC	MAGGIORE
d)	KBEFAGZOVCTWMWLR	COCOMERO



a)

CHIAVE	P	A	L	E	R	M	O						
Testo cifrato	A	A	D	T	Z	M	S	V	I	L	R	E	U
Testo in chiaro													

b)

CHIAVE	M	A	N	T	O	V	A					
Testo cifrato	P	O	Z	T	B	D	N	Q	V	V	V	O
Testo in chiaro												

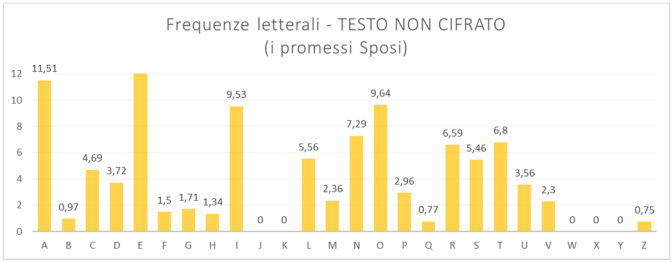
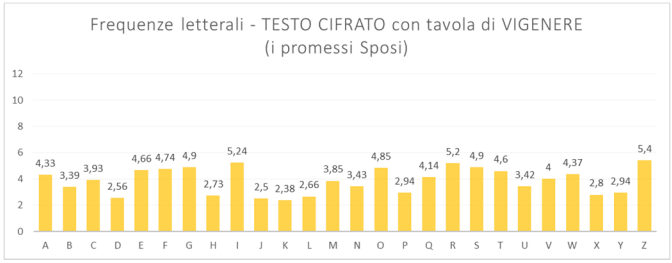
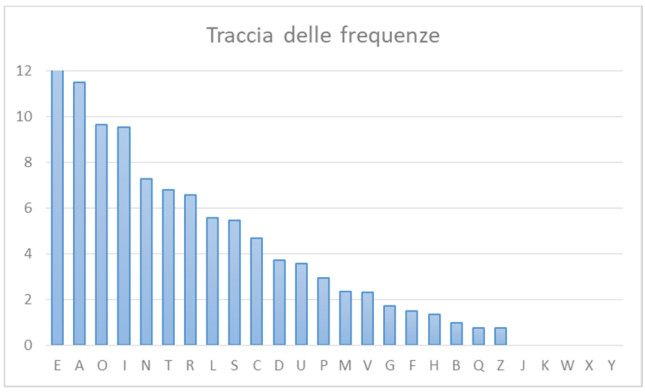
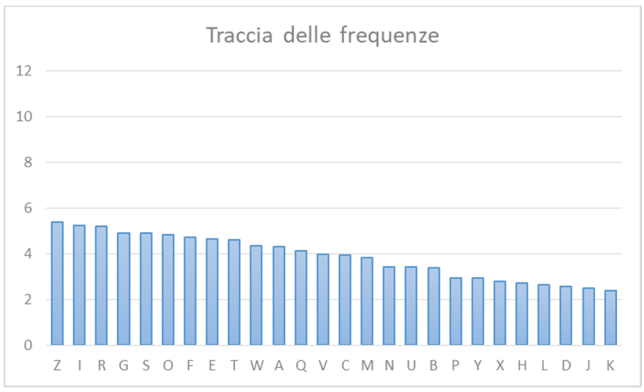
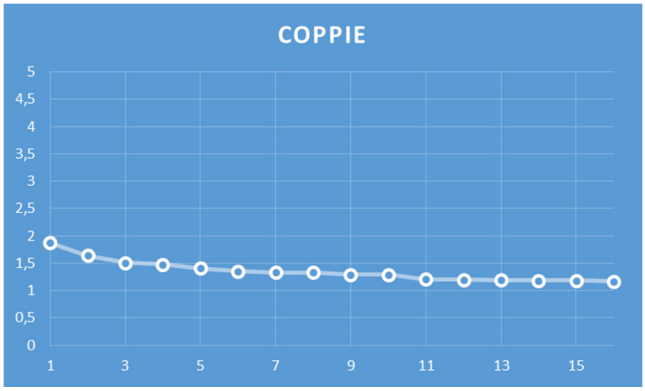
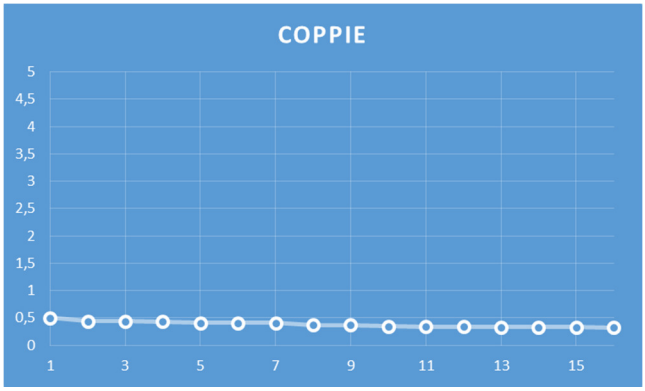
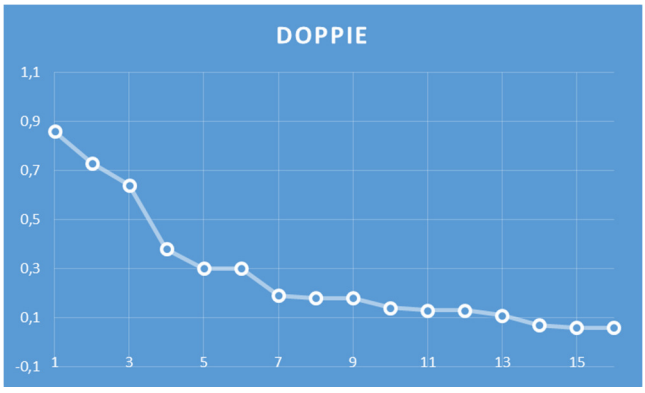
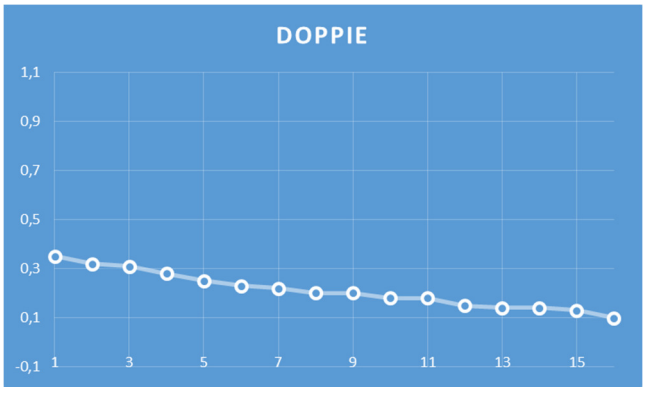
c)

CHIAVE	M	A	G	G	I	O	R	E						
Testo cifrato	N	R	G	I	K	W	F	H	U	F	K	X	Z	C
Testo in chiaro														

d)

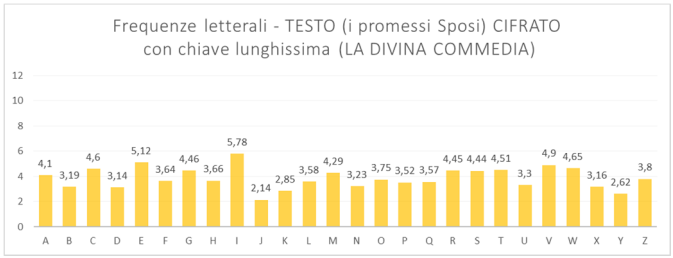
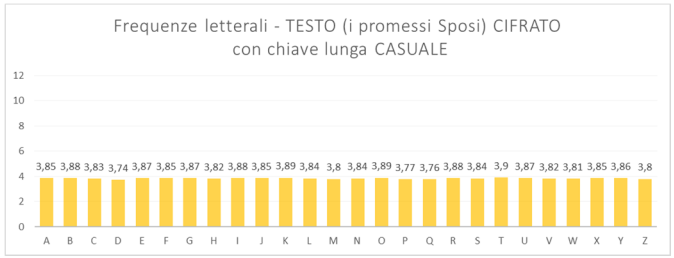
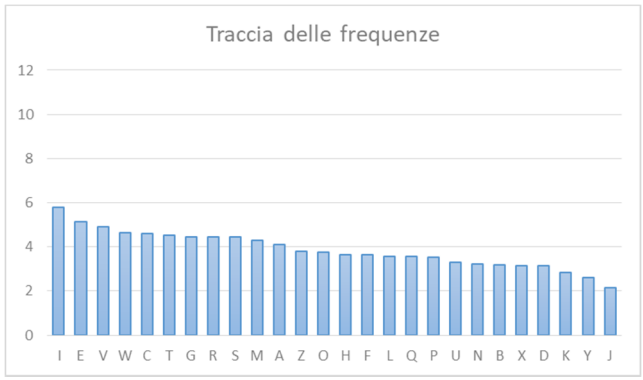
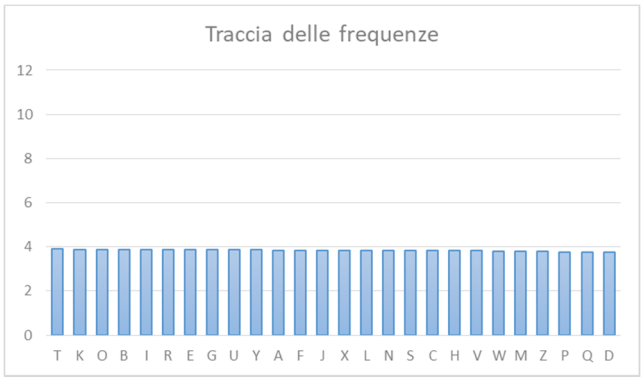
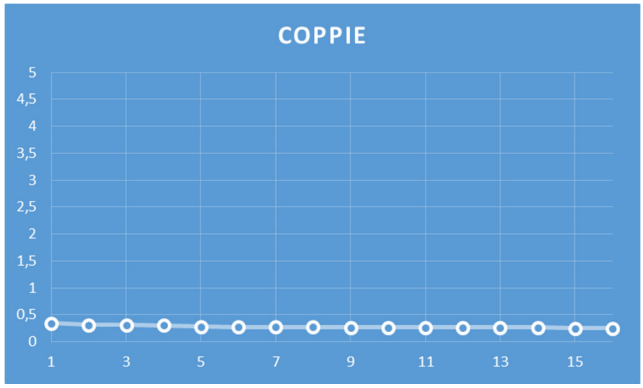
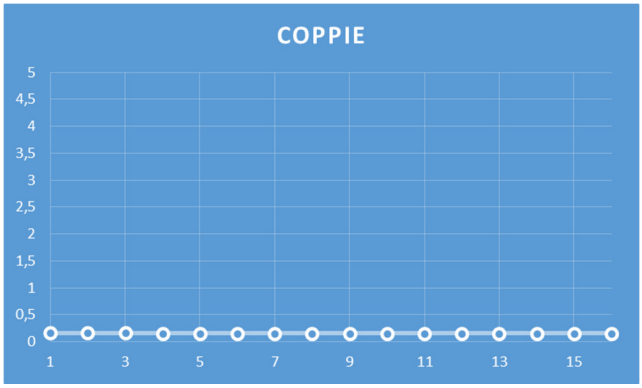
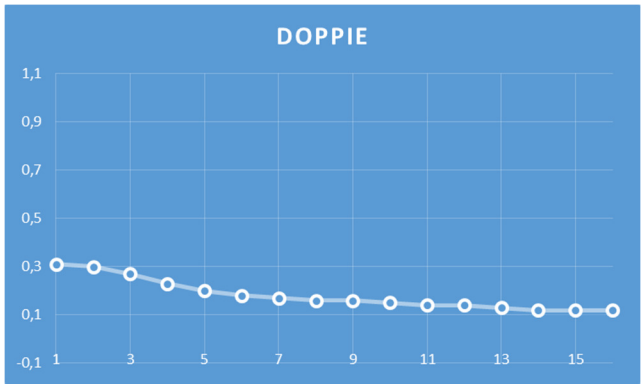
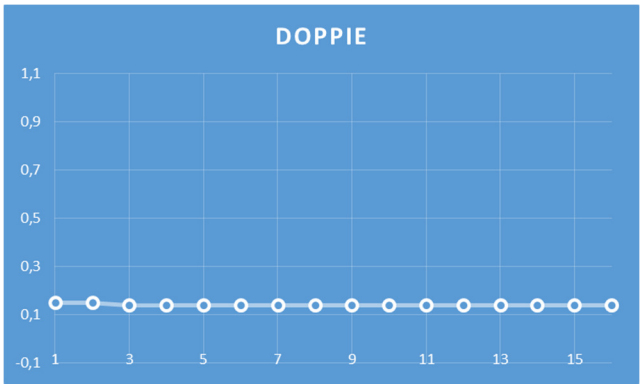
CHIAVE	C	O	C	O	M	E	R	O								
Testo cifrato	K	B	E	F	A	G	Z	O	V	C	T	W	M	W	L	R
Testo in chiaro																

Per valutare l'efficacia della tavola di Vigenère consideriamo il nostro solito testo di riferimento, *I promessi sposi*, è sottoponiamolo alla sostituzione polialfabetica con chiave `MONGOLFIERA`. Otteniamo i seguenti grafici (sono messi a confronto il testo in chiaro e il messaggio crittato)

MESSAGGIO PRIMA DI ESSERE CRITTATO	MESSAGGIO CRITTATO CON VIGENÈRE
	
	
	
	

Il cifrario di Vigenère mostra di funzionare molto bene, avvicinando le varie statistiche alle distribuzioni di una sequenza casuale e quindi coprendo in modo egregio le informazioni strutturali del testo. Si potrebbe pensare che una chiave estesa, idealmente lunga quanto il testo, possa eliminare del tutto tali informazioni generando grafici sostanzialmente piatti. In basso si è scelto di cifrare i *Promessi Sposi* (poco più di un milione di simboli alfabetici) con un cifrario di Vigenère utilizzando prima una chiave estremamente lunga (tutta la *Divina*

Commedia composta da più di 400.000 lettere) e poi una chiave di 10.000 caratteri disposti a caso e quindi privi di interconnessioni ortografiche. Il risultato è molto significativo:

MESSAGGIO CRITTATO CON VIGENÈRE utilizzando come chiave la *Divina Commedia*	MESSAGGIO CRITTATO CON VIGENÈRE utilizzando come chiave una sequenza casuale di 10.000 lettere
	
	
	
	

Come si vede, la chiave `MONGOLFIERA` e la chiave composta dall'intera *Divina Commedia* generano statistiche simili: abbiamo così scoperto che la "sovrapposizione" di due testi ortograficamente strutturati inquina ma non cancella le regolarità sottostanti (ci torneremo in seguito per decrittare Vigenère senza chiave). La prestazione migliore la raggiunge la chiave casuale, restituendo un testo apparentemente privo di struttura e che nasconde invece un romanzo di un milione di lettere! Le chiavi casuali indeterminatamente lunghe e soprattutto "usa e getta" (è cioè fatto divieto di usare la stessa chiave più di una volta) generano cifrature perfette e inviolabili: si

tratta di una tecnica ideale detta "**cifrario di Vernam**" e che può essere realizzata nella pratica soltanto con ragionevoli limitazioni.

Proponiamo in seguito alcune "quasi-realizzazioni" del cifrario di *Vernam* abbastanza facili da descrivere. Per facilitare l'esposizione e semplificare l'algoritmo stesso, è opportuno abbandonare per un po' le lettere e considerare soltanto messaggi composti dalle cifre decimali $0,1,2,\ldots 9$ (ottenute traducendo il testo con una qualche tavola 10×10 con *omofoni*, *metasimboli* e chissà che altro). In casi del genere la tavola di Vigenère si riduce alla tabella mostrata a fianco. Come vedremo sotto, essa gode di una bella proprietà che rende inutile averla sotto gli occhi (sia in fase di cifratura che di decifratura):

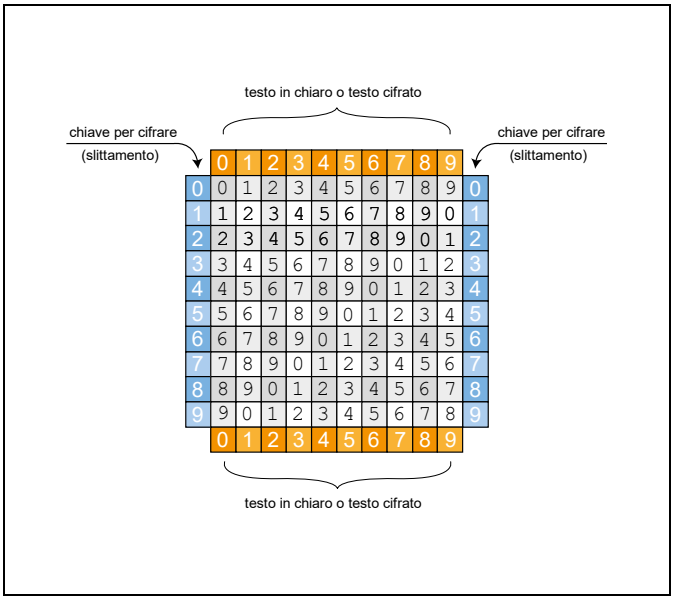


Tavola di Vigenere numerica

I numeri presenti agli incroci di una riga e di una colonna sono dati dalla *somma circolare* dei numeri ai bordi. La "somma circolare" è la somma senza riporto ed è spiegata nel seguente un esempio:

Chiave	5	3	7	0	9
Testo	2	9	1	2	4
Cifra	**7**				

Perché $5 + 2 = 7$

Chiave	5	3	7	0	9
Testo	2	9	1	2	4
Cifra	7	**2**			

Perché $3 + 9 = 12$ e nella *somma circolare* conta soltanto le cifra delle unità $(12 \rightarrow \boxed{2})$

Chiave	5	3	7	0	9
Testo	2	9	1	2	4
Cifra	**7**	**2**	**8**	**2**	**3**

…e così via…

Per decifrare basterà eseguire la "differenza circolare" fra cifra e chiave, cioè la differenza senza riporto. Essa si calcola come la normale sottrazione se il minuendo è maggiore o uguale al sottraendo e, in caso contrario, aggiungendo 10 al minuendo prima di effettuare l'operazione. È importante ricordarsi di effettuare la sottrazione circolare "`Cifra` *meno* `chiave`" (e non viceversa).

Cifra	**7**	**2**	**8**	**2**	**3**
Chiave	5	3	7	0	9
Testo	2				

Perché $7 - 5 = 2$

Cifra	**7**	**2**	**8**	**2**	**3**
Chiave	5	3	7	0	9
Testo	2	9			

Perché $2 < 3$ e $12 - 3 = 9$.

Cifra	**7**	**2**	**8**	**2**	**3**
Chiave	5	3	7	0	9
Testo	2	9	1	2	4

…e così via…

Possiamo immaginare le operazioni di addizione e sottrazione circolare come normali operazioni svolte su un orologio con 10 ore anziché 12. L'insieme delle regole di calcolo in questo tipo di spazio numerico si chiama **Aritmetica Modulare** e rappresenta un campo della Matematica importantissimo.

Vediamo ora di fare un po' di esercizio con questa tecnica di calcolo (e di crittazione di Vigenère):

Considera la chiave composta dalle prime 20 cifre di π

CHIAVE: 31415926535897932385

Critta il testo "Domani nevica", cioè "DOMANINEVICA" tradotto con la tavola 10×10 mostrata a fianco.

MESSAGGIO: 96729550358852993835741

(*da notare che trattandosi di una tavola con omofoni, esistono vari modi per tradurre in cifra il testo*)

Critta "alla Vigenère" effettuando una somma circolare:

TAVOLA 10×10 CON OMOFONI

	0	1	2	3	4	5	6	7	8	9
0	R	I	U	S	A	T	A	N	I	U
1	O	T	R	I	O	Q	U	D	T	T
2	E	S	N	C	C	M	T	R	X	E
3	O	J	I	S	L	N	E	E	N	O
4	R	A	E	I	I	E	O	N	L	A
5	A	L	I	A	E	A	A	C	I	O
6	E	S	N	G	P	K	S	R	A	H
7	P	A	O	B	A	E	R	D	L	L
8	P	V	T	I	T	N	F	O	E	O
9	W	E	C	V	E	M	D	Y	Z	Z

Chiave	3	1	4	1	5	9	2	6	5	3	5	8	9	7	9	3	2	3	8	5	3	1	4	1
Testo	**9**	**6**	**7**	**2**	**9**	**5**	**5**	**0**	**3**	**5**	**8**	**3**	**8**	**5**	**2**	**9**	**9**	**3**	**8**	**3**	**5**	**7**	**4**	**1**
Cifra	**2**	**7**	**1**	**3**	**4**	**4**	**7**	**6**	**8**	**8**	**3**	**1**	**7**	**2**	**1**	**2**	**1**	**6**	**6**	**8**	**8**	**8**	**8**	**2**

9.3) Seguendo la stessa logica, utilizzando sempre la tavola 10×10 mostrata sopra e la chiave numerica composta dalle prime 20 cifre di π, critta il seguente messaggio: ALLARME GENERALE.

Chiave	3	1	4	1	5	9	2	6	5	3	5	8	9	7	9	3	2	3	8	5	3	1	4	1	5	9	2	6	5	3
Testo																														
Cifra																														

9.4) Le seguenti cifrature sono state ottenute sempre con la tavola e le chiavi precedenti. Trova in ciascun caso il messaggio in chiaro:

a)

Cifra	**9**	**4**	**9**	**3**	**1**	**6**	**6**	**7**	**1**	**9**	**8**	**8**	**4**	**8**	**4**	**7**
Chiave	3	1	4	1	5	9	2	6	5	3	5	8	9	7	9	3
TESTO																

b)

Cifra	**1**	**2**	**4**	**5**	**2**	**7**	**9**	**4**	**1**	**3**	**4**	**4**	**3**	**6**	**7**	**0**	**5**	**6**	**9**	**4**	**0**	**5**
Chiave	3	1	4	1	5	9	2	6	5	3	5	8	9	7	9	3	2	3	8	5	3	1
Testo																						

c)

Cifra	**2**	**6**	**9**	**6**	**2**	**5**	**1**	**3**	**1**	**7**	**2**	**0**	**7**	**7**	**7**	**3**	**5**	**5**	**1**	**0**	**6**	**4**
Chiave	3	1	4	1	5	9	2	6	5	3	5	8	9	7	9	3	2	3	8	5	3	1
Testo																						

Consideriamo una chiave numerica come "72823". Essa si ripete virtualmente all'infinito in modo da adattarsi a messaggi di lunghezza arbitraria. Possiamo allora considerare la chiave come la parte frazionaria del quoziente $\frac{72.823}{99.999}$ (sappiamo infatti che $\frac{72.823}{99.999} = 0,\overline{72823}$). Seguendo questa linea di pensiero e pensando a mantisse più caotiche, possiamo barattare la casualità della chiave (requisito essenziale del cifrario di *Vernam*) con la complessità delle cifre che compongono ad esempio le parti non intere dei numeri irrazionali. Non è difficile inventare sistemi che generino numeri irrazionali a partire da chiavi numeriche:

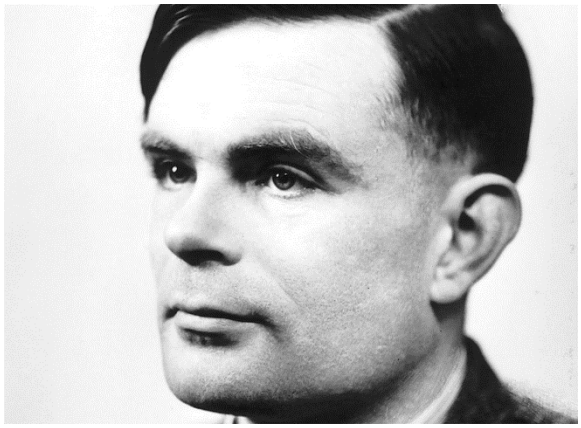
- Se la chiave numerica N è un intero positivo maggiore di 1 si può considerare il numero $\sqrt[N]{a(N)}$ dove $a(N)$ è una funzione definita a priori che restituisce un valore intero strettamente compreso tra due potenze N-esime successive (si può imporre ad esempio $N^N < a(N) < (N+1)^N$)
- Se la chiave numerica è una sequenza $a_1, a_2 .. a_n$ di numeri interi positivi (quindi maggiori di 0) si può considerare la frazione continua periodica $[1, \overline{a_1 a_2 a_3 \dots a_n}]$
- Se la chiave numerica è composta da tre interi positivi a, b, n con $a < b < n$ si può considerare il numero $\sqrt[n]{a^n + b^n}$. Il celebre "ultimo" teorema di Fermat assicura che $\sqrt[n]{a^n + b^n}$ sarà irrazionale .
- Qualche funzione trascendente (vedrete al triennio funzioni come $\sin(N)$ o $\ln(N)$)

Un altro modo per disporre di sequenze casuali potrebbe essere quello di appoggiarsi ad una "sequenza casuale pubblica", messa a disposizione da qualche sito ed enormemente lunga (triliardi di triliardi di cifre). Tale sequenza costituirebbe la chiave pubblica, mentre la chiave privata sarebbe semplicemente "l'indice di partenza" (corrispondente all'indicazione su dove iniziare a "pescare" le cifre). Un'altra opzione prevede che la "sequenza pubblica" venga sostituita da un "algoritmo pubblico", atto a creare sequenze caotiche a partire da una chiave privata fornita in ingresso.

Tutte queste idee portano ad altre domande che purtroppo non abbiamo modo di approfondire nel nostro percorso e alle quali accennerò soltanto brevemente:

ARITMETICIZZAZIONE DEGLI ALGORITMI - **È possibile inventare un sistema capace di "tradurre" ogni algoritmo in un numero?** Questa questione è importante perché, se la risposta fosse affermativa, si potrebbe pensare di condividere non già una chiave privata ma addirittura un "algoritmo privato", come il generatore di numeri caotici che negli esempi precedenti pensavamo di affidare ad un soggetto pubblico.

CASUALITÀ DETERMINISTICA – **Può un algoritmo generare una sequenza casuale?**



Entrambe le domande, per essere espresse e risolte in termini matematici, necessitano prima di tutto di robuste e chiare definizioni dei concetti di **algoritmo** e di **sequenza casuale**. La prima questione (ARITMETICIZZAZIONE DEGLI ALGORITMI) fu trattata tra gli altri da *Alan Turing (mostrato a fianco)*, importante matematico britannico del Novecento. Egli "atomizzò" il concetto di algoritmo in una serie di poche capacità primitive (leggere un simbolo, scrivere un simbolo, scorrere un elenco finito e ordinato) che potessero essere svolte tanto da un uomo quanto da un macchina. Turing mostrò che un meccanismo del genere (chiamato in seguito ***Macchina di Turing***) era in grado di svolgere tutti quei calcoli che comunemente si ritiene possano essere svolti in un tempo finito: in altre parole ogni algoritmo poteva essere tradotto in una Macchina di Turing e ogni Macchina di Turing era definita da un algoritmo. In base alla corrispondenza tra "problema calcolabile" e Macchina di Turing e per come viene definita quest'ultima, è molto facile associare a qualsiasi algoritmo un numero intero positivo. La domanda **È possibile inventare un sistema capace di "tradurre" ogni algoritmo in un numero?** Ha quindi risposta affermativa. Turing dimostrò inoltre che nessuna "macchina algoritmica" sarebbe stata in grado di rispondere correttamente a TUTTE le domande (ma questa è un'altra questione)

Il problema dell'esistenza di un algoritmo capace di generare "sequenze casuali" potrebbe sembrare assurdo, dal momento che ogni algoritmo per sua stessa definizione obbedisce a una serie di istruzioni in modo del tutto "non casuale"! Supponiamo però di disporre di una sequenza finita effettivamente non prevedibile (magari ottenuta trascrivendo la terza cifra dopo virgola della temperatura misurata in un certo posto), di trasformare i dati in una sequenza binaria finita come `0010100101110101…11`. Costruiamo poi una macchina di Turing atta a generare esattamente la sequenza binaria di partenza: in questo modo e a patto di usare l'algoritmo una volta soltanto, esso genera una sequenza che noi stessi abbiamo definito casuale all'inizio del testo. Prendiamo per buona questa idea di algoritmo "usa e getta" e aggiungiamo una condizione: fra tutti i possibili algoritmi che generano la sequenza iniziale consideriamo sempre quello più compatto, cioè quello composto da meno istruzioni. Poniamoci ora il seguente fondamentale problema: date delle sequenze di cui conosciamo gli algoritmi generatori, è possibile disinguere le sequenze casuali da quelle non casuali? Una possibile risposta è stata data da un altro matematico del Novecento, il russo Andrej Kolmogorov, ed è pressapoco la seguente (quella presentata ne rappresenta una versione molto semplificata): **se la sequenza e l'algoritmo sono scritti con lo stesso alfabeto, la sequenza può dirsi "casuale" (rispetto al linguaggio utilizzato) se è più breve dell'algoritmo che la genera.**

Vediamo un esempio e consideriamo il seguente strano linguaggio che utilizza l'alfabeto binario:

- `00` vuol dire `0`
- `01` vuol dire `1`
- `10` vuol dire "le prossime 4 cifre binarie sono il timbro"
- `11` vuol dire "timbro"

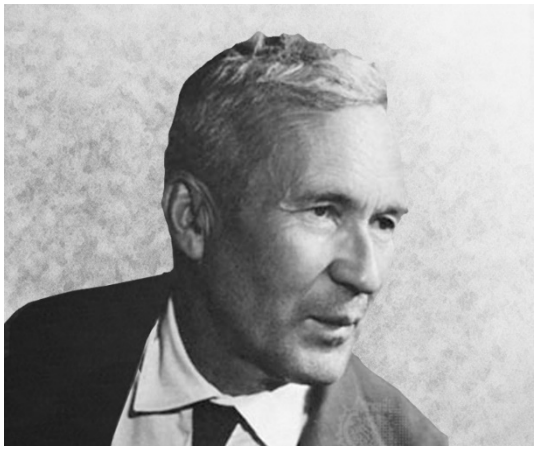
Con questo linguaggio la sequenza `0010100101110101` può essere generata in vari modi. Nella tabella in basso sono rappresentati l'algoritmo "banale" (che non usa i due simboli di istruzione `10` e `11`) e quello migliore (che fa uso del "timbro" `0101`), l'unico che ci interessa.

Sequenza originaria	0010100101110	13 cifre
Algoritmo generativo banale	00 00 01 00 01 00 00 01 00 01 01 01 00	26 cifre
Algoritmo generativo migliore	00 10 0101 11 00 11 01 01 11	**20 cifre**

Consideriamo per confronto una sequenza evidentemente non casuale come 0101010101010101.

Sequenza originaria	0101010101010101	16 cifre
Algoritmo generativo banale	00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01	32 cifre
Algoritmo generativo migliore	10 0101 11 11 11 11	**14 cifre**

Possiamo concludere che rispetto al linguaggio definito sopra, la prima sequenza 0010100101110101 è casuale secondo Kolmogorov (così come del resto appariva), mentre 010101010101 non lo è.



Il senso della definizione di Andrej Kolmogorov (a fianco una sua fotografia) è una ragionevole traduzione matematica dell'idea intuitiva che abbiamo della casualità: una serie di avvenimenti è casuale se non si può prevedere, se cioè se non c'è una legge che la descrive. Visto che qualsiasi elenco è, fra le altre cose, una descrizione di se stesso, bisogna precisare che una sequenza è casuale se il modo più breve per descriverla è proprio quello di elencarla elemento per elemento, e questo implica che, nel linguaggio adottato, qualsiasi algoritmo in grado di generarla deve essere più lungo della sequenza stessa.

Per concludere, è importante sottolineare che il "linguaggio" introdotto sopra a titolo di esempio è evidentemente pessimo, dallo scarsissimo potere riassuntivo. Tra le altre cose esso non genererà mai alcune configurazioni (11 che precede il primo 10, stringa che finisce con 10 e così via), indizio di cattiva compressione.

Per rispondere alla domanda dalla quale eravamo partiti "**Può un algoritmo generare una sequenza casuale?**" con l'aggiunta "**secondo Kolmogorov**", dobbiamo rispondere "No, perlomeno se vogliamo essere certi del risultato". Il motivo è il seguente: affinché un algoritmo generi una sequenza che possiamo definire casuale, la sequenza stessa non solo dovrebbe essere più breve dell'algoritmo stesso, ma più breve di qualsiasi algoritmo che, scritto con lo stesso linguaggio, la possa generare. Purtroppo fra le tante domande alle quali una macchina di Turing NON può generalmente dare una risposta c'è proprio la seguente: "Esiste una macchina di Turing B che con meno istruzioni fa la stessa cosa della macchina A?".

9.5) Inventa un linguaggio che usi soltanto le cifre 0 e 1 e composto, tra le altre cose, da istruzioni capaci di "descrivere" un codice binario. Relativamente al tuo linguaggio, valuta se le seguenti sequenze si possono definire causali:

	SEQUENZA	Lunghezza	Casuale (sì/no)
a)	1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0	30	

b)	1101001000100001000001000000	28	
c)	11111111111111111111111111111	30	
d)	11101111011111000000000	23	
e)	10111001010110101111	20	
f)	11111111111111100000000000000000	30	

9.6) È possibile inventare un linguaggio tale che nessuna sequenza sia casuale?

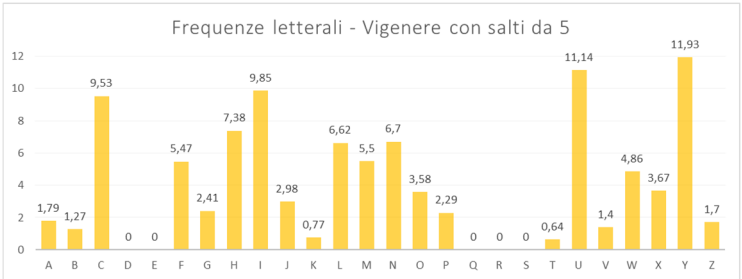
Torniamo al cifrario di Vigenère e cerchiamo di romperlo senza conoscere la chiave. Qui in basso è mostrato un esempio che ci consentirà di accompagnare il discorso teorico con un esempio. Supponiamo quindi di cifrare i soliti *Promessi Sposi* con un cifrario di Vigenère utilizzando una chiave di cinque lettere $X_1X_2X_3X_4X_5$. In basso è mostrato l'inizio del processo di crittazione:

Testo	Q	U	E	L	R	A	M	O	D	E	L	L	A	G	O	D	I	C	O	M	O
Chiave	X_1	X_2	X_3	X_4	X_5	X_1	X_2	X_3	X_4	X_5	X_1	X_2	X_3	X_4	X_5	X_1	X_2	X_3	X_4	X_5	X_1
Cifra	**K**	**L**	**E**	**Y**	**F**	**U**	**D**	**O**	**Q**	**S**	**F**	**C**	**A**	**T**	**C**	**X**	**Z**	**C**	**B**	**A**	**I**

La lunghezza della chiave sconosciuta $X_1X_2X_3X_4X_5$ ci dice che ogni cinque lettere è stato usato lo stesso alfabeto per cifrare.

Testo	Q	U	E	L	R	A	M	O	D	E	L	L	A	G	O	D	I	C	O	M	O
Chiave	**X_1**	X_2	X_3	X_4	X_5	**X_1**	X_2	X_3	X_4	X_5	**X_1**	X_2	X_3	X_4	X_5	**X_1**	X_2	X_3	X_4	X_5	**X_1**
Cifra	**K**	**L**	**E**	**Y**	**F**	**U**	**D**	**O**	**Q**	**S**	**F**	**C**	**A**	**T**	**C**	**X**	**Z**	**C**	**B**	**A**	**I**

Considerando quindi non già l'intero testo cifrato ma quello ottenuto estraendo ogni quinta lettera, possiamo considerare il messaggio come il frutto di una sostituzione **monoalfabetica** di un testo senza senso. Ciononostante esso è stato ottenuto tramite estrazione da un testo scritto in italiano e manterrà alcune caratteristiche statistiche della lingua di partenza, prima fra tutte le distribuzione delle frequenze letterali. A riprova di quanto detto in basso sono riportate l'analisi delle frequenze e la traccia delle frequenze relative alla "pesca" di ogni quinta lettera del messaggio "KLEYFUDO…":



Non dimentichiamo che ogni alfabeto cifrante usato è in Vigenère un alfabeto "slittato". Osservando le distanze reciproche delle colonne dominanti, è del tutto evidente che la U e la Y corrispondono alla A e alla E: a questo punto è "crollato" l'intero alfabeto indotto da X_1. Possiamo ripetere questo tipo di "attacco a salti regolari" partendo dalla seconda lettera della chiave e così via, ad esaurire tutte e cinque le sue lettere.

Testo	Q	U	E	L	R	A	M	O	D	E	L	L	A	G	O	D	I	C	O	M	O
Chiave	X_1	X_2	X_3	X_4	X_5	X_1	X_2	X_3	X_4	X_5	X_1	X_2	X_3	X_4	X_5	X_1	X_2	X_3	X_4	X_5	X_1
Cifra	**K**	**L**	**E**	**Y**	**F**	**U**	**D**	**O**	**Q**	**S**	**F**	**C**	**A**	**T**	**C**	**X**	**Z**	**C**	**B**	**A**	**I**

Un modo per rendere il cifrario di Vigenère più robusto è quello di sostituire i singoli alfabeti "slittati" con alfabeti rimescolati in modo meno regolare. Questo si può fare usando la chiave di Vigenère per trasporre l'alfabeto collegato alla A (magari tramite una trasposizione a colonne o a chiave scalare), determinare la traccia di permutazione (accertandosi al contempo del periodo della trasformazione) e iterare la permutazione su ogni alfabeto cifrante: in questo modo l'alfabeto della A corrisponde ad una cifratura semplice, l'alfabeto della B alla doppia cifratura, l'alfabeto della C alla tripla e così via.

Vediamo un esempio e consideriamo la chiave SCUOLA. Iniziamo con il calcolo della traccia di permutazione.

S	C	U	O	L	A
5	2	6	4	3	1
					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	

1	2	3	4	5	6	7	8	9	10	11	12	13
12	2	13	23	3	14	18	24	4	9	15	19	25

14	15	16	17	18	19	20	21	22	23	24	25	26
5	7	10	16	20	26	1	6	8	11	17	21	22

	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
traccia	20	2	5	9	14	21	15	22	10	16	23	1	3	6	11	17	24	7	12	18	25	26	4	8	13	19

Traccia: $[20, 2, 5, 9, 14,21,15, 22, 10, 16, 23, 1, 3, 6, 11, 17, 24, 7, 12, 18, 15, 16, 4, 8, 13, 19]$

Rappresentazione per cicli: $(1, 20, 18, 7, 15, 11, 23, 4, 9, 10, 16, 17, 24, 8, 22, 26, 19, 12)\ (2)(3, 5, 14, 6, 21, 25, 13)$

Calcolo del periodo: $mcm(18,1,7) = 126$

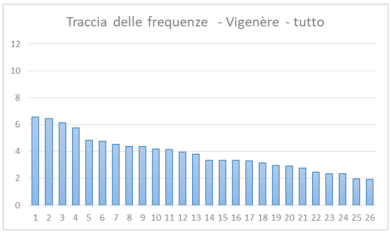
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	L	B	M	W	C	N	R	X	D	I	O	S	Y	E	G	J	P	T	Z	A	F	H	K	Q	U	V
B	V	F	M	T	D	I	L	H	S	E	Q	G	J	N	X	V	B	F	G	U	M	L	J	O	K	T
C	T	D	C	P	X	B	E	T	N	U	Z	D	R	G	L	Q	C	F	S	O	K	V	P	H	Y	I
D	K	A	T	Z	J	Y	E	V	R	G	X	I	Q	F	W	S	O	U	D	J	B	Y	S	M	E	X
E	W	J	E	O	V	R	N	K	D	B	F	V	U	M	P	R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

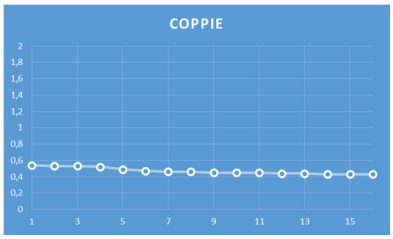
K	V	W	T	R	S	P	N	Y	Z	G	O	H	J	X	C	D	L	K	E	I	P	B	N	L	F	Y
L	L	B	M	W	C	N	R	X	D	I	O	S	Y	E	G	J	P	T	Z	A	F	H	K	Q	U	V
M	V	F	M	T	D	I	L	H	S	E	Q	G	J	N	X	V	B	F	G	U	M	L	J	O	K	T
N	T	D	C	P	X	B	E	T	N	U	Z	D	R	G	L	Q	C	F	S	O	K	V	P	H	Y	I
O	K	A	T	Z	J	Y	E	V	R	G	X	I	Q	F	W	S	O	U	D	J	B	Y	S	M	E	X
P	W	J	E	O	V	R	N	K	D	B	F	V	U	M	P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

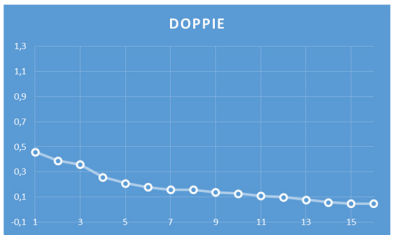
Questo potenziamento di Vigenère ha naturalmente un prezzo in termini di velocità, dal momento che la costruzione (da parte del cifratore) e la ricostruzione (da parte del decifratore) della tavola sono due operazioni dispendiose, perlomeno se fatte manualmente. Si potrebbe pensare che tali precauzioni siano comunque superflue, dal momento che la rottura del codice resta possibile a patto di conoscere la lunghezza della chiave. Il prossimo esempio mostra che purtroppo la lunghezza della chiave è un segreto di Pulcinella.
Consideriamo ad esempio il solito romanzo di Manzoni cifrato alla Vigenère (semplice o potenziato, non importa) con una chiave di lunghezza ignota. Si può sottoporre il messaggio alle solite analisi, considerando tutto il testo o il messaggio ottenuto per saltando una lettera ogni due, ogni tre, ogni quattro e così via:

PASSO

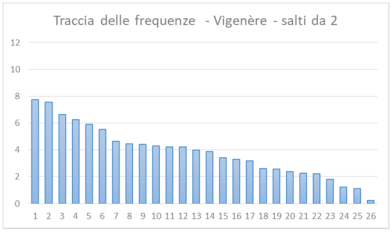
1

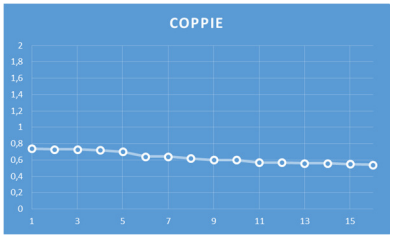


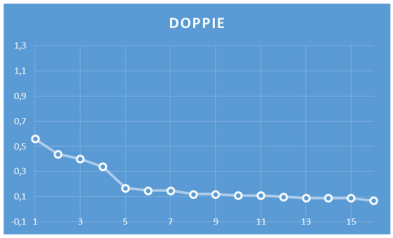




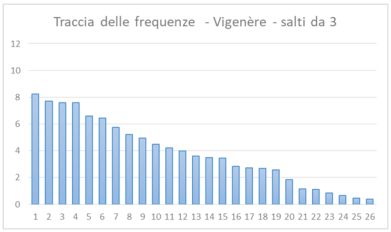
2

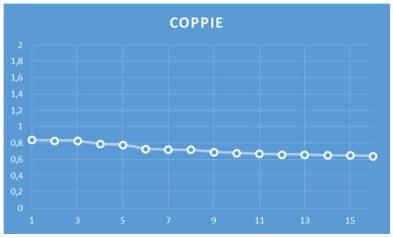


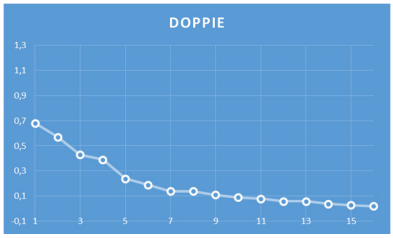




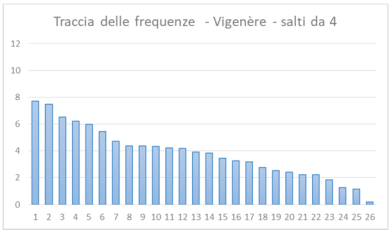
3

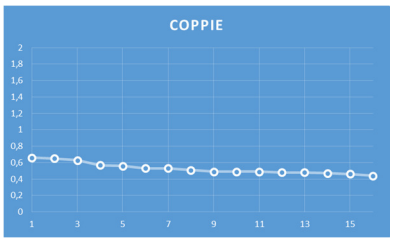


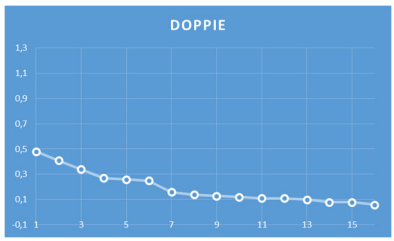




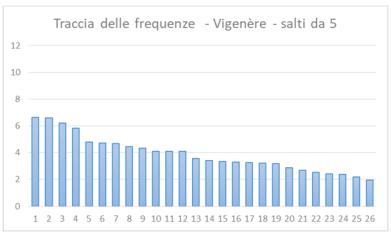
4

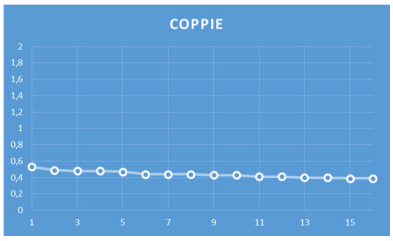


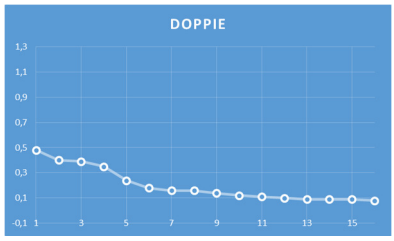




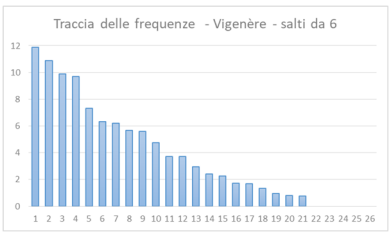
5

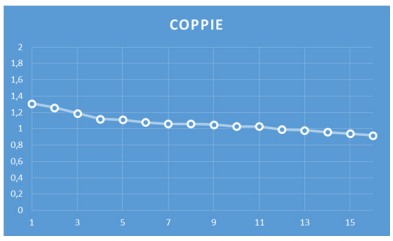


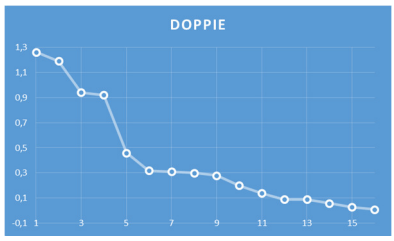




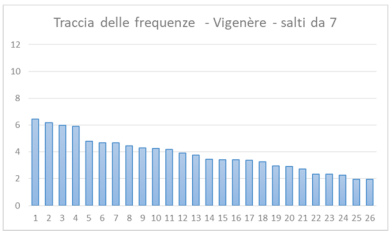
6

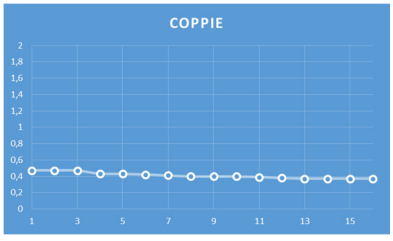


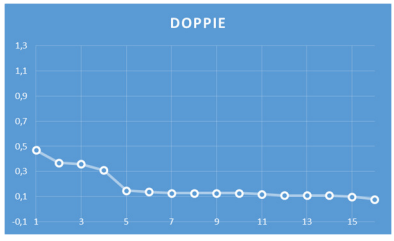




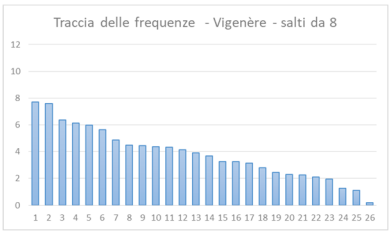
7

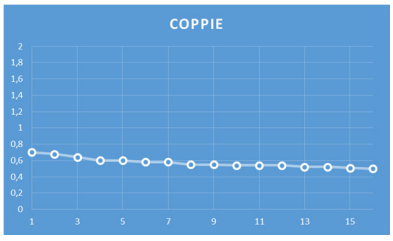


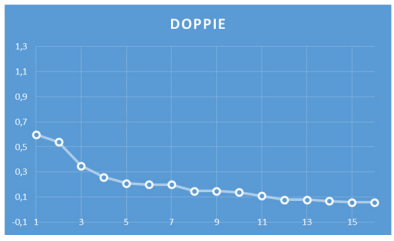




8







9.7) Tra tutte le righe sovrastante ve ne è una che spicca sulle altre. Sapresti trovarla e ipotizzare le cause della sua peculiarità?

Da un punto di vista statistico e squisitamente numerico, tra tutti i dati analizzati sopra quello più indicativo pare essere la percentuale associata alla *doppia* più frequente: si passa da valori compresi tra $0{,}5$ e $0{,}7$ nel caso di "lunghezze sbagliate" ad un clamoroso $1{,}3$ (cioè il doppio) per la lunghezza corretta. La strategia critto-analitica basata sull'analisi statistica delle doppie è stata inventata da un importante crittoanalista americano del Novecento, William Frederick Friedman.

Un altro tipo di attacco che può essere mosso ad un cifrario di Vigenère (efficace se applicato a messaggi lunghi) si basa su una semplice constatazione: visto che il verme si ripete sempre uguale a se stesso, può capitare che esso cifri sequenze letterali "in fotocopia" Per capire il senso di quanto appena detto, considerate una chiave breve (quindi pessima ma adatta all'esemplificazione) come "CUORE" e un messaggio con molte ripetizioni, come "amor che a nullo amato amar perdona". Abbiamo quindi…

Testo	A	M	O	R	C	H	A	E	N	U	L	L	O	A	M	A	T	O	A	M	A	R	P	E	R	D	O	N	A
Chiave	C	U	O	R	E	C	U	O	R	E	C	U	O	R	E	C	U	O	R	E	C	U	O	R	E	C	U	O	R
Cifra	**C**	**G**	**C**	**I**	**G**	**J**	**Y**	**O**	**E**	**Y**	**N**	**F**	**C**	**R**	**Q**	**C**	**N**	**C**	**R**	**Q**	**C**	**L**	**D**	**V**	**V**	**F**	**I**	**B**	**R**

Osservando con attenzione la cifra, è facile riconoscere un'anomala ricorrenza di un gruppo di 4 lettere.

Cifra	**C**	**G**	**C**	**I**	**G**	**J**	**Y**	**O**	**E**	**Y**	**N**	**F**	**C**	**R**	**Q**	**C**	**N**	**C**	**R**	**Q**	**C**	**L**	**D**	**V**	**V**	**F**	**I**	**B**	**R**

L'anomalia potrebbe essere semplicemente frutto del caso o più verosimilmente causata dal perfetto sovrapporsi del verme con una sequenza ricorrente del messaggio.

Testo	A	M	O	R	C	H	A	E	N	U	L	L	O	A	M	A	T	O	A	M	A	R	P	E	R	D	O	N	A
Chiave	C	U	O	R	E	C	U	O	R	E	C	U	O	R	E	C	U	O	R	E	C	U	O	R	E	C	U	O	R
Cifra	**C**	**G**	**C**	**I**	**G**	**J**	**Y**	**O**	**E**	**Y**	**N**	**F**	**C**	**R**	**Q**	**C**	**N**	**C**	**R**	**Q**	**C**	**L**	**D**	**V**	**V**	**F**	**I**	**B**	**R**

L'ipotesi che la ricorrenza sia dovuta a una perfetta sovrapposizione del verme con una sequenza letterale del messaggio, porta a concludere che il verme stesso sia lungo 5 lettere (nel caso di lunghezze che non siano numeri primi potrebbe trattarsi di un divisore dell'intervallo di ricorrenza).
L'analisi dei gruppi ricorrenti è una tecnica inventata autonomamente nell'Ottocento dall'inglese Babbage, e dal tedesco Kasiski (a cui normalmente si attribuisce la tecnica). Lo scarso vantaggio crittografico di una chiave "lunghissima" scritta però in una lingua reale (il cifrato dei *Promessi Sposi* ottenuto con la chiave *Divina Commedia* ne è un esempio) è dovuto anche a sequenze "di tipo di Kasiski", che preservano incidentalmente informazioni sulla struttura ortografica del binomio messaggio-chiave.

I cifrari di Vigenère si possono quindi effettivamente rompere e il loro punto debole risiede nella relativa trasparenza alla lunghezza della chiave, specialmente se essa è molto più breve del testo. Per migliorare Vigenère è quindi sensato perseguire una delle due strategie:

1) Indurre continui e casuali interruzioni o modifiche del verme attraverso *metasimboli*
2) "Rigenerare" il verme in un modo diverso dalla semplice ripetizione continua della chiave e in questo modo creare vermi molto lunghi, eventualmente estesi quanto il testo stesso

Vediamo la strategia **1)**
Per dissimulare l'uso di uno o più *metasimboli*, è opportuno trasvestirli da lettere dell'alfabeto: per fa ciò sarà necessario rinunciare a qualche lettera rara, sostituendola con lettere foneticamente sovrapponibili. L'alfabeto in basso fa una grande "economia di lettere" e permette di ricavare dall'alfabeto classico ben quattro *metasimboli*.

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

In un alfabeto del genere, una frase come “`Quando Joker andò a New York`” verrebbe scritta come “`Kuando Ioker andò a Nev Iork`”, che, al di là dell’ortografia, non inficia la leggibilità del testo.

Per i nostri scopi basterà comunque un alfabeto con un solo *metasimbolo*: sacrifichiamo quindi la W:

Alfabeto con metasimbolo `W`																									
Lettera	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
significato	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

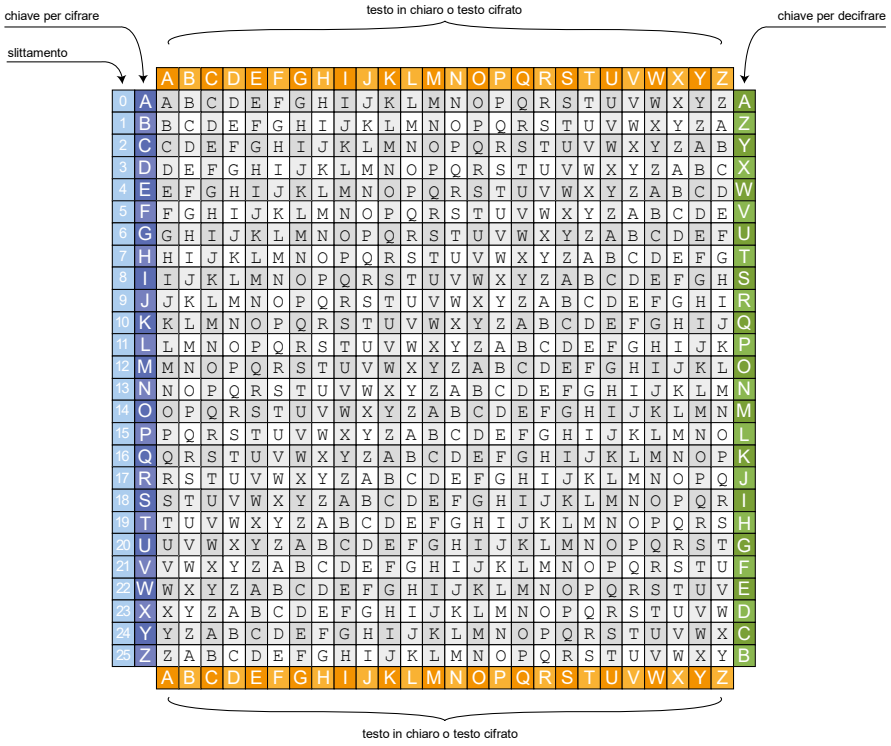
Supponiamo ora di cifrare la frase “`Chi non risica non rosica`”, con la chiave “`Ciao`”. Per spezzare la normale ripetizione della chiave, inseriamo a caso 3 metasimboli **`W`** : `Chi`**`W`**` non ri`**`W`**`sica non ros`**`W`**`ica`

Testo	C	H	I	W	N	O	N	R	I	W	S	I	C	A	N	O	M	R	O	S	W	I	C	A
Chiave	C	I	A	O	C	I	A	O	C	I	C	I	A	O	C	I	A	O	C	I	A	C	I	A
Cifra																								

Come si vede, dopo ogni occorrenza del *metasimbolo* **`W`** la chiave viene ripetuta daccapo. Ciò avviene obbligatoriamente “dopo” la comparsa del *metasimbolo* e non in contemporanea (vedremo che ciò è essenziale per permettere al destinatario di decrittare il messaggio):

Applichiamo al messaggio sovrastante la cifratura (con una tavola di Vigenère classica come quella riportata in basso) e inseguito tentiamo la decifratura.

Testo	C	H	I	W	N	O	N	R	I	W	S	I	C	A	N	O	N	R	O	S	W	I	C	A
Chiave	C	I	A	O	C	I	A	O	C	I	C	I	A	O	C	I	A	O	C	I	A	C	I	A
Cifra	**E**	**P**	**I**	**K**	**P**	**W**	**N**	**F**	**K**	**E**	**U**	**Q**	**C**	**O**	**P**	**W**	**N**	**F**	**Q**	**A**	**W**	**K**	**K**	**A**



Cifra		E	P	I	K	P	W	N	F	K	E	U	Q	C	O	P	W	N	F	Q	A	W	K	K	A
Chiave	(ciao)	C																							
Testo																									

Stavolta non possiamo riempire la riga della chiave con continue ripetizioni di "ciao" perché non sappiamo se e quando queste ripetizioni verranno interrotte. L'unica lettera sicura è la "C" (la prima lettera della chiave):

Cifra		E	P	I	K	P	W	N	F	K	E	U	Q	C	O	P	W	N	F	Q	A	W	K	K	A
Chiave	(ciao)	C																							
Testo		**C**																							

Visto che la lettera trovata non è il *metasimbolo* **W**, possiamo continuare al solito modo. Proseguiamo quindi così fino a incappare in una **W**.

Cifra		E	P	I	K	P	W	N	F	K	E	U	Q	C	O	P	W	N	F	Q	A	W	K	K	A
Chiave	(ciao)	C	I	A	O																				
Testo		**C**	**H**	**I**	**W**																				

Eccola qui! La W non fa parte del messaggio e quindi non deve essere trascritta. Bisogna però ripartire daccapo con il verme.

Cifra		E	P	I	K	P	W	N	F	K	E	U	Q	C	O	P	W	N	F	Q	A	W	K	K	A
Chiave	(ciao)	C	I	A	O	C	I	A	O	C	I														
Testo		**C**	**H**	**I**	**W**	**N**	**O**	**N**	**R**	**I**	**W**														

Di nuovo ignoriamo la W nella trascrizione del messaggio (il testo in chiaro è quindi, a questo momento, "CHINONRI") e facciamo ripartire il verme.

Cifra		E	P	I	K	P	W	N	F	K	E	U	Q	C	O	P	W	N	F	Q	A	W	K	K	A
Chiave	(ciao)	C	I	A	O	C	I	A	O	C	I	C	I	A	O	C	I	A	O	C	I	A			
Testo		**C**	**H**	**I**	**W**	**N**	**O**	**N**	**R**	**I**	**W**	**S**	**I**	**C**	**A**	**N**	**O**	**N**	**R**	**O**	**S**	**W**			

Siamo quasi alla fine…

Cifra		E	P	I	K	P	W	N	F	K	E	U	Q	C	O	P	W	N	F	Q	A	W	K	K	A
Chiave	(ciao)	C	I	A	O	C	I	A	O	C	I	C	I	A	O	C	I	A	O	C	I	A	C	I	A
Testo		**C**	**H**	**I**	**W**	**N**	**O**	**N**	**R**	**I**	**W**	**S**	**I**	**C**	**A**	**N**	**O**	**N**	**R**	**O**	**S**	**W**	**I**	**C**	**A**

Abbiamo così ritrovato il messaggio iniziale.

9.8) Decifra i seguenti messaggi cifrati con Vigenère con "interruzione del verme" indotta dal *metasimbolo* **W**.

	MESSAGGIO	CHIAVE
a)	BINRIMNZXTEAIPRDAIUMDVE	PIAVE
b)	NOIROIUGHDLWIUWSPJQGNQGI	COMPUTER
c)	EONLDZIRKZKBOEVV	TORINO
d)	AQZIFQKERQBLPLNAKD	ARDORE

Cifra		B	I	N	R	I	M	N	Z	X	T	E	A	I	P	R	D	A	I	U	M	D	V	E
Chiave	(piave)	P																						
Testo																								

Cifra		N	O	I	R	O	I	U	G	H	D	L	W	I	U	W	S	P	J	Q	G	N	Q	G	I
Chiave	(computer)	C																							
Testo																									

Cifra		E	O	N	L	D	Z	I	R	K	Z	K	B	O	E	V	V
Chiave	(torino)	T															
Testo																	

Cifra		A	Q	Z	I	F	Q	K	E	R	Q	B	L	P	L	N	A	K	D
Chiave	(ardore)	A																	
Testo																			

Possiamo ora passare alla strategia numero **2)**: allungare, rigenerare, moltiplicare il verme in modi differenti dalla semplice ripetizione:

Esistono molti modi per ottenere questo risultato e alcuni li abbiamo già visti sotto spoglie diverse. Vediamo quindi alcuni esempi:

VERMI AUTOGENERANTI PER SOSTITUZIONE

Consideriamo la tavola di Vigenère "potenziata" creata in precedenza iterando su ogni riga un rimescolamento definito dalla chiave di 6 lettere SCUOLA. Avevamo così ottenuto il seguente quadrato 26×26 che, in base ai nostri calcoli, potrebbe essere allungato di altre 100 righe fino a portarlo ad un rettangolo 126×26 (infatti il periodo dell'iterazione risultava uguale a 126).

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

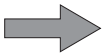
T	D	C	P	X	B	E	T	N	U	Z	D	R	G	L	Q	C	F	S	O	K	V	P	H	Y	I
K	A	T	Z	J	Y	E	V	R	G	X	I	Q	F	W	S	O	U	D	J	B	Y	S	M	E	X

Leggendo ora il rettangolo riga per riga o addirittura procedendo a *ZigZag* per maggiore segretezza, disporremmo potenzialmente di un verme di $126 \cdot 26 = 3276$ lettere: si tratta di un verme tutt'altro che casuale, definito da un algoritmo semplice e decisamente laborioso da implementare. Abbiamo comunque generato un verme molto lungo come ci eravamo prefissi.

VERMI AUTOGENERANTI PER TRASPOSIZIONE

Consideriamo un verme composto da 16 lettere come DUELAVASTOVIGLIE. Consideriamo le ultime 4 lettere come chiave per cifrare il verme stesso. Usiamo una tecnica crittografica qualsiasi come la trasposizione per la chiave scalare:

G	L	I	E
2	4	3	1
			D
U	E	L	A
		V	A
	S	T	O
			V
I	G	L	I
		E	



UIESGLVTLEDAAOVI

Abbiamo così ottenuto un secondo verme da giustapporre al primo. Il procedimento si può ora applicare a quest'ultima parola e così via, iterando il procedimento secondo necessità.

Il difetto dell'autogenerazione per trasposizione è quello di riutilizzare sempre e solo le lettere del verme originale (e quindi, nel cifrario di Vigenère, di utilizzare sempre e solo gli alfabeti associati a quelle lettere).

VERMI FAGOCITANTI

I due metodi visti in alto hanno il difetto di essere legati a sistemi crittografici semplici e soprattutto al rimescolamento di insiemi fissi (in un caso l'alfabeto, nell'altro il verme stesso). L'uovo di Colombo è di usare il messaggio stesso per allungare del verme. Con ciò si realizzano due obiettivi ambiziosi: in primo luogo il verme è per definizione lungo quanto il messaggio (anzi, lo supera della chiave iniziale), in secondo luogo esso è "casuale", nel senso che non obbedisce ad una regolarità matematica.

Consideriamo il seguente esempio:

Messaggio da cifrare: AVVISTATOAEREONEMICO
Chiave: UNO

Testo	A	V	V	I	S	T	A	T	O	A	E	R	E	O	N	E	M	I	C	O
Chiave	U	N	O	**A**	**V**	**V**	**I**	**S**	**T**	**A**	**T**	**O**	**A**	**E**	**R**	**E**	**O**	**N**	**E**	**M**
Cifra	**U**	**I**	**J**	**I**	**N**	**O**	**I**	**L**	**H**	**A**	**X**	**F**	**E**	**S**	**E**	**I**	**A**	**V**	**G**	**A**

Questo ultimo metodo è tanto elegante quanto vulnerabile, come mostrato nell'esempio seguente.

Testo																										
Chiave																										
Cifra	**V**	**R**	**X**	**I**	**M**	**W**	**X**	**U**	**D**	**B**	**I**	**A**	**T**	**K**	**I**	**J**	**X**	**J**	**X**	**V**	**J**	**M**	**K**	**R**	**B**	**M**	**T**	**R**

Supponiamo che il messaggio sia stato intercettato nelle comunicazioni standard del primo mattino che contengono informazioni sul tempo. Possiamo immaginare che il testo in chiaro contenga la parola “meteo”. Il verme fagocitante avrà esso stesso tale parola da qualche parte dopo la chiave: non resta che provare varie posizioni (supponendo per velocizzare un po’ i tempi che la chiave sia lunga almeno 4 lettere).

Chiave					M	E	T	E	O																		
Cifra	**V**	**R**	**X**	**I**	**M**	**W**	**X**	**U**	**D**	**B**	**I**	**A**	**T**	**K**	**I**	**J**	**X**	**J**	**X**	**V**	**J**	**M**	**K**	**R**	**B**	**M**	**T**	**R**
Testo					A	S	E	Q	P																			

Chiave						M	E	T	E	O																		
Cifra	**V**	**R**	**X**	**I**	**M**	**W**	**X**	**U**	**D**	**B**	**I**	**A**	**T**	**K**	**I**	**J**	**X**	**J**	**X**	**V**	**J**	**M**	**K**	**R**	**B**	**M**	**T**	**R**
Testo						K	T	B	Z	N																		

Chiave							M	E	T	E	O																	
Cifra	**V**	**R**	**X**	**I**	**M**	**W**	**X**	**U**	**D**	**B**	**I**	**A**	**T**	**K**	**I**	**J**	**X**	**J**	**X**	**V**	**J**	**M**	**K**	**R**	**B**	**M**	**T**	**R**
Testo							L	Q	K	X	U																	

Chiave								M	E	T	E	O																
Cifra	**V**	**R**	**X**	**I**	**M**	**W**	**X**	**U**	**D**	**B**	**I**	**A**	**T**	**K**	**I**	**J**	**X**	**J**	**X**	**V**	**J**	**M**	**K**	**R**	**B**	**M**	**T**	**R**
Testo								I	Z	I	E	M																

Chiave									M	E	T	E	O															
Cifra	**V**	**R**	**X**	**I**	**M**	**W**	**X**	**U**	**D**	**B**	**I**	**A**	**T**	**K**	**I**	**J**	**X**	**J**	**X**	**V**	**J**	**M**	**K**	**R**	**B**	**M**	**T**	**R**
Testo									R	X	P	W	F															

Chiave										M	E	T	E	O														
Cifra	**V**	**R**	**X**	**I**	**M**	**W**	**X**	**U**	**D**	**B**	**I**	**A**	**T**	**K**	**I**	**J**	**X**	**J**	**X**	**V**	**J**	**M**	**K**	**R**	**B**	**M**	**T**	**R**
Testo										P	E	H	P	W														

Chiave											M	E	T	E	O													
Cifra	**V**	**R**	**X**	**I**	**M**	**W**	**X**	**U**	**D**	**B**	**I**	**A**	**T**	**K**	**I**	**J**	**X**	**J**	**X**	**V**	**J**	**M**	**K**	**R**	**B**	**M**	**T**	**R**
Testo											W	W	A	G	U													

Chiave												M	E	T	E	O												
Cifra	**V**	**R**	**X**	**I**	**M**	**W**	**X**	**U**	**D**	**B**	**I**	**A**	**T**	**K**	**I**	**J**	**X**	**J**	**X**	**V**	**J**	**M**	**K**	**R**	**B**	**M**	**T**	**R**
Testo												O	P	R	E	V												

Chiave													M	E	T	E	O											
Cifra	**V**	**R**	**X**	**I**	**M**	**W**	**X**	**U**	**D**	**B**	**I**	**A**	**T**	**K**	**I**	**J**	**X**	**J**	**X**	**V**	**J**	**M**	**K**	**R**	**B**	**M**	**T**	**R**
Testo													H	G	P	F	J											

Chiave														M	E	T	E	O										
Cifra	**V**	**R**	**X**	**I**	**M**	**W**	**X**	**U**	**D**	**B**	**I**	**A**	**T**	**K**	**I**	**J**	**X**	**J**	**X**	**V**	**J**	**M**	**K**	**R**	**B**	**M**	**T**	**R**
Testo														Y	E	Q	T	V										

Fermiamoci e valutiamo quanto ottenuto finora: dei dieci tentativi due sembrano aver prodotto una stringa compatibile con l'italiano:

Prima stringa potenziale																										
Chiave								M	E	T	E	O														
Cifra	V	R	X	I	M	W	X	U	D	B	I	A	T	K	I	J	X	J	X	V	J	M	K	R	B	M	T	R
Testo								I	Z	I	E	M														

Seconda stringa potenziale																										
Chiave												M	E	T	E	O										
Cifra	V	R	X	I	M	W	X	U	D	B	I	A	T	K	I	J	X	J	X	V	J	M	K	R	B	M	T	R
Testo												O	P	R	E	V										

Il fatto di aver trovato due stringhe plausibili è tutt'altro che casuale, come si evince ritornando brevemente alla cifratura vista nell'introduzione:

Testo	A	V	V	I	S	T	A	T	O	A	E	R	E	O	N	E	M	I	C	O
Chiave	U	N	O	A	V	V	I	S	T	A	T	O	A	E	R	E	O	N	E	M
Cifra	**U**	**I**	**J**	**I**	**N**	**O**	**I**	**L**	**H**	**A**	**X**	**F**	**E**	**S**	**E**	**I**	**A**	**V**	**G**	**A**

Il cifrario di Vigenère tratta infatti verme e messaggio esattamente allo stesso modo (basta studiare la tavola e confrontare gli incroci con righe e colonne scambiate), per cui cifrare il messaggio con il verme o cifrare il verme con il messaggio produce lo stesso testo. Questo implica che se il verme stesso contiene il messaggio (come succede con questa tecnica crittografica), la parola civetta usata per decifrare produrrà due stringhe sensate in due posti diversi (una volta quando decifra il testo e una quando decifra il verme). Per di più lo slittamento relativo tra le due occorrenze sensate restituisce proprio la lunghezza della chiave.

Lo slittamento relativo delle due stringhe potenziali individuate prima è di 4 unità (più breve della parola civetta). Abbiamo quindi la seguente situazione:

Testo	T_1	T_2	T_3	T_4	T_5	T_6	T_7	**M**	**E**	**T**	**E**	**O**	T_{13}	T_{14}	T_{15}	…
Chiave	**X**	**X**	**X**	**X**	T_1	T_2	T_3	T_4	T_5	T_6	T_7	**M**	**E**	**T**	**E**	…

…che possiamo affinare con le prime informazioni trovate…

Testo	T_1	T_2	T_3	T_4	T_5	T_6	T_7	**M**	**E**	**T**	**E**	**O**	**P**	**R**	**E**	**V**	T_{17}
Chiave	**X**	**X**	**X**	**X**	T_1	T_2	T_3	**I**	**Z**	**I**	**E**	**M**	**E**	**T**	**E**	**O**	T_{11}

e quindi….

Testo	T_1	T_2	T_3	**I**	**Z**	**I**	**E**	**M**	**E**	**T**	**E**	**O**	**P**	**R**	**E**	**V**	T_{17}
Chiave	**X**	**X**	**X**	**X**	T_1	T_2	T_3	**I**	**Z**	**I**	**E**	**M**	**E**	**T**	**E**	**O**	**P**

Possiamo ora usare le informazioni per continuare a decrittare:

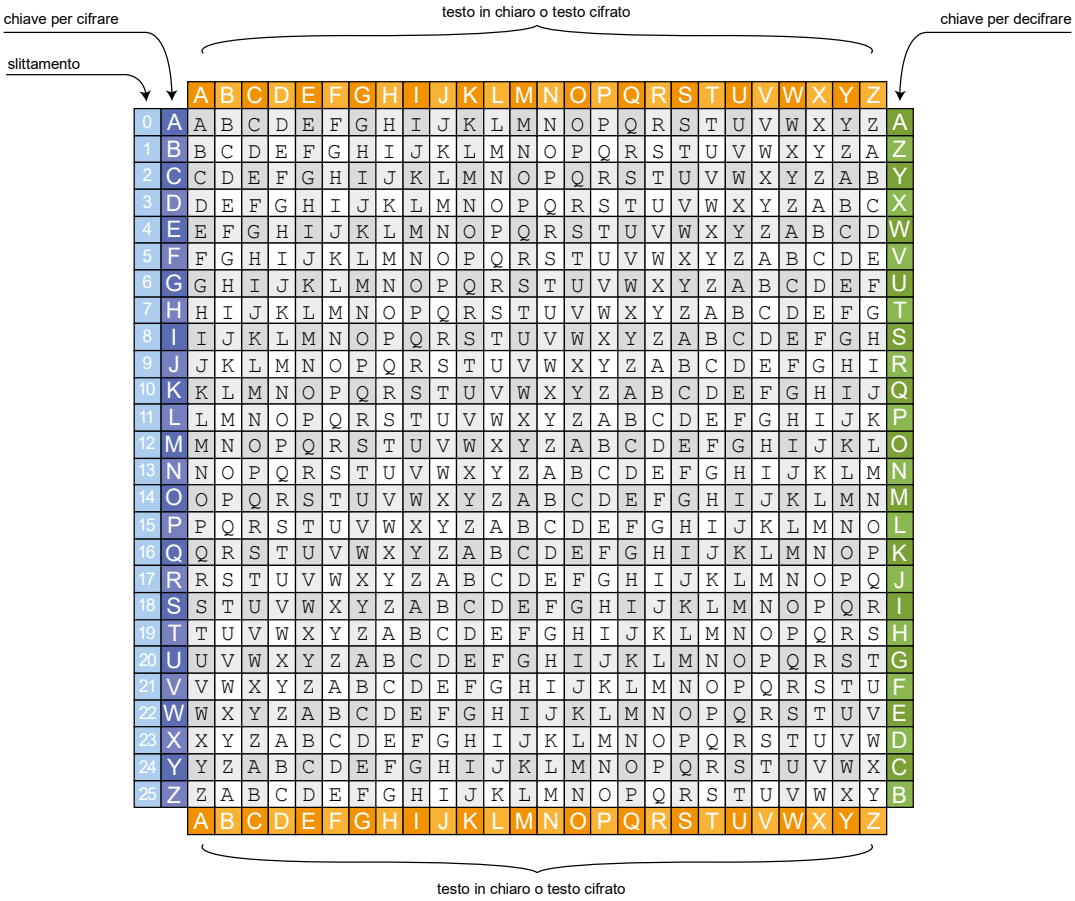
Testo	T_1	T_2	T_3	I	Z	I	E	M	E	T	E	O	P	R	E	V	**I**

Chiave	X	X	X	X	N	O	T	I	Z	I	E	M	E	T	E	O	P
Cifra	V	R	X	I	M	W	X	U	D	B	I	A	T	K	I	J	X

Siamo ora in grado di scoprire anche la chiave utilizzata:

Testo	N	O	T	I	Z	I	E
Chiave	X	X	X	X	N	O	T
Cifra	V	R	X	I	M	W	X

Testo	N	O	T	I	Z	I	E
Chiave	I	D	E	A	N	O	T
Cifra	V	R	X	I	M	W	X



9.9) Cimentatevi ora voi la seguente decifratura segreta (la tecnica crittografica usata è un cifrario di Vigenère con verme fagocitante). Unico indizio: il messaggio svela dove ho nascosto i cioccolatini! *In alto trovate una tavola di Vigenère.*

Cifra	H	M	U	T	O	A	X	M	I	J	I	K	V	W	X	I	F	G	K	Q

Cifra	T	O	V	K	B	T	D	X	D	V	K	H	V	X	I	T	I	S	G	N

Cifra	V	R	F	P	Y	E	F	G	L	E	O	D	C	D	X	Z	W	E	Q	M

Cifra	R	X	E

Come ultima osservazione, considerate che la tecnica della “parola civetta” potrebbe essere usata anche per rompere un cifrario di Vigenère classico (o modificato per *metasimboli*): da un lato si avrebbe una sola “stringa potenziale” (perché la chiave e il messaggio conterrebbero parole diverse), ma dall’altro la conoscenza di una parte del verme verrebbe amplificata dalla continua ripetizione dello stesso.