Matematica e … crittografia

I legami fra matematica e crittografia sono complessi, ma particolarmente attuali in questa epoca moderna ove codici a barre, codici numerici per bancomat e carte di credito, telefonini cellulari che possono ricevere e inviare messaggi in ogni parte del mondo, hanno dato un enorme sviluppo alla scienza del *nascondere il messaggio* (originale) *scritto* (questa in sostanza l'etimologia della parola crittografia).

Si pensi che risale solo alla fine del secolo scorso (1990), da parte dei matematici Arjen K. Lenstra (Olanda) e Mark S. Manasse (USA) la *fattorizzazione* di un numero di 155 cifre; fattorizzazione che ha messo in pericolo tutte le basi dei moderni sistemi crittografici.

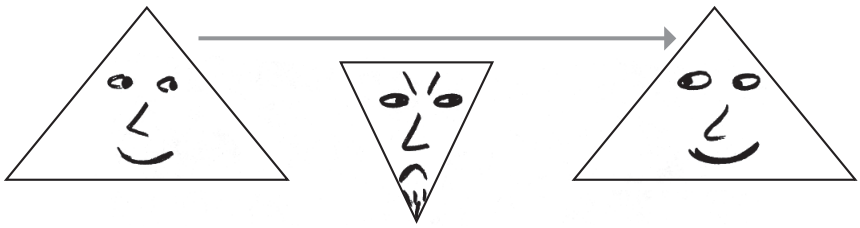
Vi proponiamo attività semplici, relative alla nascita della crittografia:

Crittografia

Da sempre l'uomo ha desiderato di inviare messaggi in modo riservato, cioè in modo che non fossero comprensibili da parte di un'eventuale persona che li intercettasse, ma fossero comprensibili soltanto dal destinatario.

A questo scopo si ricorre ad artifici che vanno sotto il nome di *cifratura* dei messaggi. Chiariamo alcuni termini.

Crittografia significa letteralmente «scrittura segreta». Con questo termine si intende oggi un insieme di tecniche che consentono di trasmettere messaggi mantenendoli segreti a tutti, tranne ad alcune persone che possiedano la chiave per comprenderli. La crittografia può operare su diversi tipi di supporti (testi, immagini, filmati), ma noi ci limiteremo ad alcune semplici tecniche relative ai testi.



- La *cifratura* (sinonimo: *crittazione*) è l'operazione con la quale si nascondono le informazioni; essa viene effettuata tramite un procedimento chiamato *cifrario*.
- Il *testo in chiaro* è il messaggio da cifrare.
- Il *testo cifrato* (sinonimo: *crittogramma*) è il messaggio trasformato in modo da non essere più leggibile tramite una semplice lettura.
- La *decrittazione* è la riconversione di un testo cifrato nella sua forma originaria, cioè nel testo in chiaro.
- Il *cifrario* è il procedimento (algoritmo) che consente di crittare e decrittare i testi.

I cifrari a sostituzione

I più semplici cifrari, e anche i più antichi, sono i cifrari cosiddetti a *sostituzione*: essi consistono nella sostituzione di ciascuna delle 26 lettere che costituiscono il moderno alfabeto con un'altra lettera dello stesso alfabeto.

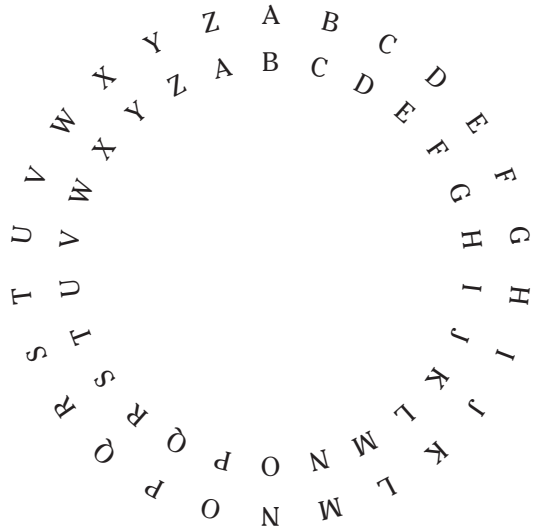
In *termini matematici* si tratta dunque di operare una *permutazione* dell'alfabeto, dove per permutazione s'intende una *funzione* che trasforma l'alfabeto in se stesso facendo corrispondere a ogni lettera un'altra lettera (in generale diversa) e viceversa.

Il cifrario di Cesare Augusto

Il più semplice di tali cifrari è il cosiddetto *cifrario di Cesare Augusto*; esso consiste nel sostituire ad ogni lettera dell'alfabeto la lettera successiva e di sostituire alla Z la A. In forma esplicita:

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
	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|
cifrato	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

la parola CESARE diventa DFTBSF.



Se immaginiamo di disporre in cerchio le 26 lettere dell'alfabeto su due diverse circonferenze, e poi di disporre queste due circonferenze in modo che abbiano lo stesso centro ma siano *ruotate* di un passo una rispetto all'altra, otteniamo un'immagine fisica del cifrario di Cesare Augusto.

Ecco perché questo cifrario viene anche indicato, in forma simbolica, col simbolo ROT 1. L'operazione di decrittazione può essere indicata col simbolo ROT –1, cioè consiste nel sostituire ogni lettera con la sua precedente.

Una notazione curiosa: nel film *2001: Odissea nello spazio* il calcolatore, che è in qualche modo il protagonista, si chiama HAL, nome che si ottiene se si applica a ritroso il cifrario di Cesare (cioè si applica il cifrario ROT –1) alla parola IBM, la ben nota ditta produttrice di calcolatori e computer.

Il cifrario di Giulio Cesare

Del tutto analogo al precedente è il cosiddetto *cifrario di Giulio Cesare*.

Semplicemente adesso ogni lettera viene sostituita con quella che si trova tre passi avanti nell'alfabeto, mentre le ultime tre lettere X, Y, Z vengono sostituite con A, B e C. Possiamo usare per tale cifrario il simbolo ROT 3, in quanto l'alfabeto viene ruotato di tre posizioni.

In forma esplicita:

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

Ad esempio la parola CESARE diventa FHVDUH.

Il cifrario carbonaro

Citiamo ancora un cifrario a sostituzione, il cosiddetto *cifrario carbonaro*; esso consiste nello scambiare tra loro le coppie A/O, B/P, C/G, D/T, E/I, F/V, L/R, M/N S/Z (si tratta di coppie di lettere dal suono simile) mentre si lasciano invariate le restanti lettere dell'alfabeto. In forma esplicita:

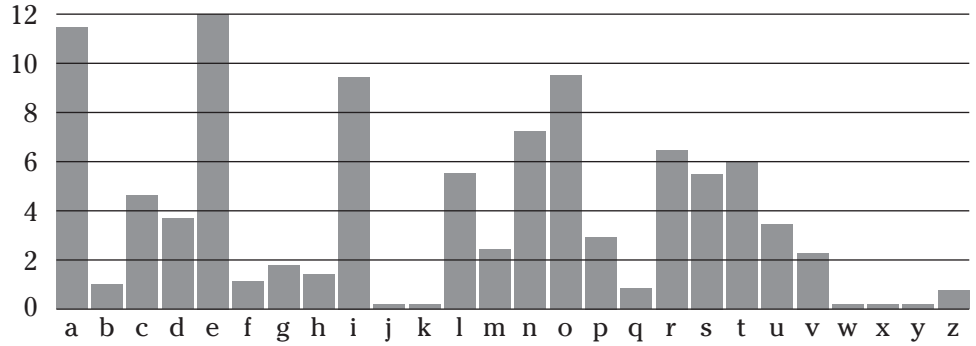
chiaro	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|
cifrato	O	P	G	T	I	V	C	H	E	J	K	R	N	M	A	B	Q	L	Z	D	U	F	W	X	Y	S

Nel cifrario carbonaro il nome CESARE diventa GIZOLI.

Abbiamo già detto che il numero dei cifrari a sostituzione è molto elevato e questo potrebbe far pensare che essi siano molto sicuri. In realtà non è così, almeno se si dispone di messaggi cifrati abbastanza lunghi.

Occorre tener presente che, in ciascuna lingua, la frequenza con cui compaiono le singole lettere dell'alfabeto segue leggi statistiche piuttosto precise e lo stesso vale per i diagrammi (coppie di lettere), i trigrammi (terne di lettere), ecc. Se si dispone di un testo cifrato abbastanza lungo si può farne un'analisi frequenziale e individuare le lettere, i diagrammi, ecc. più frequenti ed abbinarli con quelli di uguale frequenza nella lingua del messaggio in chiaro.

Per esempio nella lingua italiana le lettere più frequenti sono nell'ordine e, a, o, i, n, r, t, l, s, ... L'istogramma mostra ciò in modo sintetico.



Il cifrario di Vigenère

Un'idea per ovviare al pericolo di una troppo facile decifrazione consiste nell'usare a rotazione più cifrari a sostituzione.

Un esempio abbastanza antico al riguardo è il cosiddetto *cifrario di Vigenère*, così chiamato dal nome del diplomatico francese Blaise de Vigenère (1523-1596).

Esso consiste nel costruirsi una tabella (*matrice*) di 26 righe e altrettante colonne; nella prima riga è riportato l'alfabeto e successivamente ciò che si ottiene traslando a sinistra di un passo ciò che è scritto nella riga soprastante. Nella prima colonna della matrice ottenuta leggiamo ancora l'alfabeto nel suo ordine naturale.

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

Il cifrario richiede l'uso di una *parola chiave*. Questa parola chiave viene ripetuta quante volte occorre sopra il testo in chiaro.

La lettera della parola chiave che si trova sopra la lettera del testo in chiaro determina la riga del quadrato di Vigenère da usare per la cifratura.

Ad esempio, se vogliamo cifrare il messaggio «domani piove» usando la chiave «amore» prepareremo questa corrispondenza:

```
a m o r e a m o r e a m o r e
| | | | | | | | | | | |
d o m a n i p i o v e
```

Per cifrare la *d* useremo la riga *a* (è la lettera della chiave che sta scritta sopra), quindi *d* resta *d*, per cifrare la *o* useremo la riga *m* (in quanto *m* è la seconda lettera della chiave), ottenendo *a*, per cifrare la *m* useremo la riga *o*, ottenendo *a*, e così via. In definitiva il messaggio diventa

d a a r r i b w f z e

Chi riceve il messaggio cifrato dovrà avere a disposizione:
– il quadrato di Vigenère
– la parola chiave
e preparerà la corrispondenza inversa

```
d a a r r i b w f z e
| | | | | | | | | | |
a m o r e a m o r e a m o r e
```

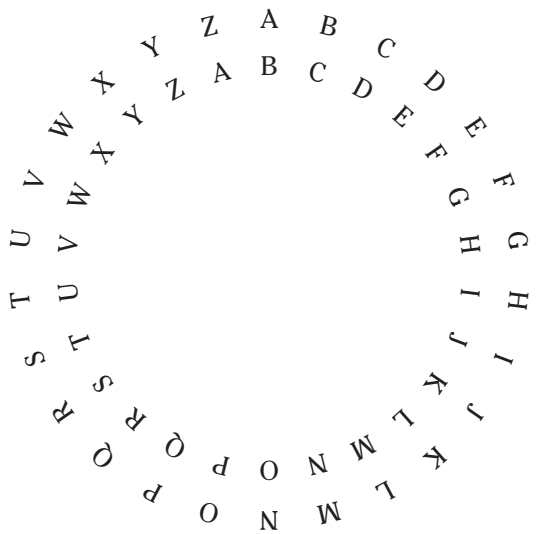
che dovrà interpretare.

Il cifrario di Vigenère è più robusto di quelli che abbiamo descritto in precedenza, tuttavia, usando i moderni calcolatori, può essere attaccato con successo.

I criteri che si usano attualmente per nascondere le informazioni nelle applicazioni militari, nelle transazioni bancarie, ecc., sono basati su tecniche matematiche sofisticate che sfruttano la teoria dei *numeri primi*.

ATTIVITÀ 1 **IL CIFRARIO DI CESARE AUGUSTO**

Questi messaggi sono stati costruiti usando il cifrario di Cesare Augusto (ROT 1).
Il tuo compito è quello di decifrarli.



1. b tfuufousjpof tdpqqjb vob hvfssb

.....

2. jm qsftjefouf tub nbmf

.....

3. bcjubouj ej nbsuf iboop dptusvjup ovpwp wjsvt, buufoajpof

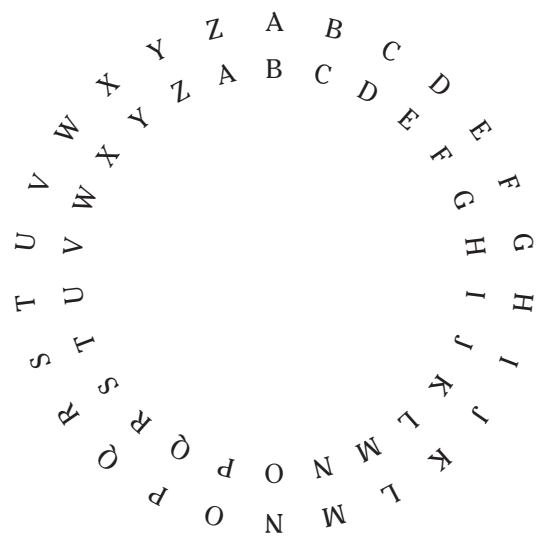
.....

4. ofnjdj iboop dpmqjup btuspobwf; sftubop qpdif psf pttjhfop

.....

ATTIVITÀ 2 **ANCORA IL CIFRARIO DI CESARE AUGUSTO**

Questo messaggio è stato costruito usando il cifrario di Cesare Augusto (ROT 1).
Cerca di decodificarlo.



1. opo ejsf be bmdvop dif njdifmb ib

.....

mbtdjbup hjbooj qfs nfuufstj jotjfnf b nbttjnp

.....

Cerca ora di crittare, sempre con il cifrario di Cesare Augusto, questo messaggio da inviare ai tuoi amici.

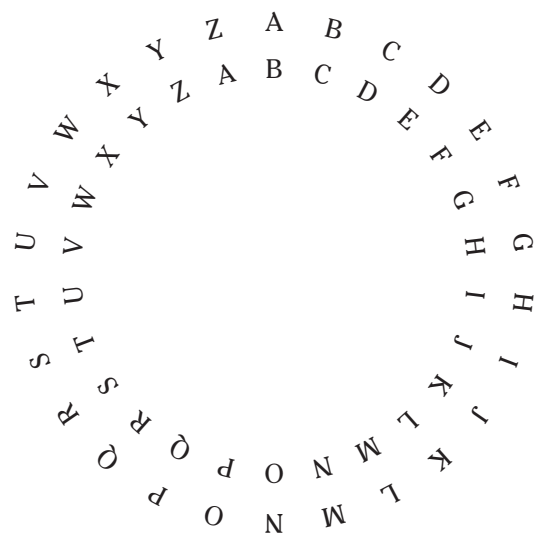
2. La prof di matematica non viene, evviva non si fa lezione

.....

.....

ATTIVITÀ 3 **IL TUO CIFRARIO**

Il cifrario di Cesare Augusto (ROT 1) può essere rappresentato con 2 ruote concentriche o con 2 nastri fra loro paralleli.



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
	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|
cifrato	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

1. Prova a costruire da solo il cifrario ROT 7

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
	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|
cifrato																										

2. Prova a costruire il cifrario ROT 11

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
	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|
cifrato																										

Traduci ora, sia in ROT 7 che in ROT 11 il seguente messaggio.

I fichi sono maturi e vanno raccolti.

3. ROT 7

.....

.....

4. ROT 11

.....

.....

Confronta i tuoi risultati con quelli dei tuoi compagni.

ATTIVITÀ 4 **UNA SPIA IN GUERRA**

I messaggi che seguono sono stati crittati con il cifrario ROT 3.

1. Completa il cifrario.

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
	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|
cifrato																										

Usando il cifrario ROT 3, cerca di crittare le seguenti frasi:

2. Ambasciatore in prigione

.....

3. I soldati sono fuggiti

.....

4. Non dire a Dolores che Piero va in Polonia

.....

Usando il cifrario ROT 3, cerca di decifrare i seguenti messaggi.

5. dood ilqh gho qryhfhqwr sklolsv h vrqb kdqqr lqwurgrwwr lo frpsdfw glvn

.....

.....

6. od gldjrqdoh qrq vl plvxud frq xq udssruwr gl qxphul lqwhul

.....

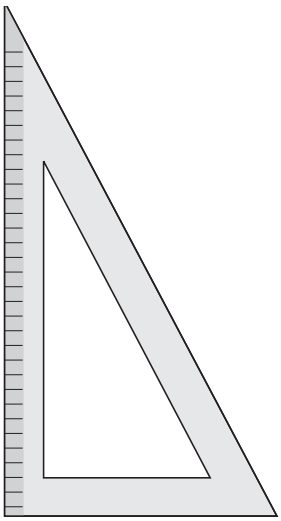
.....

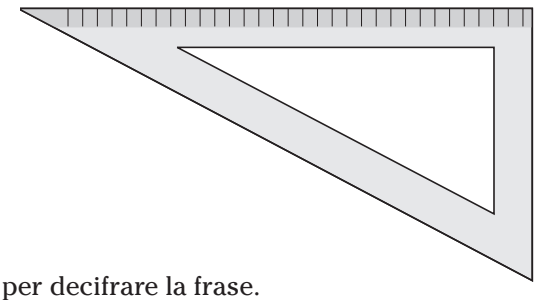
Confronta i tuoi risultati con quelli dei tuoi compagni.

ATTIVITÀ 5 **IL CIFRARIO DI VIGENÈRE**

Dovresti già conoscere il funzionamento del quadrato (o matrice) di Vigenère.
Per crittare o decrittare messaggi possono esserti utili due piccole squadre (vedi figura), costruite con del cartoncino.

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





Usa il cifrario di Vigenère per decifrare la frase.

1. Le rondini volano, usando la parola chiave «uovo»

Usando la parola chiave «palo», sono stati codificati con il quadrato di Vigenère due messaggi. Cerca di decodificarli.

2. x p c w v i z b x e c w h o y c u u r u x t t

.....

.....

3. x c z b u i y w h o y c h t l h x v t c a a e w

.....

SOLUZIONI

ATTIVITÀ 1

1. «A settentrione scoppia una guerra»

2. «Il presidente sta male»

3. «Abitanti di Marte hanno costruito nuovo virus, attenzione»

4. «Nemici hanno colpito astronave; restano poche ore ossigeno»

ATTIVITÀ 2

1. «Non dire ad alcuno che Michela ha lasciato Gianni per mettersi insieme a Massimo»

2. mb qspg ej nbufnbujdb opo wjfof, fwwjwb opo tj gb mfajpof

ATTIVITÀ 3

1.

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

2.

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

3. p mpjop zvuv thabyp l chuuv yhjjvsap

4. t qtnst dzyz xlefct p glyyz clnnzwet

ATTIVITÀ 4

1.

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

2. dpedvfldwruh lq suljlrqh

3. l vrogdwl vrqr ixjjlwl

4. qrq gluh d groruhv fkh slhur yd lq srorqld

5. «Alla fine del novecento Philips e Sony hanno introdotto il compact disk»

6. «La diagonale non si misura con un rapporto di numeri interi»

ATTIVITÀ 5

1. fsmchrdbcjjzubj

2. lprigionierisonofuggiti

3. lconfinisonostativiolati