Can you keep a secret?

Discovering and playing cryptography

Svelare segreti, risolvere enigmi, decifrare codici...
Entro pochi minuti!



CIFRARIO DI CESARE

Il famoso imperatore fece uso della crittografia e il suo sistema era molto semplice.

Prendete l'alfabeto: a, b, c, d, e, f, g, h, i, l...

e associate ad ogni lettera, la lettera che si trova tre posizioni più avanti:

 $A \rightarrow D$

 $B \rightarrow E$

 $C \rightarrow F$

E così via.

Tocca a voi

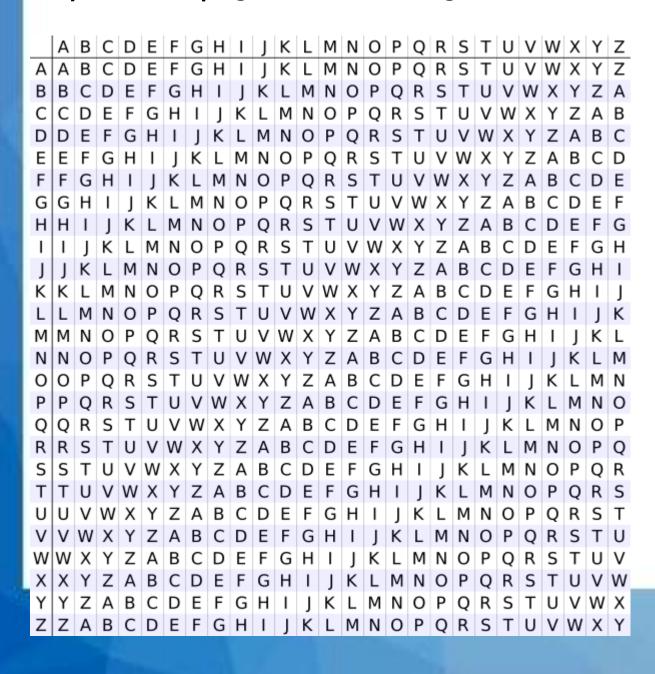
Gruppo 1: GRPDQNDZZDFFMNDPRODLD OOND

Gruppo 2:
NOGDGRHZUDZZRVAOUAENR
QH

Minuti a disposizione

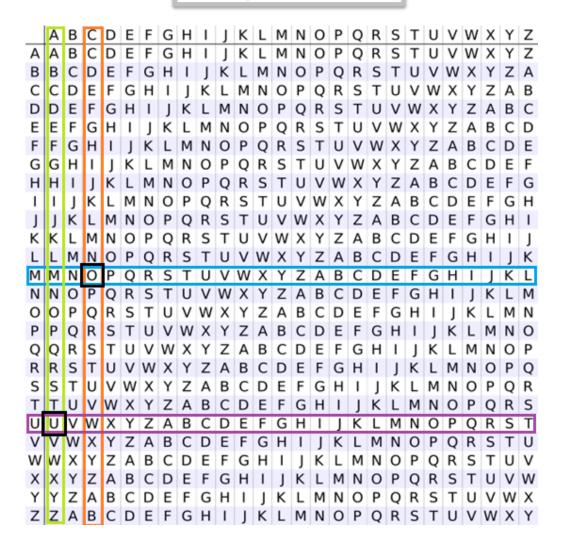
CIFRARIO DI VIGÈNERE

Una crittatura tanto semplice da applicare quanto inespugnabile, senza la giusta chiave...



CIFRARIO DI VIGNÈRE

Esempio: CIFRARE



Parola in chiaro «CAMALEONTE»

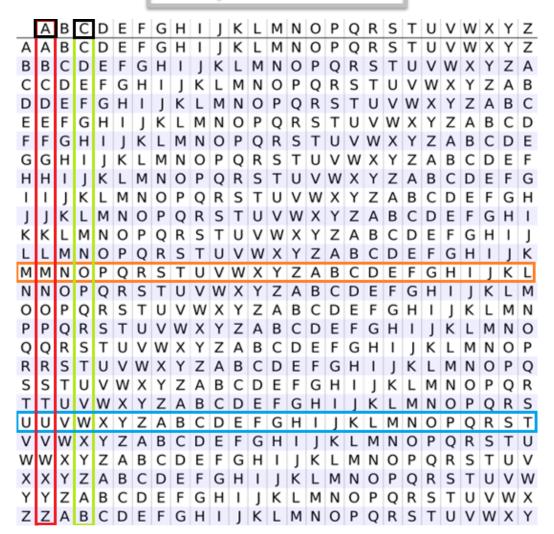
«C»: Si interseca la prima colonna contenente «C» con la prima riga contenente «M»

«A»: Si interseca la prima colonna contenente «A» con la prima riga contenente «U»

Parola cifrata «OUEEXYFRFY»

CIFRARIO DI VIGÈNERE

Esempio: DECIFRARE



Parola cifrata «OUEEXYFRFY»

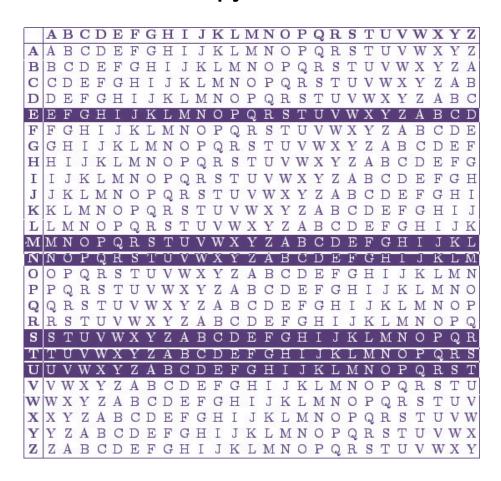
«O»: Sulla prima riga contenente «M» si individua «O» e si risale la colonna «U»: Sulla prima riga contenente «U» si individua «U» e si risale la colonna

•••

Chiave: MUSETN

Messaggio crittato:

xueemryulmvnqfsvmrpcvekrxikxxfeifsfrmwgwxq upyvlr

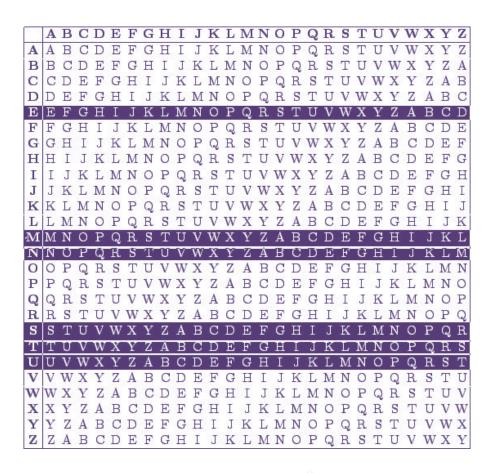


Minuti a disposizione

Chiave: MUSETN

Messaggio crittato:

ugsxxzmnagbazmwkgnziulxbshatkbnfwqtumofelb xormhaq



Minuti a disposizione

STUDIO DELLE FREQUENZE

Per crittare il messaggio è necessario creare un alfabeto permutando le lettere dell'alfabeto italiano e semplicemente rimpiazzare.

Α	В	C	D	Е	ш	G	I	_	_	M
L	ı	U	Т	R	E	Q	Α	S	D	F

0	N	P	Q	R	S	T	U	٧	Z
G	В	С	Z	N	М	0	Р	Н	٧

Esempio

Parola in chiaro
«FENICOTTERO»

Sostituendo lettera a
lettera, parola cifrata
«ERBSUGOORNG»

Più il testo da cifrare è lungo, più semplice sarà la decifratura

qn sb trztnzsgb n pchgub trz hssnzdbrzn, scssr qb tmbhgbqtn uh qn. bz acnqsr pghzun frzur zrz t'n znqqczr tmn fb sghssb trz shzsh pnzsbonddh, h vhgsn oh fhsnfhsbth

Lettera crittata	h	t	Z	S
Lettera in chiaro	Α	С	N	T

Minuti a disposizione

oh fhsnfhsbth vcr nqqngn unebzbsh trfn oh qtbnzdh bz tcb zrz qhvvbhfr fhb ub tmn trqh qsbhfr vhgohzur, zn qn tbr tmn ubtbhfr n ingr.

Lettera crittata	h	t	z	S
Lettera in chiaro	A	С	N	Т

Minuti a disposizione

14 18 - 13 10 19 19 18 - 7 8 19 19 10 - 12 19 8 - 1 8 11 11 17 10 19 18 - 1 18 16 - 14 8 **- 4 8 15 18 4 8 17 5 8. 13 17 20 17 13 10** 19 10 - 14 8 - 14 10 16 10 - 18 15 8 - 8 **- 4 18 15 8, - 16 8 13 13 10 1 1 17 8 19 10 - 17 14 - 1 16 18 6 6 10- 13 18 17 - 14 10** 16 10 - 8 2 17 15 17 - 18 - 8 9 9 17 12 19 9 10 19 10 - 11 18 4 1 16 18 - 8 14 4 18 19 10 - 5 17 19 3 12 18 - 8 19 19 17 - 8 14 14' - 18 15 8 - 13 18 14 14 8 - 14 10 16 10 **- 4 17 9 14 17 10 16 18 - 8 4 17 5 8.**

Minuti a disposizione

19 10 19 - 11 10 19 10 - 2 16 8 20 8 - 17 19 - 4 8 15 18 4 8 15 17 5 8 . - 7 10 - 17 4 1 8 16 8 15 10 - 8 13 - 8 5 5 18 15 15 8 16 18 - 17 14 - 21 8 15 15 10 - 11 17 19 -13 8 - 1 17 5 5 10 14 8. - 3 12 8 19 13 10 **– 17 14 – 4 17 10 – 17 19 11 18 9 198 19 15** 18 - 4 17 - 1 8 11 11 8 20 8 - 17 14 - 15 18 11 15, - 4 17 - 14 17 4 17 15 8 20 10 - 8 -11 5 16 17 20 18 16 18:- " 11 1 10 11 18 16 10 **- 3 12 8 14 5 10 19 10 - 17 19 - 9 16 8 13 10 - 13 17 - 16 17 11 10 14 20 18 16 14** 10".

Minuti a disposizione

SISTEMA T9

1	2	3	
ABC	DEF	GHI	
4	5	6	
JKL	MNO	PQRS	
7	8	9	
TUV	WXYZ	.,!?	

Ad ogni tasto sono associate più lettere: «2222» può essere «FEDE» oppure «EFFE»

Sarete più veloci del vostro T9 nel riconoscere la parola desiderata allo scrivente?

Tocca a voi

Gruppo 1:

555 1262 765665 1476352573 21613 3 575263

Gruppo 2:

652773 23 1262 62 272 637 272 555 21 637 6717765

Minuti a disposizione