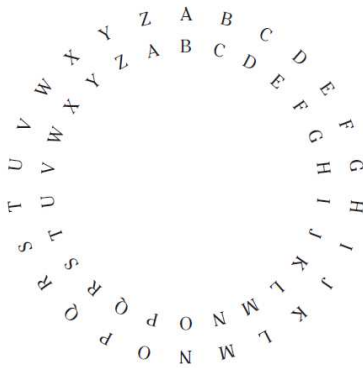


LABORATORIO 1

- Utilizza il cifrario di Cesare, con rotazione 4, per cifrare il seguente messaggio:
Domani i nemici attaccheranno a ovest



- Utilizza il cifrario di Cesare, con rotazione 3 per decifrare il seguente messaggio
DPR OD PDZHPDZNF
- Utilizza il cifrario di Vigenère per decifrare la frase: “I confini sono stati violati” con la parola chiave LUNA

	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	Italiano	Frequenza
a	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	E	11.79
b	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	A	11.74
c	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	I	11.28
d	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	O	9.83
e	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	N	6.88
f	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	L	6.51
g	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	R	6.37
h	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	T	5.62
i	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	S	4.98
j	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	C	4.50
k	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	D	3.73
l	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	P	3.05
m	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	U	3.01
n	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	M	2.51
o	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	V	2.10
p	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	G	1.64
q	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	H	1.54
r	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	F	0.95
s	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	B	0.92
t	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	Q	0.51
u	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	Z	0.49
v	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	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	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	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	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		

- Scrivi un testo di dieci parole e codificalo con il metodo di Vigenere, utilizzando come parola chiave il nome di una città italiana di quattro lettere. Passa poi il messaggio cifrato al gruppo di lavoro che ti viene indicato e cerca di decrittare il testo che riceverai da un altro gruppo di lavoro.

Soluzioni esercizi laboratorio 1

1. HSQERO O RIQOGO EAAEGGNIVERRS E SCIZA

2. Amo la matematica

3. TWBNQCAIDIAODNNTTPVOWUGI

4. Non è possibile fornire una soluzione. Si possono dare alcune indicazioni sul ruolo della tabella delle frequenze e sul fatto che è chiaro che il modo di procedere è molto falsato perché si sta facendo l'analisi di un testo troppo breve, ma l'importante è sottolineare come le tante possibilità teoriche possano essere notevolmente ridotte usando informazioni sul linguaggio e procedendo sistematicamente "per tentativi." ESEMPIO: poiché nella lingua italiana la maggior parte delle parole termina con una delle vocali *a, e, i, o* vorrà dire che le lettere finali delle parole del messaggio cifrato dovranno essere una di queste lettere. Se nel testo ci sono lettere consecutive identiche queste necessariamente devono essere consonanti. Intuita una parola si può procedere cercando "un significato" della frase.