CRITTOGRAFIA

La crittografia è un tipo speciale di scrittura segreta decifrabile esclusivamente da chi sia a conoscenza di un codice. Essa può venire utilizzata per inviare dei messaggi "segreti"; i suoi elementi principali sono:

TESTO IN CHIARO = il messaggio che vogliamo trasmettere

ALGORITMO DI TRASFORMAZIONE= la serie di operazioni che svolgiamo per rendere segreto il nostro messaggio

TESTO CIFRATO= il messaggio "incomprensibile"

CHIAVE DI CIFRATURA= parametro che ci permette di decifrare il testo

Sin dall'antichità l'uomo ha utilizzato diversi metodi per "nascondere" i propri messaggi. Nel 400 A.C. gli Spartani utilizzavano la **SCITALA** ossia un piccolo bastoncino attorno a cui veniva arrotolato una striscia di pelle contenente il messaggio. Una volta srotolata la striscia di pelle dalla scitala era impossibile decifrare il messaggio. La chiave del sistema consisteva nel diametro della scitala, la decifrazione era possibile solo se si era in possesso di una bacchetta identica a quella del mittente.

Un altro sistema di crittografia molto famoso nell'antichità è il **CIFRARIO** utilizzato da Giulio Cesare. Il generale romano, nei propri messaggi, sostituiva le lettere del testo in chiaro con altre lettere che si trovavano ad un certo numero di posizioni dopo nell'alfabeto.

ESEMPIO:

Cesare usava una chiave di 3 ossia sostituiva una lettera con un'altra posizionata tre posizioni dopo. Ad esempio una A veniva trasformata in D. Ecco lo schema completo:

The Caesar cipher 	A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z
	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	v	z	a	b	c

Questi tipi di cifrari sono detti anche **cifrari a sostituzione** o **cifrari a scorrimento** a causa del loro modo di operare: la sostituzione avviene lettera per lettera, scorrendo il testo dall'inizio alla fine. Non vengono inseriti né spazi, né segni di punteggiatura.

Nello schema che hai appena visto mancano le lettere straniere (JKWXY). Prova tu a creare una versione del cifrario con esse:

A																							
D																							

ESERCIZI:

Traduci le seguenti frasi utilizzando il cifrario che hai appena creato.

DWWDFFKHUHPRLOQHPLFRGRPDWWLQD

JOLDOXQQLVLUHFDQRDVFXROD

LOVROHVSOHQGHVXOODFROOLQD

LE NAVI SALPANO DAL PORTO

IL GUERRIERO REGGE LO SCUDO
