PCTO Liceo Bertrand Russell di Roma

Incontro 1 - Numeri, codici e crittografia

Analizzeremo alcuni metodi per codificare e cifrare utilizzati nel corso della storia, prestando particolare attenzione all'impianto matematico che ne consente la realizzazione.
I metodi per codificare e cifrare sono utili per trasmettere in modo sicuro le comunicazioni, attraverso canali di trasmissione che possono essere disturbati e\o intercettati.
A grandi linee, la struttura è la seguente:

il mittente individua un messaggio (detto **messaggio in chiaro**) che vuole trasmettere ad un certo destinatario

↓

il mittente individua un canale per la trasmissione e una modalità di 'codifica' dei dati, in modo che i dati codificati possano essere trasmessi attraverso il canale scelto.
Dopo la codifica, il messaggio viene detto **messaggio cifrato**.

↓

avviene la trasmissione

↓

il destinatario (eventualmente tramite un dispositivo) decodifica il messaggio cifrato e legge il messaggio in chiaro

Primo esempio: la scacchiera di Polibio

Nel libro X delle Storie (circa 200-118 a. C.), Polibio attribuisce ai suoi contemporanei Cleoxeno e Democleito l'introduzione di un sistema di telecomunicazione (telegrafo ottico trasmesso con due gruppi di 5 torce, un gruppo gestito con la mano destra e uno con la mano sinistra). In tale sistema, le lettere dell'alfabeto venivano inserite in una tabella quadrata con cinque righe e cinque colonne; ogni lettera veniva codificata dalla coppia di numeri corrispondenti alla riga e alla colonna.
Adattando il sistema all'alfabeto italiano, con l'aggiunta di alcuni segni di interpunzione, possiamo utilizzare la tabella 1 per codificare delle frasi.

Esercizio 1 Considera la scacchiera di Polibio in tabella 1. Nella griglia seguente, scrivi una parola (in chiaro) nella prima riga, inserendo una lettera per casella.
Nella seconda riga, cifra il messaggio, utilizzando la scacchiera, riportando la cifratura sotto ciascuna lettera in chiaro.

a	b	c	d	e
f	g	h	i	l
m	n	o	p	q
r	s	t	u	v
z	.	,	:	?

tabella 1

Esercizio 2 Completa la scacchiera seguente, inserendo l'alfabeto in modo diverso rispetto alla scacchiera nella tabella 1.

Ora considera la griglia seguente. Nella prima riga, scrivi lo stesso messaggio che avevi introdotto nell'esercizio precedente. Nella seconda riga, cifra il messaggio, utilizzando la nuova scacchiera.

Esercizio 3 La prima riga della griglia seguente contiene il testo originario (in chiaro) di un messaggio. La seconda riga contiene il testo cifrato tramite una scacchiera.

n	e	l	m	e	z	z	o	d	e	l	c	a	m	m	i	n
44	23	42	43	23	51	51	45	24	23	42	34	32	43	43	41	44

Riesci a ricostruire la scacchiera utilizzata per cifrare? Inserisci nella seguente scacchiera vuota tutte le lettere di cui conosci la posizione.

Secondo esempio: Sistema crittografico di Cesare

La notizia è stata tramandata da Svetonio, uno storico del II sec d.C. Nella sua Vita dei Cesari parla di un sistema utilizzato da Cesare per cifrare i suoi messaggi: egli spostava di tre lettere ogni lettera del messaggio da inviare.

Se indichiamo con lettere minuscole le 21 lettere dell'alfabeto, ciascuna lettera del nostro messaggio (**testo in chiaro**) sarà sostituita con la lettera che si trova tre posizioni più avanti, e che per comodità indicheremo con caratteri maiuscoli, ottenendo così un nuovo messaggio (**testo cifrato**) apparentemente privo di significato

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

Per esempio, se il messaggio da inviare è il seguente:

torno domani

il risultato dopo la cifratura sarà:

ZRUQR GRPDQN

Possiamo decidere di generalizzare questo sistema decidendo di spostare le lettere non di tre posizioni ma di una quantità arbitraria:

Definizione Un sistema di questo tipo, in cui ogni lettera del testo cifrato è ottenuta da una lettera del testo in chiaro spostando di un certo numero k di posizioni le lettere, prende il nome di **cifrario di Cesare** o di **cifratura per traslazione**.

Il numero k di posizioni di cui spostare le lettere è una informazione aggiuntiva che permette di realizzare concretamente il metodo: il numero k viene detto **chiave di cifratura (o chiave cifrante)**.

Come si decifra? La chiave per decifrare si ricava in modo immediato dalla chiave per cifrare: basta spostarsi della stessa quantità di posizioni, ma nella direzione opposta.

Ad esempio, per decifrare il cifrario di Cesare con chiave k =3 possiamo

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

Esercizio 1 Prepara l'alfabeto cifrante (in lettere maiuscole), spostando di 7 lettere aiutandoti con la griglia. Il numero 7 è la chiave cifrante.

a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	v	z

Cifra il seguente messaggio, utilizzando l'alfabeto preparato.

v	i	e	n	i		a	l		m	a	r	e	?						

Esercizio 2 A partire dalla chiave cifrante 9, ricava la chiave per decifrare. Aiutandoti con la griglia dell'alfabeto, decifra il messaggio nella griglia successivo e trascrivilo.

La chiave per decifrare è ……

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

O	A	V	L	Z	T		B	T	A	H	P								