CIFRARIO DI CESARE

Area di Matematica usata: Algebra

Storia e Descrizione

Tale cifrario prende il nome da Giulio Cesare che lo utilizzava, nel corso delle sue numerose campagne di guerra, per corrispondere con i suoi luogotenenti ed evitare che gli ordini venissero intercettati e soprattutto capiti dai suoi nemici.
Lo storico Svetonio racconta nella "Vita dei Dodici Cesari" che Giulio Cesare talvolta criptava i messaggi traducendoli semplicemente in greco, altre volte permutava le lettere secondo uno schema fisso prestabilito. Il testo veniva cifrato spostando ogni lettera dell'alfabeto di 3 passi in avanti. La decifratura avveniva semplicemente usando il procedimento inverso: tornare Indietro di 3 lettere. Nella realta, Cesare e suoi luogotenenti non conoscevano le cifre arabe 1,2,3,…, dunque, usavano una tabella circolare formata da un anello con due cerchi concentrici; nel primo ci sono, in elenco, tutte le lettere dell'alfabeto latino e nel secondo l'alfabeto spostato in base al passo di cifratura.

E' un cifrario a sostituzione monoalfabetica, in cui cioe si cifra lettera per lettera.
Nello specifico, per cifrare un messaggio, ogni lettera del testo in chiaro e sostituita nel testo cifrato con una che si trova un certo numero fisso di posizioni dopo nell'alfabeto.
Il numero di posizioni di cui si traslano le lettere e detta chiave di codifica.
Ad esempio Cesare usava uno spostamento di 3 posizioni, secondo il seguente schema:

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

Formalizzazione matematica:

La base matematica del cifrario di Cesare e l'aritmetica modulare.
Rappresentiamo le 26 lettere dell'alfabeto latino con i numeri: A diventerebbe 1, B diventerebbe 2, e cosi via fino a Z che diventerebbe 26.
A questo punto, nel caso di Cesare, la codifica sarà data dalla funzione f che ad ogni numero x tra 1 e 26 associa l'intero:

$$f(x) \equiv x + 3 \ (mod\ 26), \quad 1 \le f(x) \le 26$$

e dunque ha chiave 3, mentre la decodifica si ottiene tramite la funzione inversa f' che ad ogni x associa:

$$f'(x) \equiv x - 3 \ (mod\ 26), \quad 1 \le f'(x) \le 26$$

con chiave -3.

La chiave può essere sostituita con un generico bε $\boldsymbol{Z}$.