

Il cifrario di Augusto

1

Riccardo Paparelli

Come nasce?

2

- Lo scrittore Robert Graves, grande studioso di storia romana e autore di una finta autobiografia dell'imperatore Claudio, sostiene che Augusto usava accanto al semplice codice di Cesare, un cifrario riservato più sicuro per le comunicazioni più delicate; sarebbe stato lo stesso Claudio a comprenderne il funzionamento dopo aver studiato le carte di Augusto.



Come funziona?

3

- Il metodo usa come **chiave** i primi cento versi del I libro dell'Iliade;
- il testo chiaro e il brano dell'Iliade vengono scritti in parallelo;
- la chiave e il testo avevano un corrispettivo numerico;
- ogni lettera del chiaro viene confrontata con la corrispondente dell'Iliade, si calcola la differenza tra i due caratteri e la sequenza dei numeri così calcolati costituisce il messaggio cifrato.

La cifratura

4

- Ogni lettera del chiaro viene confrontata con la corrispondente dell'Iliade, si calcola la differenza tra i due caratteri e la sequenza dei numeri così calcolati costituisce il messaggio cifrato.

chiave: N E L M E Z Z O D E L C A M M I N O S T R A V I

chiaro: I N V I A R E R I N F O R Z I D O M A T T I N A

differenza: 5 17 16 4 4 8 21 23 21 17 6 12 9 13 4 5 25 2 18 26 24 18 8 8

Infatti I è la 9^a lettera, N la 14^a, e $14 - 9 = 5$; N è 14^a, E 5^a quindi $(26 +)5 - 14 = 17$; ecc.ecc.

Il messaggio cifrato sarà quindi:

5 17 16 4 4 8 21 23 21 17 6 12 9 13 4 5 25 2 18 26 24 18 8 8

E Q P D D H U W U Q F L I M D E Y B R Z X R H H

(aritmetica modulo 26, usando il 26 al posto dello 0)

La decifrazione

5

- Ogni lettera del chiaro viene confrontata con la corrispondente dell'Iliade, si calcola la somma tra i due caratteri e la sequenza dei numeri così calcolati costituisce il messaggio cifrato.

Per decifrare il testo basterà compiere il processo inverso (sommare invece di sottrarre):

cifrato: 5 17 16 4 4 8 21 23 21 17 6 12 9 13 4 5 25 2 18 6 9

chiave: NELMEZZODELCAMMINOSTR

chiaro: INVIARERINFORZIDOMANI

Esempio

6

Testo in chiaro:

"Le nostre truppe in Polonia sono in rotta"

Chiave:

L'inizio dell'Inferno di Dante

CHIARO	l	e	n	o	s	t	r	e	t	r	u	p	p	e	i	n	p
CHIAVE	n	e	l	m	e	z	z	o	d	e	l	c	a	m	m	i	n
Sposta:	14	5	12	13	5	26	26	15	4	5	12	3	1	13	13	9	14
CIFRATO	Z	J	Z	B	X	P	O	T	X	W	G	S	Q	R	V	W	D

CHIARO	o	l	o	n	i	a	s	o	n	o	i	n	r	o	t	t	a
CHIAVE	d	i	n	o	s	t	r	a	v	i	t	a	m	i	r	i	t
Sposta:	4	9	14	15	19	20	18	1	22	9	20	1	13	9	18	9	20
CIFRATO	S	U	C	C	A	U	K	P	J	X	C	O	E	X	L	C	U

- <http://ricerca.mat.uniroma3.it/users/merola/critto09/seminari/Storia1.pdf>
- http://www.danielepalladino.it/downloads/uni/slide_storia.della.crittografia.pdf
- <http://www.crittologia.eu/critto/augusto.htm>