

## ESERCIZIO 28/08/2024

Messaggio cifrato(cyphertext) : "HSNFRGH"

Per cifrare il plaintext è stato utilizzato il Cifrario di Cesare.

Dato un alfabeto di N caratteri e scelta una chiave k, la funzione di cifratura è data da:  
 $y = x + k \pmod{N}$ .

La funzione di decifratura è  $x = y - k \pmod{N}$ .

È stata scelta una chiave  $k=3$  per cifrare il messaggio e quindi ogni carattere y del messaggio cifrato è  $y = x + 3 \pmod{26}$ .

Per risalire al plaintext si effettua l'operazione inversa quindi  $x = y - 3 \pmod{26}$

|   |       |   |   |
|---|-------|---|---|
| H | ----- | > | E |
| S | ----- | > | P |
| N | ----- | > | I |
| F | ----- | > | C |
| R | ----- | > | O |
| G | ----- | > | D |
| H | ----- | > | E |

Il plaintext è EPICODE.