

## Esercizio per la pratica della Unit 1 - S3 - L4

Svolto da Gioele Parla

Dato un messaggio cifrato cercare di trovare il testo in chiaro,

**OBIETTIVO:** Decrittazione dei seguenti messaggi:

- HSNFRGH
- QWJhIHZ6b2VidHl2bmdyIHB1ciB6ciBhciBuchBiZXRi

Analizzando il primo messaggio possiamo provare a decifrarlo tramite il cifrario di Cesare, proviamo con uno spostamento di 3 lettere così da avere questo risultato:

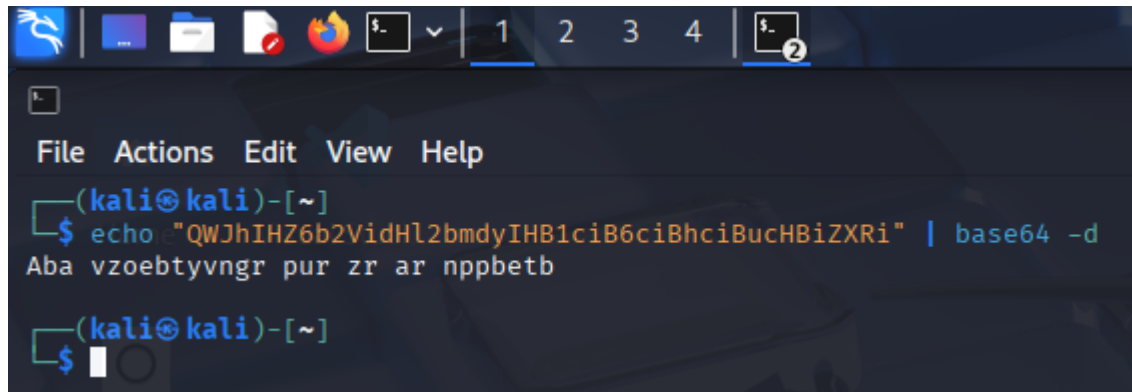
Andando indietro di 3 lettere dell'alfabeto italiano per ogni lettera di **"HSNFRGH"** otterremo la parola **"EPICODE"**.

Per il secondo esercizio abbiamo il messaggio:

**"QWJhIHZ6b2VidHl2bmdyIHB1ciB6ciBhciBuchBiZXRi"**

questo testo lo abbiamo in formato base64 che al contrario del base58 può contenere caratteri speciali come "/" o "+" e maiuscole.

Usando il comando **base64 -d** sul terminale linux decodifichiamo il messaggio e otterremo un messaggio che possiamo ipotizzare sia a sua volta da decifrare con il cifrario di Cesare.



```
(kali㉿kali)-[~]  
$ echo "QWJhIHZ6b2VidHl2bmdyIHB1ciB6ciBhciBuchBiZXRi" | base64 -d  
Aba vzoebtyvngr pur zr ar nppbetb  
  
(kali㉿kali)-[~]  
$
```

Il seguente messaggio: **"Aba vzoebtyvngr pur zr ar nppbetb"** dovremmo effettuare varie prove di quante lettere dobbiamo effettuare lo spostamento del cifrario di cesare, dopo varie prove e fermanoci con uno spostamento di 13 caratteri (ROT13) utilizzando l'alfabeto **internazionale** avremo infine il messaggio: **"Non imbrogliate che me ne accorgo"**.