

ESERCIZIO S3 L4



Esercizio
Esercizio

Esercizio di oggi: Crittografia.

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

Messaggio cifrato: "HSNFRGH"

Secondo esercizio

QWJhHZ6b2VidHI2bmdyIHb1ciB6ciBhciBucHBiZX Ri

Buon divertimento

PRIMO ESERCIZIO

Messaggio cifrato : HSNFRGH

Obiettivo : **Trovare il messaggio originale in chiaro.**

RISPOSTA

Ho ipotizzato che fosse un messaggio cifrato con il **cifrario di Cesare**, ovvero una cifratura che consiste nello spostare ogni lettera dell'alfabeto di un certo numero fisso di posizioni.

Procedimento per decifrare il messaggio :

Ho eseguito una prova con spostamento (**shift**) di 3 e lo ho applicato a tutto il messaggio

H >>> E R >>> O

S >>> P G >>> D = il risultato è EPICODE

N >>> I H >>> E

F >>> C

SECONDO ESERCIZIO

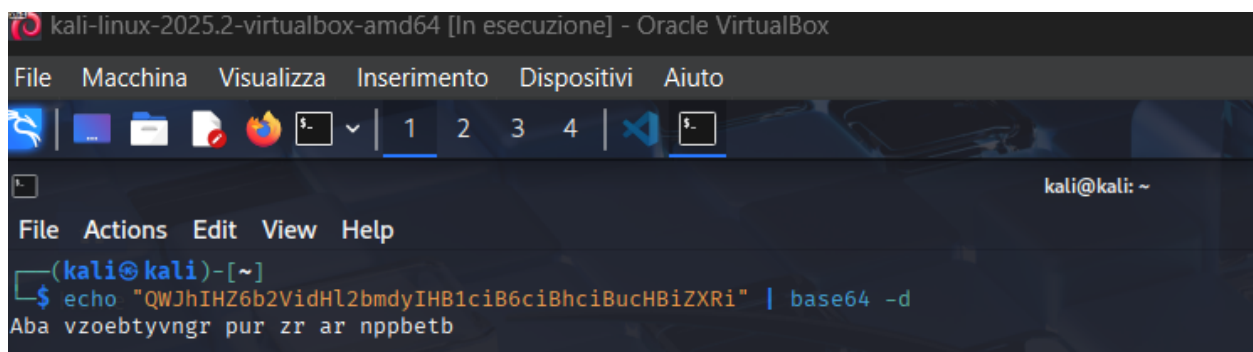
Messaggio cifrato : QWJhIHZ6b2VidHl2bmdyIHB1ciB6ciBhciBucHBiZX Ri

Obiettivo : Trovare il messaggio originale in chiaro.

RISPOSTA

Identifico la **Base64** grazie alla forma del messaggio : caratteri maiuscoli e minuscoli mescolati e numeri senza spazi, con lettere appartenenti al tipico alfabeto **Base64** (A-Z, a-z, 0-9).

Proseguo utilizzando il terminale di Linux :



```
kali-linux-2025.2-virtualbox-amd64 [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
[Icons] | 1 2 3 4 | [Icons]
kali@kali: ~
File  Actions  Edit  View  Help
(kali@kali)-[~]
$ echo "QWJhIHZ6b2VidHl2bmdyIHB1ciB6ciBhciBucHBiZX Ri" | base64 -d
Aba vzoebtyvngr pur zr ar nppbetb
```

Ottenendo il risultato : “Aba vzoebtyvngr pur zr ar nppbetb” , mi rendo conto che la decodifica non è completa. Perciò decido di utilizzare il **cifrario di Cesare** per ottenere il messaggio in chiaro.

Logica utilizzata: Ho iniziato cercando di interpretare le parole più brevi, partendo da **Aba, pur, zr, ar** .

Tra le varie ipotesi ho pensato che **Aba** potesse corrispondere a “**Non**” (essendo una parola breve con la struttura **consonante-vocale-consonante**), e da lì ho continuato a ipotizzare e testare altre sostituzioni allo stesso modo per **pur, zr** ed **ar**.

Questo ha portato a sospettare un **cifrario di Cesare** con **shift di 13**, che alla fine ha confermato le intuizioni, ottenendo il messaggio in chiaro :

“**Non imbrogliate che me ne accorgo**”.

