S3 – L4

1) Primo esercizio - Crittografia

HSNFRGH (Cifrario di Cesare, salto di 3)

Nel Cifrario di Cesare, spostamento di 3, sappiamo che ogni lettera viene spostata di **3 posizioni** nell'alfabeto.

Per **decifrare**, facciamo lo spostamento **all'indietro di 3**:

Cifrato	→	**Plaintext**
H	→	E
S	→	P
N	→	K
F	→	C
R	→	O
G	→	D
H	→	E

Risultato:

HSNFRGH = **EPKCODE**

È abbastanza chiaro che il messaggio vuole essere **EPICODE**, ma nel cifrato è stata sbagliata una lettera (**N al posto di L**), quindi esce **EPKCODE** invece di **EPICODE**.

Se il cifrato fosse stato HSLFRGH, la decodifica con -3 sarebbe esattamente **EPICODE**.

2) Secondo esercizio - Crittografia

QWJhIHZ6b2VidHl2bmdyIHB1ciB6ciBhciBucHBiZXRi

Qui l’idea è ragionare come se avessimo davanti un token di sessione: una stringa strana, con caratteri maiuscoli/minuscoli e senza spazi. Proviamo con dei tentativi.

1) Primo tentativo: decodifica Base64

Base64 decode → "Aba vzoebtyvngr pur zr ar nppbetb"

Su Kali Linux posso **provare a decodificare la stringa come Base64** con il comando:

echo "QWJhIHZ6b2VidHl2bmdyIHB1ciB6ciBhciBucHBiZXRi" | **base64** -d

---

Su Python:

python3 - << 'EOF'

import codecs

s = "Aba vzoebtyvngr pur zr ar nppbetb"

print(codecs.decode(s, "rot_13"))

EOF

2) Secondo tentativo: Struttura a più livelli (come un token complesso)

L’esercizio simula bene la logica di analisi di un token di sessione o di una stringa misteriosa:

1. Riconosco il formato (**Base64**) solo guardando la forma della stringa.
2. Decodifico il primo livello e ottengo un secondo testo cifrato.
3. Provo un secondo metodo (**ROT13** / **cifrario di Cesare con salto 13**).
4. Ottengo il messaggio finale in chiaro.

Risposta finale esercizio 2

Il messaggio cifrato:

`QWJhIHZ6b2VidHl2bmdyIHB1ciB6ciBhciBucHBiZXRi`

è stato decifrato in due passi**:**

1. **Decodifica Base64 →** `Aba vzoebtyvngr pur zr ar nppbetb`
2. **Applicazione ROT13 (cifrario di Cesare con salto 13)**
   Non imbrogliate che me ne accorgo

Questa volta il messaggio è perfettamente chiaro ed è in italiano.