

## PRATICA S3/L4:

### 1. Esercizio di Crittografia:

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

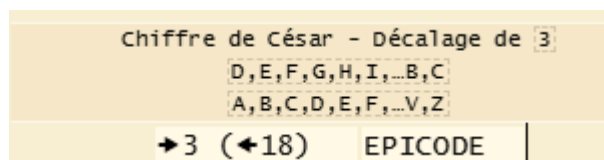
- Messaggio cifrato: "HSNFRGH":

- "HSNFRGH" è stato cifrato con il **Cifrario di Cesare (ROT)**:

- Cifrario a sostituzione: Ogni lettera del messaggio viene spostata avanti o indietro di un certo numero di posizioni nell'alfabeto (in questo caso alfabeto italiano).
- Perché si intuisce: È tipico dei cifrari classici (non moderni come AES, RSA, ecc.) utilizzare maiuscole, nessuno spazio o punteggiature. I cifrari moderni producono testo binario o codificato in Base64, non lettere leggibili.
- ROT 3: spostamento in avanti di 3
- Prima prova: ho utilizzato il terminale di kali per decodificarlo

```
(kali@kali)-[~]  
$ echo "HSNFRGH" | tr "A-Z" "X-ZA-W"  
EPKCODE
```

- Seconda prova: si nota che il risultato è "EPKCODE" e intuisco che è stato utilizzato l'alfabeto italiano. Per provare che la mia intuizione fosse vera ho utilizzato il sito <https://www.dcode.fr/chiffre-cesar>, che conferma il risultato "EPICODE"



- Messaggio cifrato:

"QWJhIHZ6b2VidHl2bmdyIHB1ciB6ciBhciBucHBiZX Ri"

- È codificato in **base64**:

- Base64: serve per rappresentare dati binari (come file o testo cifrato) in un formato leggibile usando solo caratteri ASCII.
- Prima prova: ho usato il terminale di kali per decodificarlo da base64.

```
(kali@kali)-[~]  
$ echo "QWJhIHZ6b2VidHl2bmdyIHB1ciB6ciBhciBucHBiZX Ri" | base64 -d  
Aba vzoebtyvng r pur zr ar nppbetb
```

- Seconda prova: ho notato che il risultato mi portasse un tipo di cifratura ROT; quindi, con il terminale ho provato a decifrarlo in

## ROT13.

```
(kali@kali)-[~]
└─$ echo "Aba vzoebtyvngrr pur zr ar nppbetb" | tr "A-Za-z" "N-ZA-Mn-za-m"
Non imbrogliate che me ne accorgo
(kali@kali)-[~]
└─$
```

### 1. Criptazione e Firmatura con OpenSSL e Python:

- **Installazione di OpenSSL:**

- Da terminale di kali inserire i seguenti comandi:

- sudo apt update
- sudo apt install openssl

```
kali@kali: ~
File Actions Edit View Help
└─$ sudo apt update
[sudo] password for kali:
Get:1 http://kali.mirror.garr.it/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.mirror.garr.it/kali kali-rolling/main amd64 Packages [21.0 MB]
Get:3 https://packages.microsoft.com/repos/code stable InRelease [3,590 B]
Get:4 https://packages.microsoft.com/repos/code stable/main armhf Packages [20.6 kB]
Get:5 https://packages.microsoft.com/repos/code stable/main arm64 Packages [20.5 kB]
Get:6 https://packages.microsoft.com/repos/code stable/main amd64 Packages [20.5 kB]
Get:7 http://kali.mirror.garr.it/kali kali-rolling/main amd64 Contents (deb) [51.4 MB]
Get:8 http://kali.mirror.garr.it/kali kali-rolling/contrib amd64 Packages [118 kB]
Get:9 http://kali.mirror.garr.it/kali kali-rolling/contrib amd64 Contents (deb) [327 kB]
Get:10 http://kali.mirror.garr.it/kali kali-rolling/non-free-firmware amd64 Packages [10.8 kB]
Get:11 http://kali.mirror.garr.it/kali kali-rolling/non-free-firmware amd64 Contents (deb) [26.7 kB]
Fetched 73.0 MB in 5s (14.5 MB/s)
26 packages can be upgraded. Run 'apt list --upgradable' to see them.
Warning: https://packages.microsoft.com/repos/code/dist/stable/InRelease: Policy will reject signature within a year, see --audit for details
(kali@kali)-[~]
└─$ sudo apt install openssl
openssl is already the newest version (3.5.0-2).
openssl set to manually installed.
The following packages were automatically installed and are no longer required:
  python3-packaging-whl python3-pyinstaller-hooks-contrib python3-wheel-whl
Use 'sudo apt autoremove' to remove them.
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 26
(kali@kali)-[~]
└─$
```

- Installazione della libreria per Python:

- sudo apt install python3-pip
- pip3 install cryptography: darà error (externally-managed-environment). Kali limita l'installazione di pacchetti python a livello globale. In quel caso è meglio usare:

- Un virtual enviroment, i comandi da usare:

- python3 -m venv
- source venv/bin/activate
- pip install cryptography
- Exit

```
(kali@kali)-[~]
└─$ python3 -m venv /home/kali/Desktop/Consegna/Consegne/Unit1/S3/L4/venv
(kali@kali)-[~]
└─$ source /home/kali/Desktop/Consegna/Consegne/Unit1/S3/L4/venv/bin/activate
(venv)-(kali@kali)-[~]
└─$ pip install cryptography
Collecting cryptography
  Downloading cryptography-45.0.5-cp311-abi3-manylinux_2_34_x86_64.whl.metadata (5.7 kB)
Collecting cffi>=1.14 (from cryptography)
  Downloading cffi-1.17.1-cp313-cp313-manylinux_2_17_x86_64.manylinux2014_x86_64.whl.metadata (1.5 kB)
Collecting pycparser (from cffi>=1.14->cryptography)
  Downloading pycparser-2.22-py3-none-any.whl.metadata (943 bytes)
Downloaded cryptography-45.0.5-cp311-abi3-manylinux_2_34_x86_64.whl (4.5 MB)
4.5/4.5 MB 41.8 MB/s eta 0:00:00
Downloaded cffi-1.17.1-cp313-cp313-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (479 kB)
Downloaded pycparser-2.22-py3-none-any.whl (117 kB)
Installing collected packages: pycparser, cffi, cryptography
Successfully installed cffi-1.17.1 cryptography-45.0.5 pycparser-2.22
(venv)-(kali@kali)-[~]
└─$
```

- Tutto questo lo ho fatto nelle directory /consegna/Unit1/S3/L4