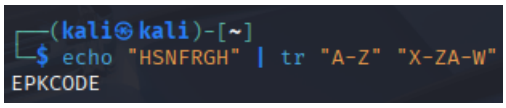
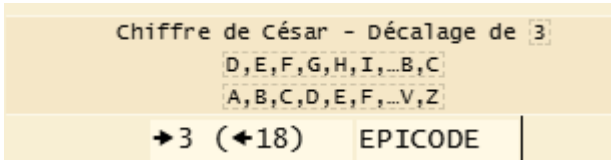
PRATICA S3/L4:

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



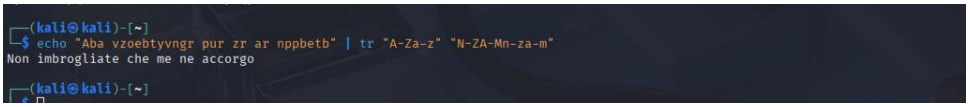
         - Seconda prova: si nota che il risultato è "EPKCODE" e intuisco che è stato utilizzato l'alfabeto italiano. Per provare che la mia intuizione fosse vera ho utilizzato il sito https://www.dcode.fr/chiffre-cesar , che conferma il risultato "EPICODE"



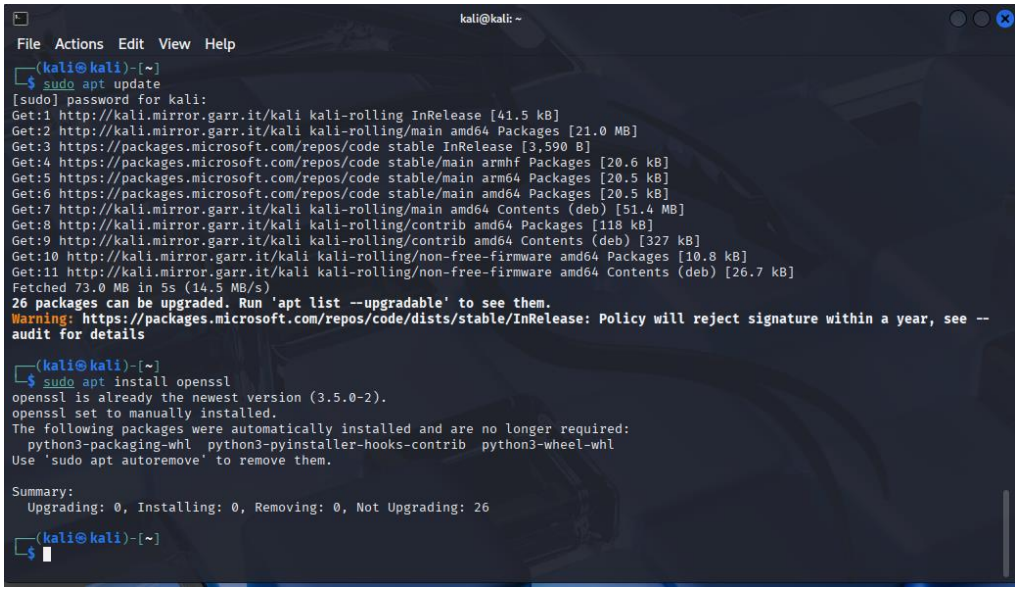
     - Messaggio cifrato: "QWJhIHZ6b2VidHl2bmdyIHB1ciB6ciBhciBucHBiZXRi"
       - È codificato in **base64:**
         - Base64: serve per rappresentare dati binari (come file o testo cifrato) in un formato leggibile usando solo caratteri ASCII.
         - Prima prova: ho usato il terminale di kali per decodificarlo da base64.

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

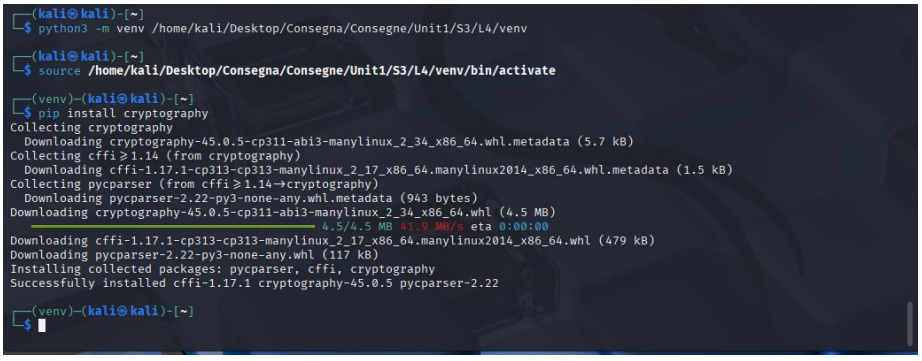
ROT13.



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

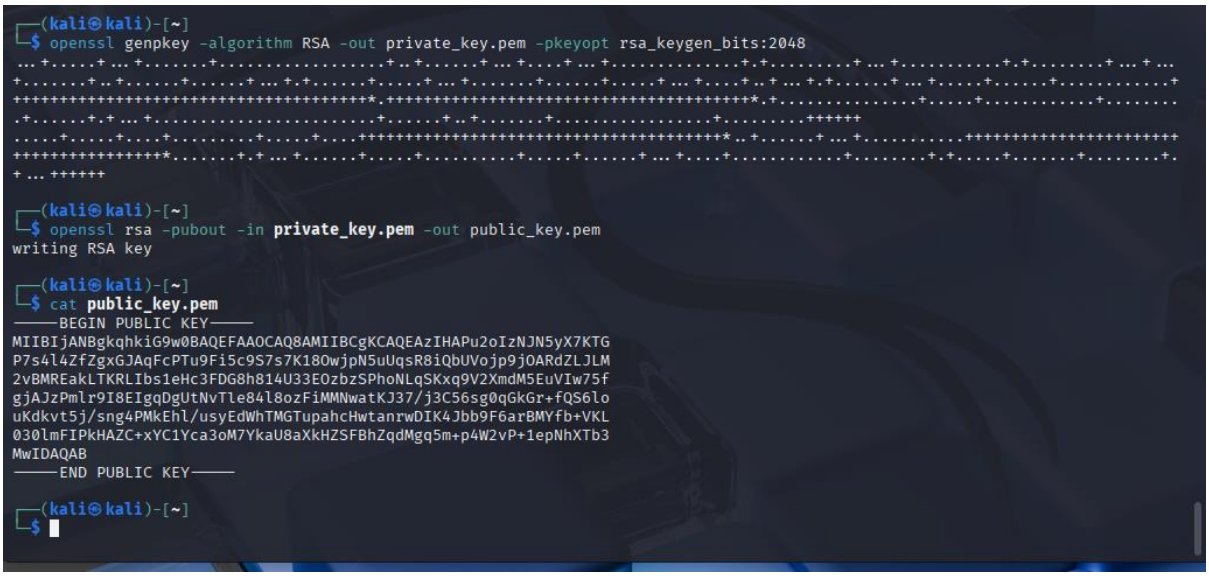


     - Installazione della libreria per Python:
       - sudo apt install python3-pip
       - pip3 install cryptography: darà error (externally-managed-environment). Kali limita l'installazione di pacchetti python a livello globale. In quel caso è meglio usare:
         - Un virtual enviroment, i comandi da usare:
           - python3 –m venv
           - source venv/bin/activate
           - pip install cryptography
           - Exit



- **Estrarre la chiave pubblica da chiave privata**
  - Comando per generare la chiave privata RSA:
    - openssl genpkey -algorithm RSA -out private_key.pem -pkeyopt rsa_keygen_bits:2048
  - Comando per estrarre la chiave pubblica:
    - openssl rsa -pubout -in private_key.pem -out public_key.pem

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



- **Per la criptazione e firmatura guardare i file:**
  - **Encdec.py**
  - **firma.py**