Esercizio di oggi: Crittografia.

1) Dato un messaggio cifrato cercare di trovare il testo in chiaro:
Messaggio cifrato: "HSNFRGH"

In questo caso è stato utilizzato il cifrario di Cesare il cui funzionamento si basa sulla scelta di un numero fisso, detto chiave, che rappresenta il numero di posizioni di cui ogni lettera del messaggio originale deve essere spostata nell'alfabeto. Ho ipotizzato che la chiave sia stata spostare di 3 lettere verso l'inizio dell'alfabeto per cui:

- H diventa E
- S diventa P
- N diventa I
- F diventa C
- R diventa O
- G diventa D
- H diventa E

Quindi la parola che ho trovato è "**Epicode**"

2) Messaggio cifrato:
QWJhIHZ6b2VidHl2bmdyIHB1ciB6ciBhciBucHBiZXRi

In questo caso ho pensato si trattasse del cifrario AES (Advanced Encryption Standard), che è uno dei più sicuri ed utilizzati. Per decifrare questa stringa ho usato il terminale di Kali Linux. Ho ripetuto le operazioni che ci sono state spiegate stamattina per arrivare al risultato del messaggio cifrato, quindi i passaggi sono stati:

- echo "QWJhIHZ2b2VidHl2bmdyIHB1ciB6ciBhciBucHBiZXRi"
  comando che stampa una stringa codificata in Base64 (codifica che permette di rappresentare dati binari come testo in 64 caratteri)

- | (pipe)
  La pipe (|) prende l'output del comando `echo` e lo passa come input al comando successivo

- openssl enc
  comando per codifica/decodifica di file o dati

- -aes-256-cbc
  Specifica l'algoritmo di cifratura (AES a 256 bit)

- -pass pass:"C1A0"
  indica la password da usare per la cifratura o decifrazione

- -a
  Questa opzione indica che il dato cifrato/decifrato è in Base64

- -d
  Significa decrypt = decifra il contenuto

Quindi la stringa scritta completa sarà così:

echo "QWJhIHZ6b2VidHl2bmdyIHB1ciB6ciBhciBucHBiZXRi" | openssl enc -aes-256-cbc pass pass:"C1A0" -a -d

Il messaggio che ho decifrato è stato: bad magic number

Vedi sotto l'esercizio pratico: