EPICODE

Esercizio
Esercizio

Esercizio di oggi: Crittografia.

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

Messaggio cifrato: "HSNFRGH"

Secondo esercizio

QWJhIHZ6b2VidHl2bmdyIHB1ciB6ciBhciBucHBiZXRi

Buon divertimento

-Messaggio cifrato 1:

Dobbiamo decifrare “HSNFRGH” e per farlo ho deciso di fare vari tentativi usando il **Cifrario di Cesare**.

Il **Cifrario di Cesare** è uno dei più semplici e noti **cifrari a sostituzione** nella crittografia. Il suo principio di funzionamento è molto semplice: ogni lettera del messaggio viene sostituita con una lettera che si trova ad una posizione fissa più avanti nell'alfabeto.

Nel nostro caso se utilizziamo una chiave di 3 il risultato è EPICODE:

H → E

S → P

N → I

F → C

R → O

G → D

H → E

-Messaggio cifrato 2:

Dobbiamo decifrare “QWJhIHZ6b2VidHl2bmdyIHB1ciB6ciBhciBucHBiZXRi”, utilizzeremo il terminale di Linux e anche qualche funzione interessante utilizzate per criptare e decriptare le chiavi della Crittografia Simmetrica e Asimmetrica.

```
┌──(kali㉿kali)-[~]
└─$ echo "QWJhIHZ6b2VidHl2bmdyIHB1ciB6ciBhciBucHBiZXRi" | base64 -d
Aba vzoebtyvngr pur zr ar nppbetb
```

Otteniamo questo risultato: “Aba vzoebtyvngr pur zr ar nppbetb” ma ovviamente questo non è sufficiente.

A questo punto ho fatto qualche tentativo con il **Cifrario di Cesare** e dopo tanti tentativi sono arrivato alla conclusione che “Aba vzoebtyvngr pur zr ar nppbetb” corrisponde a “Non imbrogliate che me ne accorgo” con ste da 13.

Come sono arrivato a questa conclusione? Ho analizzato per prima la parola “Aba” ho subito notato che 2 di quei 3 caratteri sono uguali, il che mi ha subito fatto pensare a parole come “Rar” “Bob” “Non” “Sos”. Questa chiave di lettura mi ha portato a trovare la soluzione.