ESERCIZIO LEZIONE 11 : CRITTOGRAFIA

CONSEGNA 1

Esercizio di oggi: Crittografia. Dato un messaggio cifrato cercare di trovare il testo in chiaro:
Messaggio cifrato: "HSNFRGH"

Messaggio cifrato: “QWJhIHZ6b2VidHl2bmdyIHB1ciB6ciBhciBucHBiZXRi”

CONSEGNA 2

Esercizio di oggi Criptazione e Firmatura con OpenSSL e Python:

Obiettivi dell'esercizio: ● Generare chiavi RSA.

Esercizio

Traccia e requisiti ● Estrarre la chiave pubblica da chiave privata. ● Criptare e decriptare messaggi. ● Firmare e verificare messaggi.

Strumenti utilizzati: ● OpenSSL per la generazione delle chiavi. ● Libreria cryptography in Python.

OBIETTIVI

1. Per la prima consegna analizziamo la parola e trattandosi di una lettera identica all inizio e alla fine (H) presupponiamo si tratti di una vocale, viaggiando velocemente con l’immaginazione supponiamo che la parola sia epicode (visto il nome del corso) e andiamo a verificare se ogni lettere con un banale **cifrario di cesare** mantiene lo stesso ‘slittamento di posizioni’

   la soluzione è appunto epicode, applicando un cifrario di cesare (+3)
2. la seconda frase è maggiormente complessa

QWJhIHZ6b2VidHl2bmdyIHB1ciB6ciBhciBucHBiZXRi

abbiamo pochi elementi ricorrenti e la presenza di numeri che ci fanno suggerire l'utilizzo di un sistema di codifica classico ma sofisticato, che utilizza un sistema di chiavi valore oppure una ricorrenza matematica per criptarne il significato.

tra i grandi classici della crittografia informatica, ed avendo svolto qualche breve ricerca ho individuato il metodo di cifratura **BASE 64** che converte una stringa di testo in un numero a 64 bit. per poi affibiare a ciascuna delle 64 possibilità un numero 0-9 o una lettera, maiuscola o minuscola o un carattere tra due caratteri speciali default (+ e /).

il testo decodificato risulta però ugualmente poco comprensibile

Aba vzoebtyvngr pur zr ar nppbetb

ma guardando la prima parola ci accorgiamo di nuovo di una ricorrenza di vocali e proviamo un po' di tentativi per verificare se con il cifrario di cesare otteniamo una frase con un significato

arrivati a ROT13 (carattere = carattere +13)

otteniamo

"Non imbrogliate che me ne accorgo"

e di fatto possiamo dire di aver imbrogliato solo nel non aver risolto meccanicamente l'esercizio a manina, ma aver utilizzato dei tool per decodificarlo. credo però che l'esercizio volesse proprio che ci arrivassimo barando, per dimostrare che se ce ne approfittiamo, cadremo sicuramente in trappola 😀

Esercizio bonus

Inserisci qui il testo Inserisci qui il testo Inserisci qui il testo Inserisci qui il testo Inserisci qui il testo Inserisci qui il testo Inserisci qui il testo Inserisci qui il testo.