Esercitazione 4 - Cifrari a blocchi e modalità operative

Scegliamo una Kali e attiviamo la modalità **NAT**

sudo apt-get update: aggiorna
sudo apt-get install ghex
openssl enc -list: mostra tutte le cifrature

1.
nano plain.txt -> “My name is Vortana SAY” -> **ctrl+x** -> **yes**

Cifriamo il testo:
openssl enc -aes-128-cbc -e -in plain.txt **-out** cipher_aes_128_cbc.bin

ghex cipher_aes_128_cbc.bin: apre il file (notiamo che non riusciamo a leggere nulla)

Decifriamo il testo:
openssl enc -aes-128-cbc -d -in cipher_aes_128_cbc.bin **-out** plain_aes_128_cbc.txt

ghex plain_aes_128_cbc.txt: apre il file

2.
Scaricare pic_original.bmp

Cifriamo l’immagine con due modalità operative:
A) **openssl enc -aes-128-cbc -e -in** pic_original.bmp **-out** cipher_pic_aes_128_cbc.bmp

B) **openssl enc -aes-128-ecb -e -in** pic_original.bmp **-out** cipher_pic_aes_128_ecb.bmp

Apriamo con ghex l’immagine originale (pic_original) e copiamo le prime 84 coppie di byte nelle due immagini cifrate per far sì che il sistema le riconosca come immagini.
Apriamo le due immagini cifrate e notiamo la differenza tra **ecb** e **cbc**.

3.
Le 5 principali modalità operative sono: **ecb**, **cbc**, **cfb**, **ofb**, **ctr**.
Creiamo un file di testo di 69 bytes tramite **nano** e ci scriviamo:
“My name is Vortana SAY
My name is Vortana SAY
My name is Vortana SAY”
Dobbiamo ora cifrare questo file con tutte e 5 le modalità operative.
Una volta cifrati modifichiamo il trentesimo byte dei file a piacere per corromperli. Ora decifriamo i file corrotti e vediamo come è stato propagato l’errore alle varie modalità operative.

4.
Alcune modalità operative a blocchi usano dei blocchi di dimensione standard, quindi se la dimensione del file non è un multiplo del blocco standard si avrà il **padding** per raggiungere la dimensione necessaria (standard).
Creiamo un file di testo di 20 byte e lo cifriamo con tutte e 5 le modalità operative.
Controllando la dimensione dei file attraverso “**ls -l**” possiamo vedere quale modalità operativa ha fatto uso del **padding**.

5.
Quando cifriamo possiamo usare il comando “**-nosalt**” per non aggiungere salting