Laboratorio no. 3 Cifrado de Información - parte 1

Marco Jurado 20308

In [ ]:
```
from Crypto.Cipher import DES, DES3, AES
from Crypto.Random import get_random_bytes
from Crypto.Util.Padding import pad, unpad
from PIL import Image
import numpy as np
import math
import os
```

Problema 1

AES con CBC

In [ ]:
```
def aes_cbc_encrypt(x, y):
    cipher = AES.new(y, AES.MODE_CBC)
    ct_bytes = cipher.encrypt(pad(x, AES.block_size))
    iv = cipher.iv
    return iv, ct_bytes

def aes_cbc_decrypt(iv, ct_bytes, y):
    cipher = AES.new(y, AES.MODE_CBC, iv)
    pt = unpad(cipher.decrypt(ct_bytes), AES.block_size)
    return pt
```

AES con ECB

In [ ]:
```
def aes_ecb_encrypt(x, y):
    cipher = AES.new(y, AES.MODE_ECB)
    ct_bytes = cipher.encrypt(pad(x, AES.block_size))
    return ct_bytes

def aes_ecb_decrypt(ct_bytes, y):
    cipher = AES.new(y, AES.MODE_ECB)
    pt = unpad(cipher.decrypt(ct_bytes), AES.block_size)
    return pt
```

Pipeline para cifrado y descifrado AES con ECB y CBC

In [ ]:
```
def desencriptarImagen_AES(encrypted_image_path, key_text, outputpath, mode=AES.MOD
    with open(encrypted_image_path, "rb") as encrypted_file:
            encrypted_data = encrypted_file.read()

    if mode == AES.MODE_ECB:
        cipher = AES.new(bytes.fromhex(key_text), AES.MODE_ECB)
```

```
        decrypted_data = cipher.decrypt(encrypted_data)

        decrypted_image_path = outputpath
        with open(decrypted_image_path, "wb") as decrypted_file:
            decrypted_file.write(decrypted_data)

    else:
        cipher = AES.new(bytes.fromhex(key_text), AES.MODE_CBC, bytes.fromhex(iv_he
        decrypted_data = cipher.decrypt(encrypted_data)

        try:
            decrypted_data = unpad(decrypted_data, AES.block_size)
        except ValueError:
            pass

        decrypted_image_path = outputpath
        with open(decrypted_image_path, "wb") as decrypted_file:
            decrypted_file.write(decrypted_data)

    return decrypted_image_path
```

Descifrando ambas imagenes con ECB y CBC

In [ ]:
```
key_text = '02e9bf37e279e73aa93a3b0fc3bfed8f'
encrypted_image_path = "ayno_encrypted_image.jpeg"
carpeta = 'results_parte1'

if not os.path.exists(carpeta):
    os.makedirs(carpeta)
    print(f"La carpeta {carpeta} fue creada.")
else:
    print(f"La carpeta {carpeta} ya existe.")
```

```
La carpeta results_parte1 ya existe.
```

In [ ]:
```
decrypted_image_path_ecb = desencriptarImagen_AES(encrypted_image_path, key_text, '
print(f"Imagen descifrada usando ECB guardada en: {decrypted_image_path_ecb}")
```

```
Imagen descifrada usando ECB guardada en: results_parte1/resultado_ECB_ayno.jpeg
```

In [ ]:
```
decrypted_image_path_cbc = desencriptarImagen_AES(encrypted_image_path, key_text, '
print(f"Imagen descifrada usando CBC guardada en: {decrypted_image_path_cbc}")
```

```
Imagen descifrada usando CBC guardada en: results_parte1/resultado_CBC_ayno.jpeg
```

In [ ]:
```
key_text = '406845db899854cc23484d6f3f28f3f7'
encrypted_image_path = "mr-increible_encrypted_image.jpeg"
```

In [ ]:
```
decrypted_image_path_ecb = desencriptarImagen_AES(encrypted_image_path, key_text, '
print(f"Imagen descifrada usando ECB guardada en: {decrypted_image_path_ecb}")
```

```
Imagen descifrada usando ECB guardada en: results_parte1/resultado_ECB_increible.jpe
g
```

In [ ]:
```
decrypted_image_path_cbc = desencriptarImagen_AES(encrypted_image_path, key_text, '
print(f"Imagen descifrada usando CBC guardada en: {decrypted_image_path_cbc}")
```

```
Imagen descifrada usando CBC guardada en: results_parte1/resultado_CBC_increible.jpe
g
```

Informe de hallazgos

En el proceso de descifrar imágenes cifradas utilizando el estándar AES (Advanced Encryption Standard) en los modos ECB y CBC, habian retos distintos en la eficacia de estos métodos de cifrado. La exitosa descodificación de la imagen de Mr. Increíble mediante el modo ECB demuestra que, cuando se aplica correctamente, AES puede ser efectivo para recuperar datos cifrados. Sin embargo, la naturaleza del modo ECB, que procesa cada bloque de datos de manera independiente, puede no ser siempre la opción más segura, especialmente para datos con patrones estructurales como imágenes. Por otro lado, el fracaso en descifrar la imagen "Ay No" en ambos modos, acompañado de problemas relacionados con el tamaño del padding y la corrupción de datos, sugiere desafíos técnicos como un manejo incorrecto del padding o el uso de un vector de inicialización inadecuado en el caso de CBC, lo que resalta la importancia de una implementación precisa y cuidadosa del algoritmo y sus componentes.

Este ejercicio revela que la efectividad de AES-128 depende significativamente de la correcta aplicación de sus parámetros, incluyendo la clave de cifrado, el modo de operación, y en el caso de CBC, el IV. El éxito parcial, con la descodificación de una imagen pero no de la otra, demuestra la complejidad del cifrado y descifrado de datos. Demuestra que, aunque AES es un estándar de cifrado robusto y ampliamente utilizado, su seguridad y éxito en la recuperación de datos cifrados puede verse comprometida por detalles técnicos como el manejo del padding y la selección del modo de operación, subrayando la necesidad de una implementación cuidadosa y conocimientos técnicos precisos para asegurar la integridad y confidencialidad de los datos.

¿Fue posible desencriptar las dos imagenes?

No, no fue posible descifrar ambas imágenes correctamente. Aunque logramos descifrar con éxito la imagen de Mr. Increíble utilizando el modo ECB, no de pudoc con la otra imagen, "Ay No", en ambos modos ECB y CBC. Los problemas encontrados, como el tamaño del padding incorrecto y la corrupción de datos, impidieron una recuperación exitosa de la segunda imagen.