Laboratorio no. 3 Cifrado de Información - parte 2

Marco Jurado 20308

In [ ]:
```
!openssl rand -hex 16 > clave.txt
```

In [ ]:
```
with open('clave.txt', 'r') as file:
    key = file.read().strip()
```

In [ ]:
```
!openssl enc -aes-128-ecb -nosalt -in tux_bw_content.ppm -out tux_bw_content_encryp
```

In [ ]:
```
!magick convert tux_bw_content_encrypt.ppm resultado_final.jpg
```

```
convert: improper image header `tux_bw_content_encrypt.ppm' @ error/pnm.c/ReadPNMIma
ge/343.
convert: no images defined `resultado_final.jpg' @ error/convert.c/ConvertImageComma
nd/3362.
```

Repetimos con CBC

In [ ]:
```
!openssl rand -hex 16 > clave_cbc.txt
```

In [ ]:
```
!openssl rand -hex 16 > iv.txt
```

In [ ]:
```
# Leer y mostrar el contenido de clave_cbc.txt y iv.txt
with open('clave_cbc.txt', 'r') as file:
    key = file.read().strip()
print(f"Clave (length {len(key)}): {key}")

with open('iv.txt', 'r') as file:
    iv_cbc = file.read().strip()
print(f"IV (length {len(iv_cbc)}): {iv_cbc}")
```

```
Clave (length 32): b76fd23a41e175209025d8be5cf242b5
IV (length 32): 50810778630075c43f8a12fd402c22a1
```

In [ ]:
```
!openssl enc -aes-128-cbc -nosalt -in tux_bw_content.ppm -out tux_bw_encrypted_cbc.
```

In [ ]:
```
!magick convert tux_bw_encrypted_cbc.ppm resultado_final_2.jpg
```