Lab 3 – Cifrados Simétricos

Competencias a desarrollar

- Implementar el uso de cifrado AES
- Implementar el uso de los modos CBC y ECB
- Implementar el uso de la librería pycryptodome

Problemas a resolver

En este laboratorio repasaremos y validaremos las diferencias entre los distitnos algoritmos de cifrados simétricos DES y AES.

Problema 1:

- Usted debe de conectarse al servidor por medio de ssh:
  - **Uwu-guate.site**
- Utilizar el archivo zip que se encuentra cifrado utilizando el algoritmo de cifrado :
  -
- Al descifrar el folder encontrará la credencial necesaria para conectarse al servidor

- Durante una aventura por la red mistica en el servidor encontrará un folder llamado lab3, usted ha lográdo encontrar los siguientes archivos.
  - **bad-rabbit.jpeg**
  - **pc-random.webp**
- Usted es una persona muy curiosa y se ha percatado que en un folder oculto hay una carpeta llamada llaves, en la cual encontrará los siguientes archivos:
  - **bad-rabbit-key.key**
  - **pc-random-key.key**

Utilizando las llaves e imágenes brindadas proceder a:

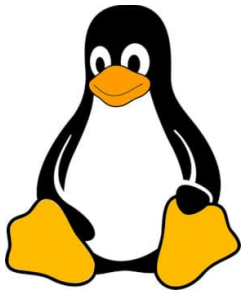
1. Implementar una función para la imagen “bad-rabbit” utilizando el cifrado AES con modo ECB.
   a. Adjunte en un archivo la imagen resultante.
2. Implementar una función para cifrar la imagen “patric-science” utilizando el cifrado AES con modo CBC.
   a. Adjunte en un archivo la imagen resultante.

3. Redacte un informe Indicando las diferencias de cifrar utilizando el modo ECB y CBC.
4. Fue posible descifrar las 2 imágenes

Problema 2 :

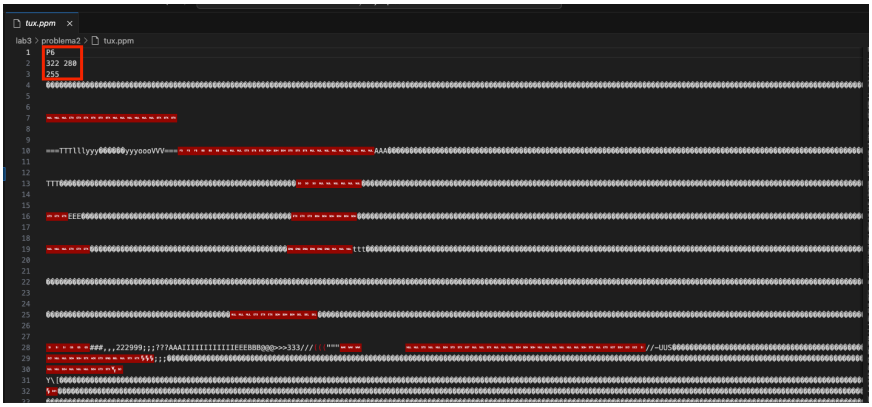
Considera AES-128 y los modos de operación. En este ejercicio demostraremos que AES-128 no es seguro por sí mismo. Para ello, estamos cifrando una imagen y observando los resultados.

1. Encuentra una imagen simple en blanco y negro de alta calidad en formato JPG/PNG o utiliza a nuestro fiel amigo tux.jpg



2. Necesitas convertir esa imagen al formato PPM. Puedes utilizar servicios web, **ImageMagick, la utilidad mogrify, etc.**

3. Elimina el encabezado de la imagen, guárdalo por separado (encabezado y cuerpo). *Normalmente, el encabezado es las primeras 3-4 líneas y el cuerpo es el resto.*



4. Descarga la biblioteca OpenSSL e instálala.
5. Utilizando OpenSSL, cifra el cuerpo de la imagen utilizando AES-128 en modo ECB, sin usar salt y con cualquier contraseña.
    a. Generen una key utilizando el siguiente comando:
        i. openssl rand -hex 16
    b. Cifrar la imagen utilizando el siguiente comando
    c. openssl enc -aes-128-ecb -nosalt -in body.ppm -out encrypted_body.ppm -K key_generada
6. Une nuevamente el encabezado al cuerpo cifrado.
7. Visualiza la imagen, muéstrala.
8. Envía la imagen obtenida y explica lo que ves.
9. Repitan el procedimiento utilizando cbc