Taller AES

En este caso práctico, se propone al estudiante la implementación de un programa que utilice el algoritmo AES-128 para cifrar y descifrar los mensajes que se muestran a continuación mediante el lenguaje de programación Python (o de su preferencia). A lo largo del ejercicio se explorarán diferentes modos de operación de AES y se analizarán sus implicaciones prácticas, incluyendo el proceso de tratamiento de errores de transmisión

Para resolver satisfactoriamente este caso práctico, el estudiante deberá completar los siguientes apartados:

1. Desarrolla un programa en el lenguaje de programación de preferencia que utilice una librería externa que implemente AES. Utiliza AES para cifrar el siguiente mensaje utilizando los siguientes parámetros:

    a. Texto plano: texto secreto

    b. Clave de cifrado: b'A\x83\xbeU\xd7\xa9b\x18\x85AN0\xbft\xc3\xab'

    c. Modo de operación: ECB (Electronic Codebook)

    PISTA: *AES requiere que se le indique un modo de operación (lo investigan), en el caso de la biblioteca como pycryptodome se corresponde con un parámetro al instanciar el algoritmo: AES.MODE_ECB*

Preguntas a responder

- ¿Qué ocurre cuando intentas cifrar el texto plano con AES?
- ¿Qué modificaciones has tenido que hacer sobre el texto plano? (PISTA: Recuerda el concepto de bloque y de **padding**)
- ¿Cuál es el texto cifrado resultante?
- ¿Cuál es el tamaño (en bytes) del texto cifrado resultante?

2. Teniendo en cuenta la implementación realizada en el punto anterior, modifica el modo de operación para que utilice CTR (en el caso de pycryptodome AES.MODE_CTR) y elimina el **padding** del texto plano.

Preguntas a responder

- ¿Qué ocurre si intentas cifrar el texto plano?

- ¿Cuál es el tamaño del texto cifrado resultante?

3. Si modifica el programa para utilizar el tamaño de clave a 256 bits en lugar de 128 bits, ***¿Qué diferencias hay en el tamaño del texto cifrado entre el modo de operación ECB y CTR?***

4. Por último, suponemos que el receptor nos ha enviado dos mensajes cifrados con AES-128 con la clave mostrada en el punto 1 y utilizando el modo ECB y CTR (**con el counter en 128**), sin embargo, se ha producido un error en la transmisión y se ha modificado 1 byte del texto cifrado. El texto cifrado que hemos recibido es el siguiente:

    a. Texto cifrado 1 (ECB): b'\xd5\x8b\xc2\xd0F\xc0w\xfe\xc1\x12\xaaX\x8f}{)i[\xf1\xc7\x9d\x1d\x08\xcd\xc2\xd8>;\r\xef\xce\xec\x89\xbd\xeb{\xe6mY\xcev\xb9\xdb\x06\x17\xd9\xd6cG6\xb4\xcfN\xf9\x15.\xbe\xed\xe7\xee#\xd0\xd9\x03\xb9l\xbap\x0c\x9c\xbe\xc3\xe1\xae\x86~pk\\\x0f'

    b. Texto cifrado 2 (CTR) *(PISTA: Revisa el parámetro counter que presentan las implementaciones de AES en el modo de operación CTR. Ponle el valor 128)*: b'{\x9a`\x04\x80\xc5\x026D\x1f\xaf\x9c&\xd1\x83\x0c\xf2wL\xd6F}\xd35B.\xb4\xe5\xb1^\x05 P\xc8\xe8\x89\xe1\xf7;G\x13\xf0\xccbs\xe8\x121\x8b4\xbf\xda\x93v\xcb\xe4\xf8g\xe72\xc5~\x97\x01TR\x9d\x0b'

Preguntas a responder

- Descifra el texto cifrado que se ha recibido.
- ¿Cuál es el texto plano resultante?
- ¿Qué diferencia hay entre un modo de operación y otro respecto a los errores en la transmisión?