Writeup P2 Tarea 1

Writeup P2 Tarea 1

Nombre: Benjamín Aguilar Osorio
Equipo: L05 1NCR31BL35

Persona a cargo de la pregunta **Benjamín Aguilar Osorio**

Descripción general del problema

Se trata de un problema de criptografia simetrica donde se deben mandar una cierta cantidad de mensajes cifrados correctos a un server (el cual te irá pidiendo los textos que debes cifrar).

Para esto, sabemos que para cifrar los mensajes se utiliza un algoritmo de cifrado CBC.

Metodología de resolución

A continuación se darán los **pasos** que se llevaron a cabo para resolver el problema:

1. Inicialmente se prueba el funcionamiento del servidor con el fin de entender su funcionamiento. Para esto, se le da a este el texto cifrado inicial y luego se le da una modificación del texto cifrado (se le cambia el primer bloque de hexadecimal), con lo que se puede identificar que el servidor da un feedback del texto que se le entrega, haciendo el descifrado del texto entregado.
2. Como siguiente paso, se decidió realizar un **Bit flipping attack**, aprovechando la característica "reversible" de la operación XOR, dónde para x, y, z arbitrarios, tal que se cumpla con la operación $x \oplus y = z$, siempre se tendrá la igualdad al intercambiar la posición de los valores **y**, **z** y **x**.
   Para esto, es necesario el uso del vector IV, por lo que se intentó encontrar la longitud de este.
3. Mientras se intentaba encontrar la longitud del vector IV mediante la modificación del mensaje cifrado inicial, viendo hasta qué parte se modificaba el mensaje original, se entregó la longitud de este en el foro del curso.
4. Teniendo la longitud del vector IV, siendo esta 16, solo bastó con modificar este usando la propiedad antes mencionada. Para lo anterior, se calcula (**IV original** $\oplus$ **Mensaje original**) $\oplus$ **Mensaje solicitado** = **Mensaje cifrado.**.
   Para llevar a cabo estas operaciones se ocupó la web **cyberchef** para conseguir el numero hexadecimal del texto plano y la web **xor.pw** para realizar las operaciones **XOR**
5. Finalmente, luego de 5 ciclos, se entrega la flag: **CC5325{fl1p_fl0p_bl1p_bl0p}**