UNIVERSIDAD DE MÁLAGA

# RELACIÓN DE EJERCICIOS

## EJERCICIO 1: cifrado

Usando la herramienta https://cryptii.com, definir el protocolo de comunicación entre Alice y Bob, de forma que Alice envíe a Bob un mensaje (M) de manera segura, usando en este caso un algoritmo simétrico en el que se garantice confidencialidad.

Precondición: Alice y Bob ya tienen negociados la clave de sesión $K_{AB}$, y todas las condiciones necesarias para enviar un mensaje, M, de manera segura.


1. Resolver el problema, asumiendo que se aplica:
   - Mensaje: "Bienvenido/a a la asignatura de Seguridad de la Información"
   - Reglas del juego:
     - Modo de operación CBC
     - IV: 00 00 00 01 00 02 00 03 00 04 00 0b 0c 0d 0e 0f
     - $K_{AB}$: 46 78 24 19 21 ab e4 b9 ff f3 17 88 09 cf 4f 3c
   - Resultado: *68 12 f2 bd 15 4a aa 19 f4 ba 2b ae 3e b6 cb 31 a5 5a 6b 19 2e 6a b2 1b ec ac 7b fd 19 a9 9c 7a 6d a5 30 fa c4 0d 02 93 62 9a f9 40 c9 15 f5 e3 22 94 12 9a fd d2 01 38 61 1d 28 5d fd e7 9f 05*
2. Volver a definir el problema aplicando AES-256:
   - Reglas del juego:
     - Modo de operación CTR
     - IV: completamente a 0.
     - $K_{AB}$: 46 78 46 78 24 19 21 ab e4 b9 ff f3 17 88 09 cf 4f 3c46 78 24 19 21 ab e4 b9 ff f3 17 88 09 cf
   - Resultado: *16 8c 27 92 7d 62 da 9b 6b 56 e4 8c 53 5a ac b1 5d 0c b5 8e c5 da 34 27 f4 c5 df 30 8d 68 08 5b 0a 9a b6 87 52 e6 a8 20 e0 22 40 28 6f c8 80 85 f0 2a 59 ab c3 b4 ca 99 a5 74 29 17*

## EJERCICIO 2: efecto avalancha

Considerando el ejercicio anterior, y mediante la herramienta https://cryptii.com, provocar el efecto avalancha:

1. Realizar el mismo ejercicio anterior con AES-128 en CBC, pero usando $K_{AB}$: 56 78 24 19 21 ab e4 b9 ff f3 17 88 09 cf 4f 3c
    a. Si se compara los criptogramas resultantes, ¿qué ocurre?
    b. Razonar y explicar muy brevemente a qué se debe ese efecto.
2. Realizar el mismo ejercicio, pero cambiando solo el último bit del texto en plano.