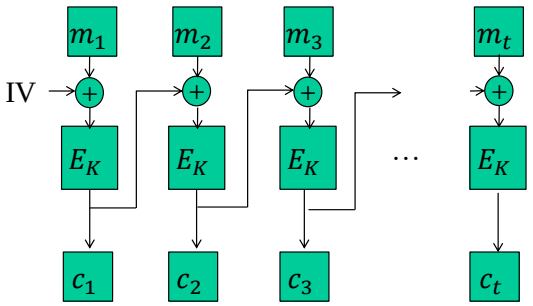
Programa de cifrado/descifrado AES

- Se deberá generar una interfaz para cifrar/descifrar un archivo dado en cualquier formato (Word, pdf, etc) usando AES. Además deberá poder establecer cualquier llave para ambos procesos.
- El AES a implementar será de 128 bits (16 bytes) de bloque a cifrar y 128 bits (16 bytes) de llave.
- Se deberá implementar el algoritmo interno tanto para el cifrado como descifrado de AES. No se podrá utilizar ninguna librería para cifrado y/o descifrado.
- Es importante que el archivo de entrada a la hora de cifrar quede idéntico al archivo descifrado (longitud y datos).
- Se cifrará en AES en modo de CBC con un IV igual a todos los bits en 0 y llenando los bits del último bloque con un byte en hexadecimal en 01 y después con bytes en 00. Esto para que concuerde con Cryptool.
- Se deberá hacer una demostración al profesor en dicha demostración el profesor tendrá un archivo a cifrar/descifrar y tendrá una llave que deberán ser utilizadas en el proceso.
- Se entregará un reporte con:
    - Descripción breve del proyecto
    - Código fuente
    - Resultados (captura de pantallas de tu programa vs Cryptool para cada uno de 4 casos seleccionados). Las imágenes deberán ser leíbles y dar evidencia del correcto funcionamiento del código
    - Conclusiones individuales

Cipher Block Chaining (CBC)

- Aquí c_0=IV (Initialization Vector)
- Mensaje original $m = m_1 + m_2 + \cdots + m_t$.



- Cifrado $c = c_1 + c_2 + \cdots + c_t$, donde $c_i = E_K(m_i \oplus c_{i-1})$
- Descifrado $m_i = E_K^{-1}(c_i) \oplus c_{i-1}$