Programa de cifrado/descifrado AES (Examen Final)

- Se deberá generar una interfaz para cifrar/descifrar un archivo dado en cualquier formato (Word, pdf, etc) usando AES.

- En la primera parte se deberá implementar el algoritmo interno tanto para el cifrado como descifrado de AES. En la segunda parte se utilizará alguna librería que use las instrucciones AES-NI y hacer lo mismo.

- Se deberá dar el tiempo tomado tanto para cifrar como descifrar.

- Es importante que el archivo de entrada a la hora de cifrar quede idéntico al archivo descifrado (longitud y datos).

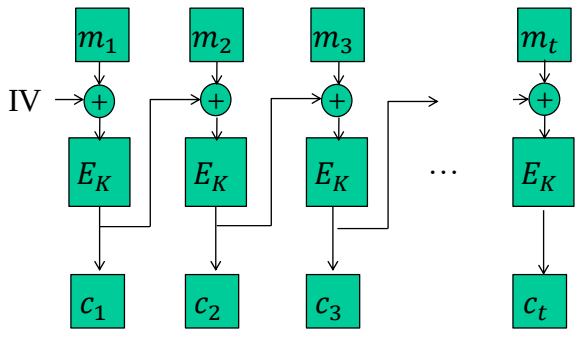
- Se cifrará en AES en modo de CBC con un IV igual a todos los bits en 0 y llenando los bits del último bloque con un byte en hexadecimal en 01 y después con bytes en 00. Esto para que concuerde con Cryptool.

- Se deberá hacer una demostración al profesor y entregar un reporte con:

  - Descripción breve del proyecto
  - Código fuente (en un archivo por separado)
  - 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.
  - Tabla que muestre el tiempo de cifrado y descifrado sin y con librería AES-NI para al menos 3 archivos de diferentes tamaños.
  - 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 $m_i = E_K^{-1}(c_i) \oplus c_{i-1}$