

**EJERCICIO 1 (5p): Crea dos soluciones con VS denominada CifraAES y DescifraAES.**  
Comprueba que **NO** esté seleccionada la opción "Crear directorio para la solución" en la esquina inferior-derecha.

Deberás llevar a cabo dos pequeños programas, uno para el cifrado (CifraAES) y otro para el descifrado (DescifraAES). Puedes usar como base la práctica sobre cifrado/descifrado AES desarrollada en clase.

Crea un proveedor AES haciendo uso de AESManaged.

Genera una clave AES de 256 bits (32 bytes). La clave generada se rellenará con números consecutivos desde 0x00 hasta el máximo de clave.

Genera el Vector de Inicialización (VI) usando los valores comprendidos en el rango 0xA0, 0xA1, ..., 0xAE, 0xAF (16 bytes).

Asigna la clave, el VI, un relleno de tipo *ISO10126* y un modo CBC.

Prepara la cadena de Streams necesarios para cifrar el fichero de entrada. Al principio debe estar un FileStream y al final un BinaryReader.

Prepara la cadena de Streams necesarios para escribir el fichero de salida (cifrado). Utiliza un FileStream y un BinaryWriter.

Ahora, estarás en disposición de realizar el proceso de cifrado del fichero "*prueba.pdf*"

Para la ejecución del programa **CifraAES** deberemos tener en cuenta pasarle 2 parámetros que serán el fichero a cifrar (*prueba.pdf*) y el nombre del fichero de salida (*cifrado.bin*)

*C:\CifraAES prueba.pdf cifrado.bin*

Para el descifrado del fichero utiliza los mismos parámetros para el proveedor AES que creamos anteriormente (clave, VI, relleno y modo).

Realiza la lectura del fichero cifrado atendiendo a la cadena de Streams, teniendo al principio a un FileStream y al final a un BinaryReader.

Realiza la escritura del fichero descifrado atendiendo a la cadena de Streams, teniendo al principio a un FileStream y al final a un BinaryWriter.

Para la ejecución del programa **DescifraAES**, deberemos tener en cuenta pasarle 2 parámetros que serán el fichero a descifrar (*cifrado.bin*) y el fichero de salida (*resultado.pdf*)

*C:\DescifraAES cifrado.bin resultado.pdf*



Apellidos \_\_\_\_\_ Nombre \_\_\_\_\_ DNI \_\_\_\_\_  
**Examen de Seguridad - Prácticas (Convocatoria Extraordinaria)** 22-Junio-2020

Finalmente, cierra ordenadamente los Streams y vuelca (flush) su contenido.

Para comprobar el resultado puedes realizar 2 tareas:

- 1) Cifrar el fichero “prueba.pdf” creando un nuevo fichero llamado “cifrado.bin”
- 2) Descifrar el fichero “cifrado.bin” creado anteriormente y comprobar que le resultado es el mismo que el original. Puedes llamar al fichero resultante “resultado.pdf” cuando realices la llamada.

**El código de los programas debe estar sangrado correctamente y tener comentarios apropiados separando las secciones. Debe ser perfectamente legible. Si no se cumplen estas condiciones, no se puntuarán los programas aunque funcionen correctamente.**

**PARA ENTREGAR EL EXAMEN EN EL CAMPUS VIRTUAL:**

- 1) Crea un directorio con tus apellidos y nombre en el formato APE1\_APE2\_NOMBRE.
- 2) Introduce en este directorio, el directorio completo de la solución de Visual Studio.
- 3) Inserta el directorio APE1\_APE2\_NOMBRE en APE1\_APE2\_NOMBRE.ZIP.
- 4) Entrega APE1\_APE2\_NOMBRE.ZIP en el Campus Virtual.

