



Práctica. CIFRADOR POR BLOQUES (DES, AES)

Implementar el algoritmo asignado con modos de operación haciendo uso de bibliotecas existentes.

Algoritmo	Equipos
DES	1, 2, 5, 8,9, 10,
AES	3, 4, 6, 7, 11, 12

La implementación puede ser una aplicación de escritorio, web o móvil, debe contar con una interfaz gráfica que permita escoger

- Cifrado
- Descifrado

- ECB
- CBC
- CFB
- OFB

Solicitar al usuario y validar los siguientes campos:

Archivo de entrada

Llave (DES=8bytes, AES=16bytes)

Vector de Inicialización (C0) (DES=8bytes, AES=16bytes)

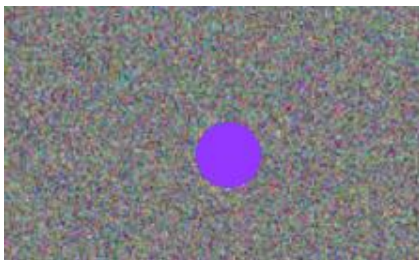
El archivo de salida debe recibir el mismo nombre del de entrada mas una letra e/d dependiendo de si fue cifrado o descifrado asi como las siglas en MAYÚSCULAS del modo de operación seleccionado.

Ejemplo para la salida despues de cifrar `image.bmp` con el modo CBC `image_eCBC.bmp`

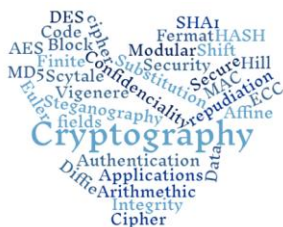
Ejemplo para la salida despues de descifrar `image_eCBC.bmp` con el modo CBC `image_eCBC_dCBC.bmp`

Cifrar las imágenes `imagen1.bmp` e `imagen2.bmp` con todos los modos de operación y hacer una tabla similar que se muestra a continuación con la imagen original y las 4 salidas ECB, CBC, CFB, OFB.

Posterior a las pruebas de descifrado exitosas, tomar la `imagen1_eCBC.bmp` y modificarla haciendo uso de algun editor de imágenes. Dibujar un círculo de color morado encima (ver ejemplo), descifrar, explicar con sus propias palabras que sucede al descifrar (mostrar imagen resultante `imagen1_eCBC_dCBC.bmp`)



Dra. Nidia A. Cortez Duarte





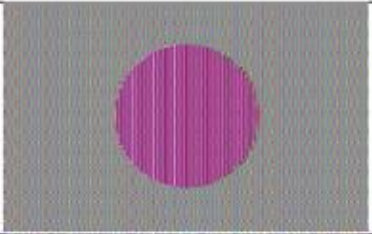





Original		
ECB		
CBC		
OFB		

Ilustración 1Ejemplo de Tabla de Resultados

Una vez concluida su implementación elaborar un vídeo (de 10-15min) de la explicación de la práctica haciendo uso de diapositivas previamente preparadas que contenga lo siguiente: *No pueden aumentar la velocidad de la grabación



Vídeo		sú
Se presentan diapositivas de power point empezando con portada y aparece el vídeo en miniatura de quién está hablando.	1	1
Tienen una diapositiva para los cifradores por bloque y redes de Feistel su explicación es fluida	1	1
Tienen una diapositiva de los modos de operación y la explicación es clara y fluida	1	1
Se explica claramente sobre la biblioteca utilizada y las funciones criptográficas	1	1
Se detallan los parametros que reciben las funciones utilizadas	1	1
Se explican a detalle los pasos necesarios para procesar la imagen(tanto para leer el archivo original como para general los nuevos)	1	1
Se incluye la tabla de los cifrados obtenidos para las imágenes imagen1.bmp e imagen2.bmp así como el descifrado de una por una correctamente	1	1
Explicar que pasa al descifrar *_eCBC.bmp con el modo OFB y *_eCFB.bmp con el modo CBC (mostrando las imágenes resultantes)	1	0
Explicar qué pasa al cifrar *.bmp con el modo OFB dos veces (mostrando las imágenes resultantes)	1	1
Se explica qué pasa al descifrar image1_eCBC.bmp editada con un círculo morado (mostrando la imagen resultante) fundamentando con la parte teórica (haciendo uso del diagrama de descifrado CBC)	1	1
Presenta conclusiones individuales sobre usos y ventajas de cada modo de operación	1	1
Demostración de Práctica		
El programa cuenta con interfaz gráfica que le permita al usuario elegir la opción deseada: cifrado o descifrado y el modo de operación así como introducir K y C0.	1	1
La interfaz permite seleccionar el archivo que se va a cifrar/descifrar	1	1
Su programa genera los archivos con los nombres solicitados en las especificaciones.	1	1
Alicia muestra como manda las imágenes cifradas, Betito muestra como descarga las imágenes recibidas	1	1
TOTAL	15	14

Hernández López Bryan
Rodriguez Olmos Noé

Nota: Favor de llenar la columna de la derecha en caso de cumplir con lo requerido y subirla a la entrega de la práctica. En caso de que no puedan grabar el vídeo juntos, es posible que Alicia grabe su parte, Betito su parte y finalmente se integre en un solo vídeo.

Dra. Nidia A. Cortez Duarte

