Nombre: Ortega Silva Jorge Eduardo

Fecha: 15/05/2022

Nombre de la práctica: “Lab 5: Block ciphers and modes of operation”

Organización de los programas

KeyDES.py

Es el encargado del primer punto requerido, genera dos llaves aleatorias de triple DES, y las guarda en un archivo con su respectivo nombre, estas son generadas en su ejecución en archivos con los nombres:

- “LlaveDES112.txt”: haciendo referencia a la llave de 112 bits
- “LlaveDES168.txt”: haciendo referencia a la llave de 168 bits

Cipher_DES.py

Es el encargado de cumplir con el segundo punto requerido, cifrado con triple DES, guarda el cifrado en un archivo con el de “Cifrado_DES.txt”, el modo de operación que implemento es CBC, la llave es guardada en “Key_DES.txt” y el vector de inicialización en “IV_DES.txt”, al momento de ejecutar el programa pide el archivo a cifrar con la extensión txt.

Dec_DES.py

Es el encargado de cumplir con el tercer punto requerido, descifra el archivo generado por el punto anterior, al momento de ejecutar solicita, el nombre del archivo a descifrar, el de la llave y el del vector de inicialización, todos escritos con su extencion txt, todos aquellos fueron generados en el punto anterior, como resultado genera un archivo llamado “Descifrado_DES.txt” donde se guarda el resultado.

KeyAES.py

Es el encargado del cuarto punto requerido, genera dos llaves aleatorias de AES, y las guarda en un archivo con su respectivo nombre, estas son generadas en su ejecución en archivos con los nombres:

- “LlaveAES128.txt”: haciendo referencia a la llave de 112 bits
- “LlaveAES192.txt”: haciendo referencia a la llave de 192 bits
- “LlaveAES256.txt”: haciendo referencia a la llave de 256 bits

Cipher_AES.py

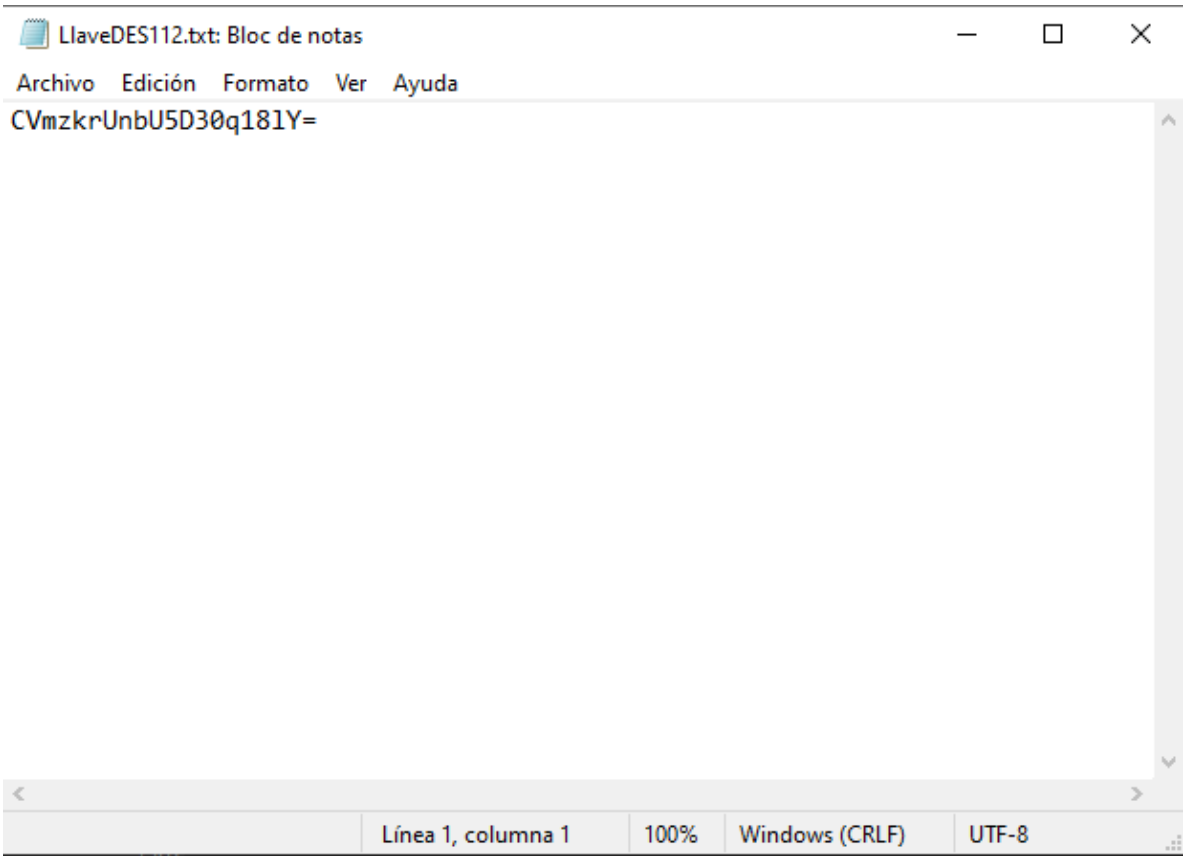
Es el encargado de cumplir con el quinto punto requerido, cifrado con AES, guarda el cifrado en un archivo con el de “Cifrado_AES.txt”, el modo de operación que implemento es CTR, la llave es de 128 bits y es guardada en “Key_AES.txt”, el vector de inicialización es guardado en “IV_AES.txt”, al momento de ejecutar el programa pide el archivo a cifrar con la extensión txt.

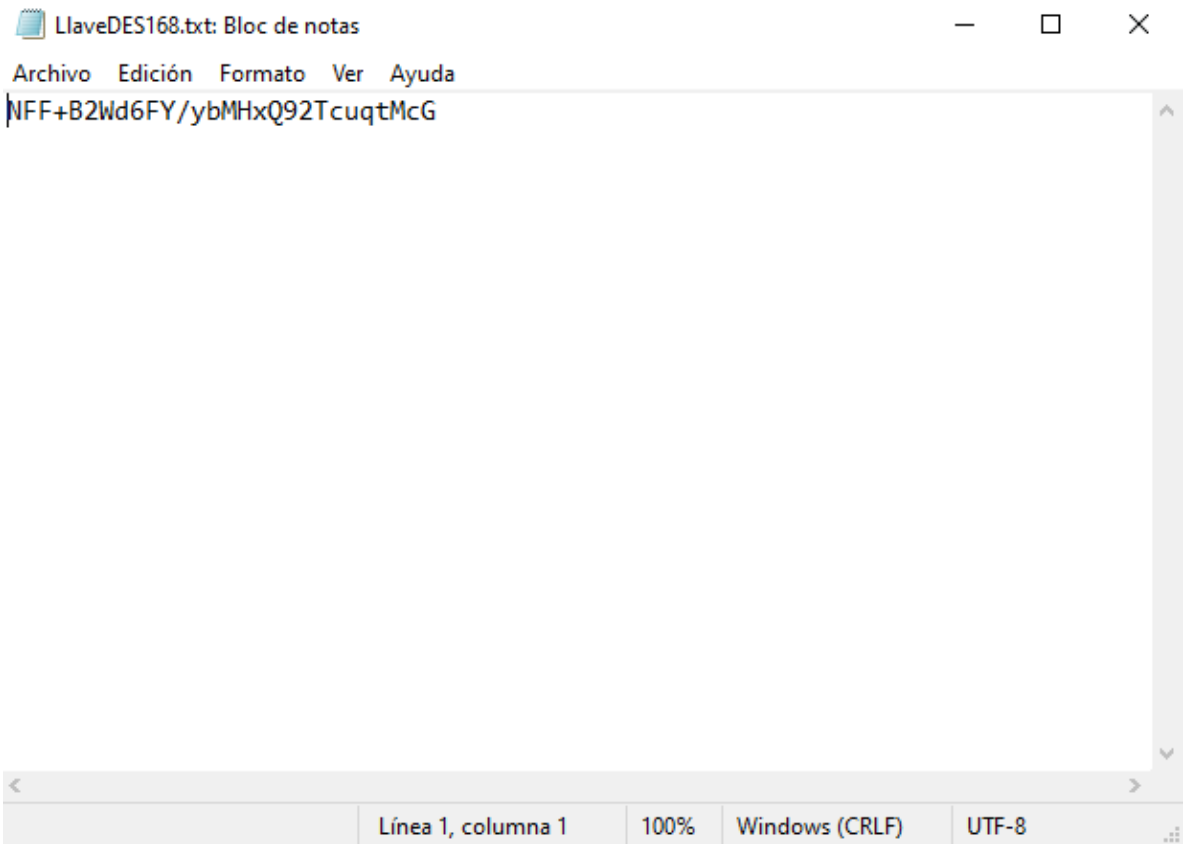
Dec_AES.py

Es el encargado de cumplir con el tercer punto requerido, descifra el archivo generado por el punto anterior, al momento de ejecutar solicita, el nombre del archivo a descifrar, el de la llave y el del vector de inicialización, todos escritos con su extencion txt, todos aquellos fueron generados en el punto anterior, como resultado genera un archivo llamado “Descifrado_AES.txt” donde se guarda el resultado.

Capturas

Primer punto



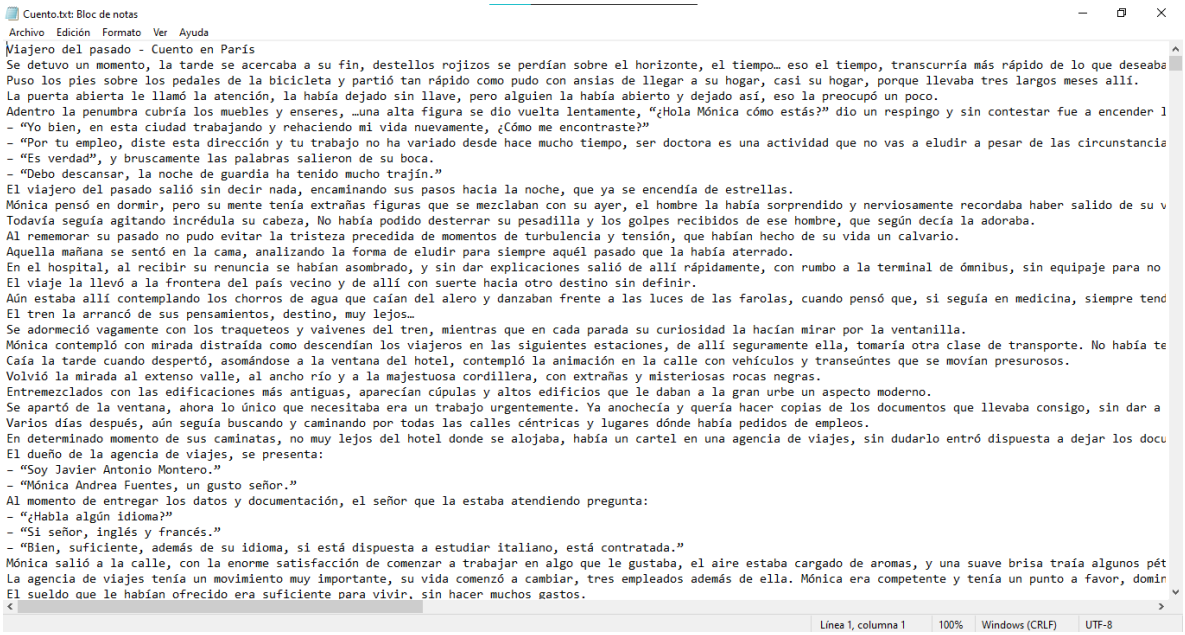


Segundo punto

Ejecución

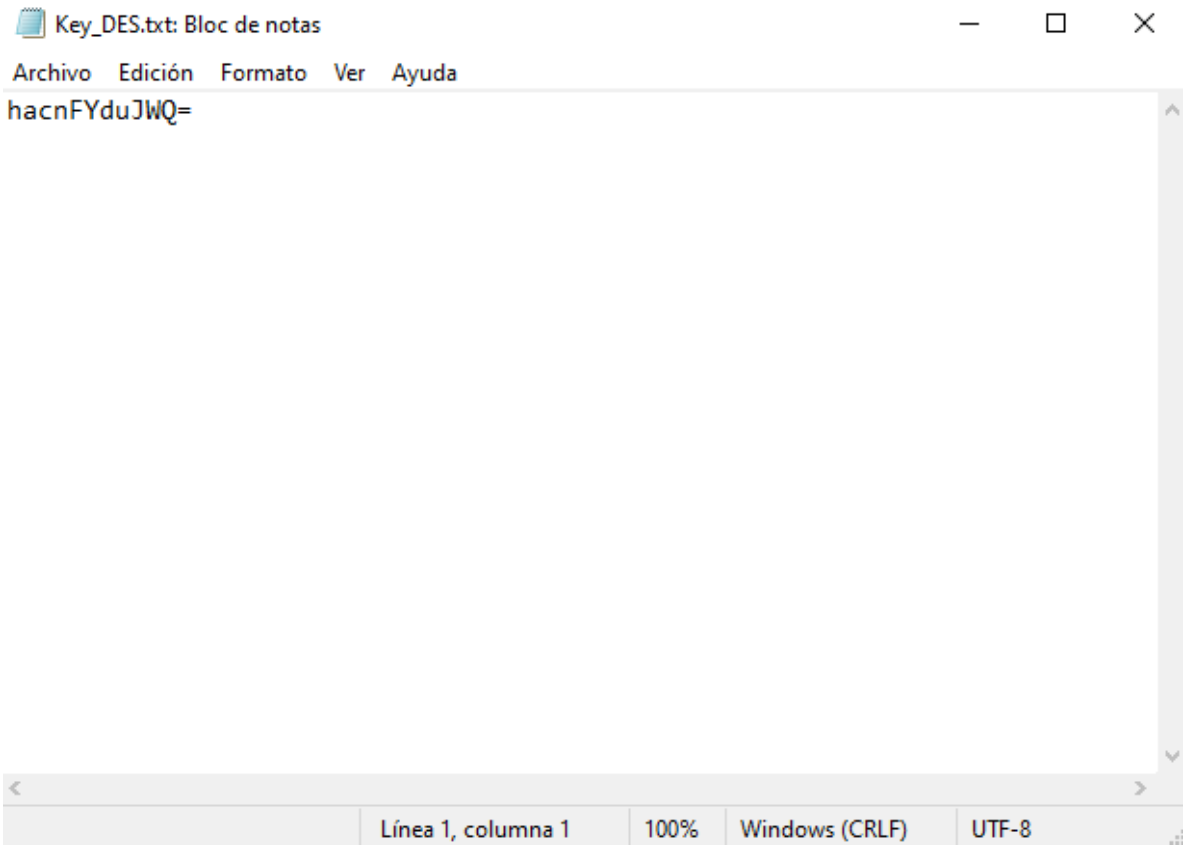
```
Instrucciones ingrese el nombre con extencion .txt


Nombre del archivo txt cifrado: Cuento.txt
```

Sin cifrar

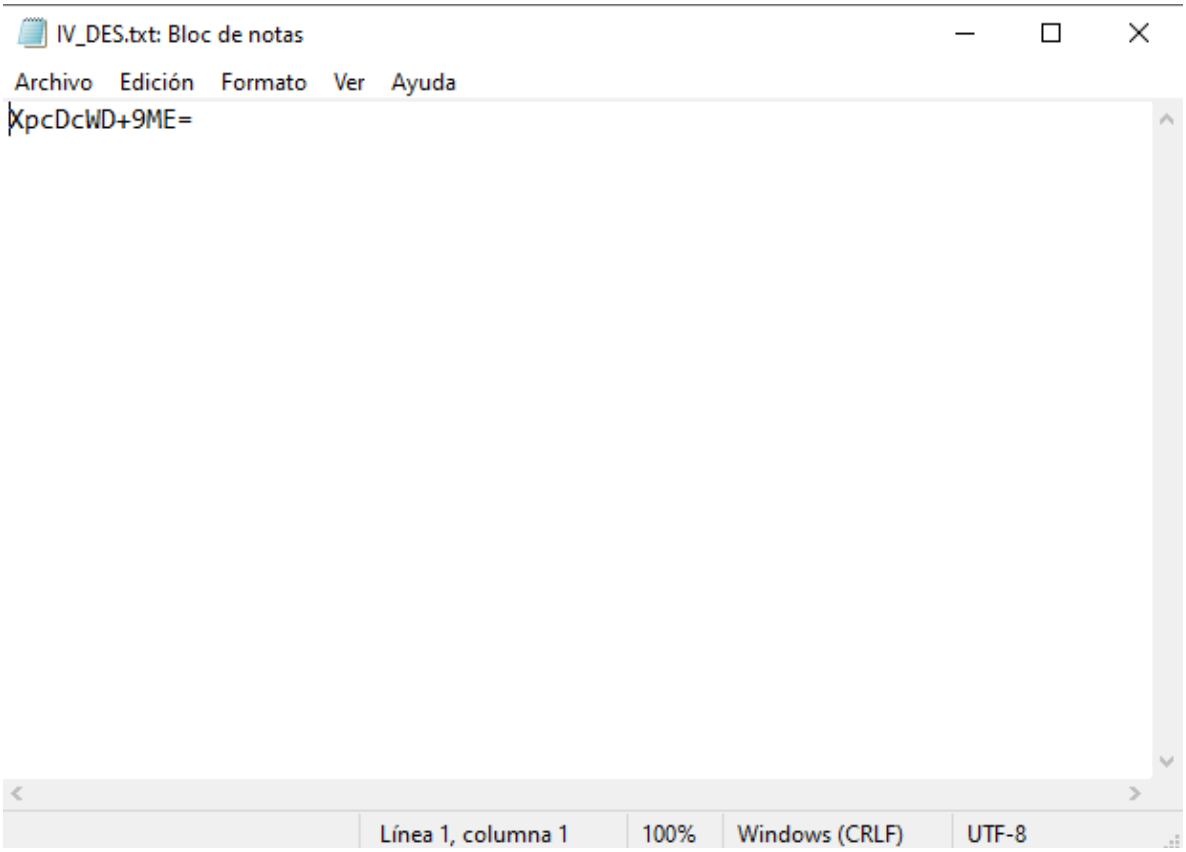


Cifrado

Llave



Vector de inicialización

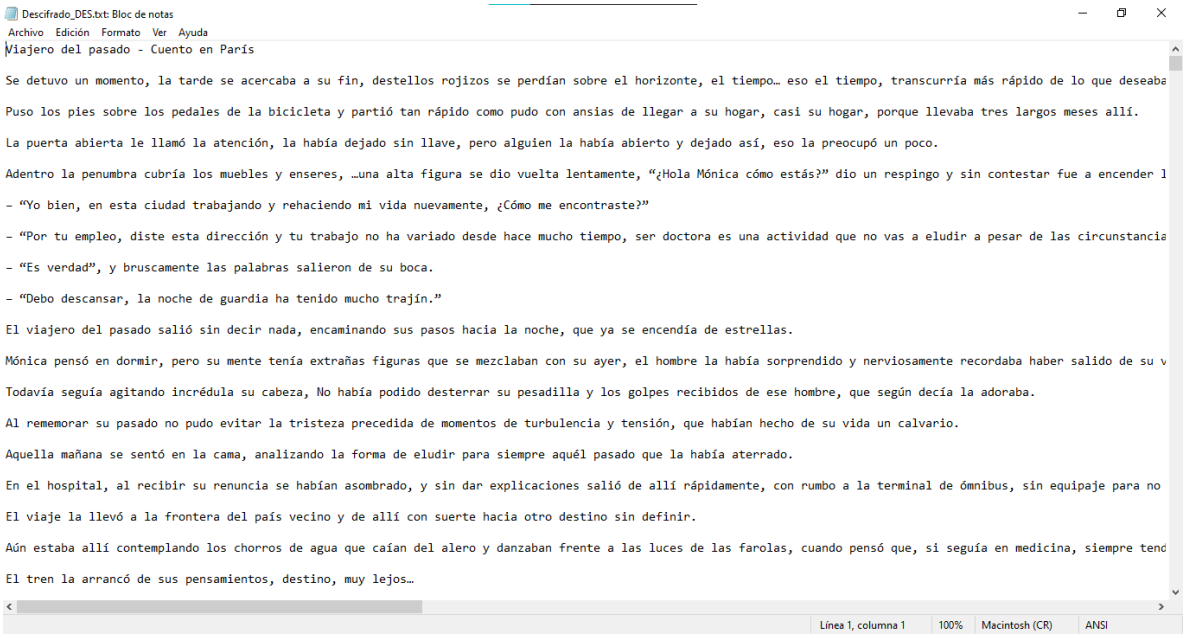


Tercer punto

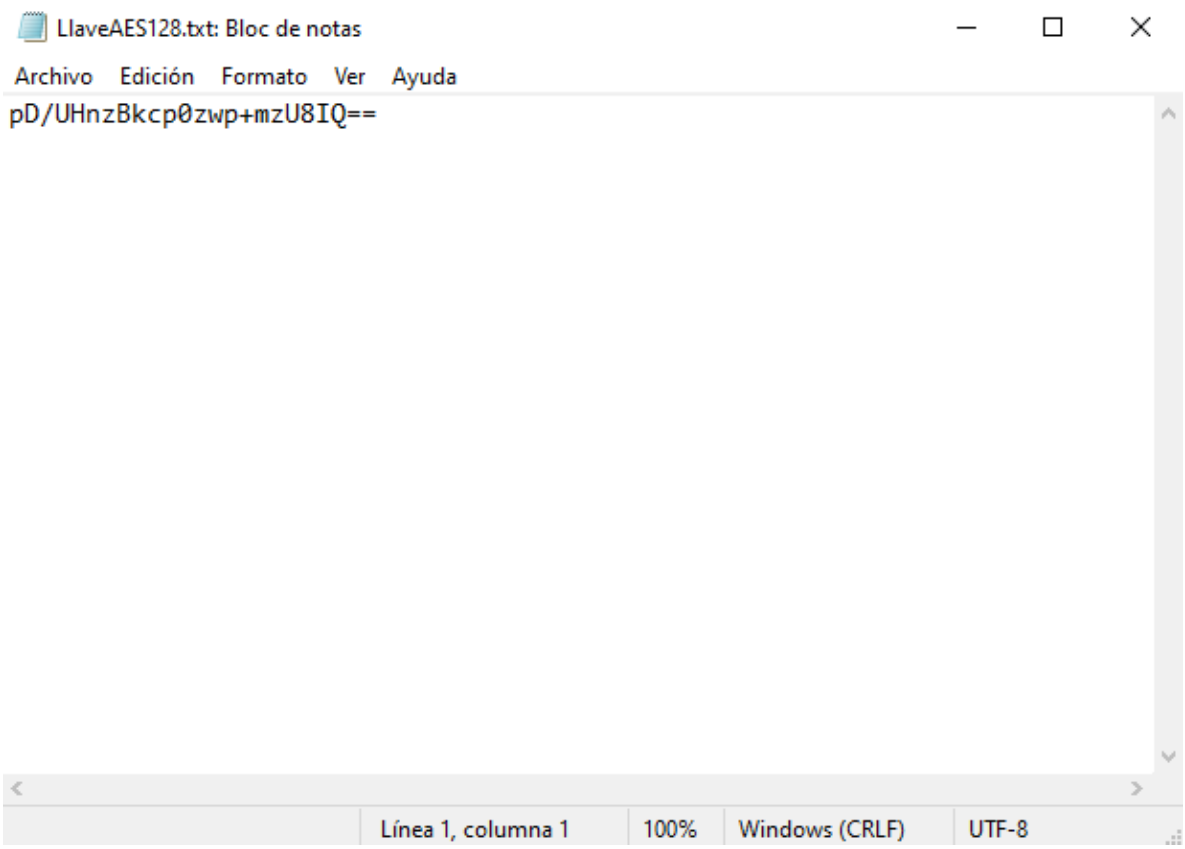
Ejecución

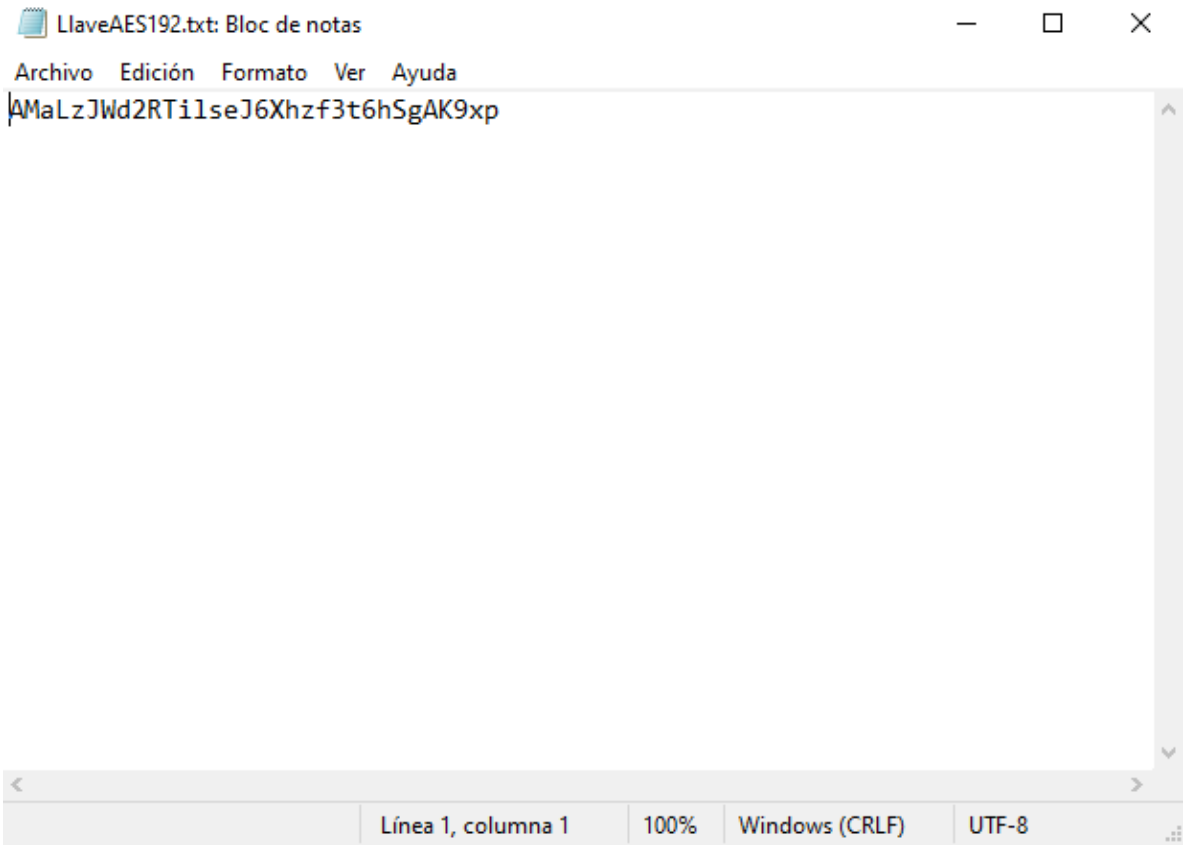
```
Instrucciones ingrese los nombres con extencion .txt


Nombre del archivo txt cifrado: Cifrado_DES.txt

Nombre del archivo con la llave: Key_DES.txt

Nombre del archivo con el vector de inicializacion:
IV_DES.txt
```

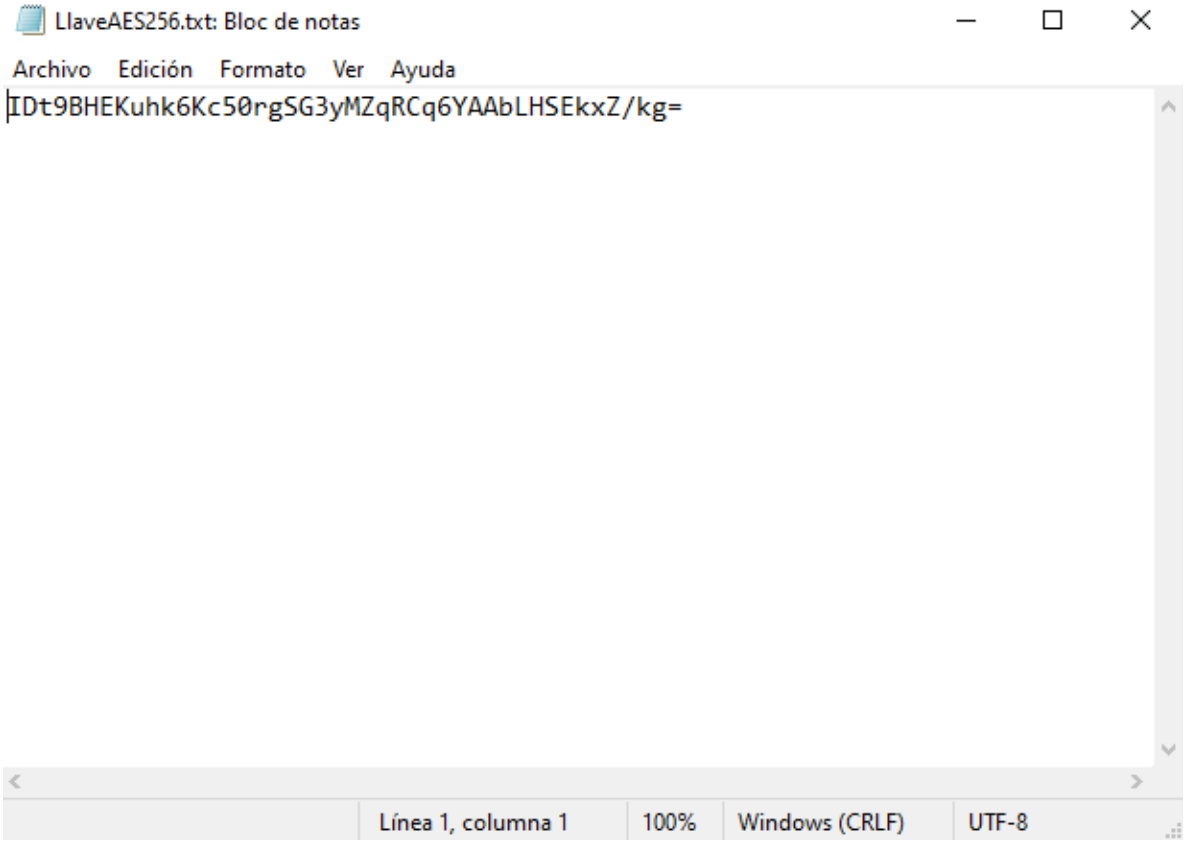
Descifrado



Cuarto punto




LlaveAES192.txt: Bloc de notas
Archivo Edición Formato Ver Ayuda
AMaLzJWd2RTilseJ6Xhzf3t6hSgAK9xp
Línea 1, columna 1
100%
Windows (CRLF)
UTF-8

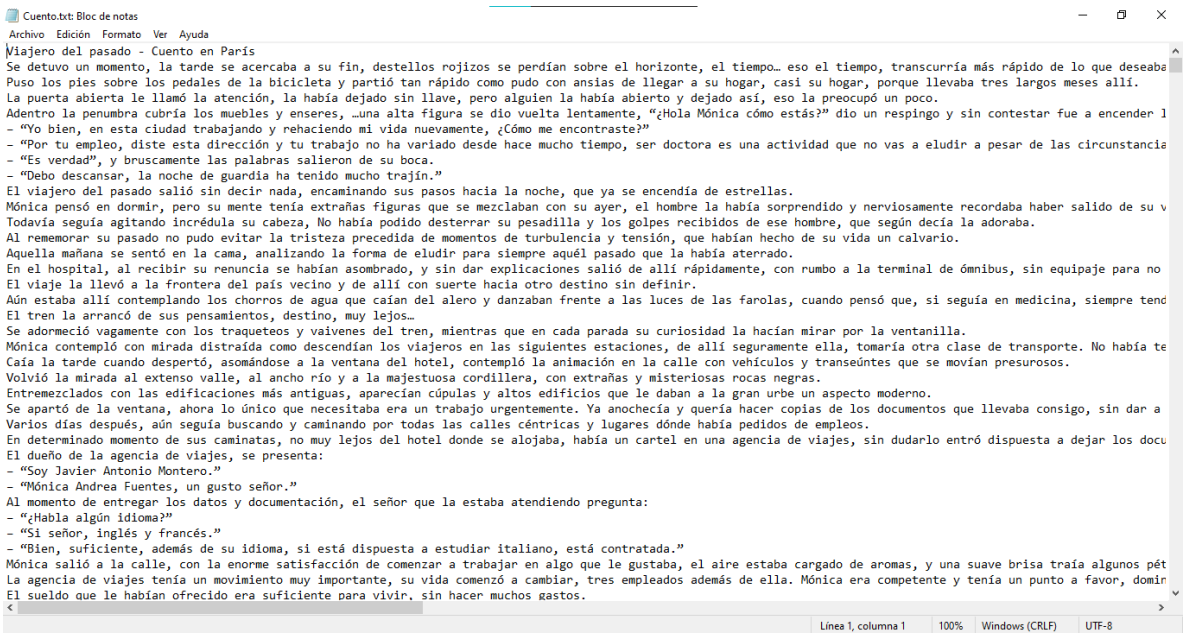

LlaveAES256.txt: Bloc de notas
Archivo Edición Formato Ver Ayuda
IDt9BHEKuhk6Kc50rgSG3yMZqRCq6YAAbLHSEkxZ/kg=
Línea 1, columna 1
100%
Windows (CRLF)
UTF-8

Quinto punto

Ejecución

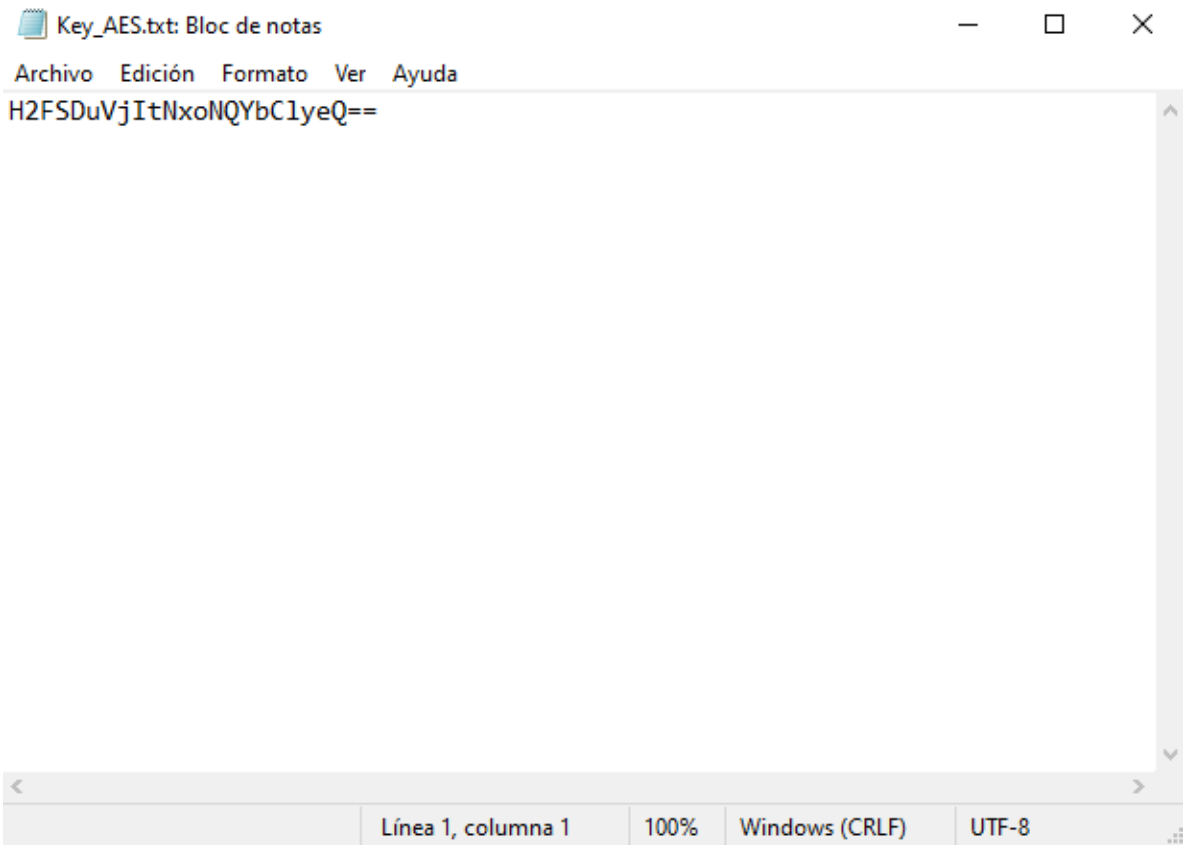
```
Instrucciones ingrese el nombre con extencion .txt


Nombre del archivo txt cifrado: Cuento.txt
```

Sin cifrar

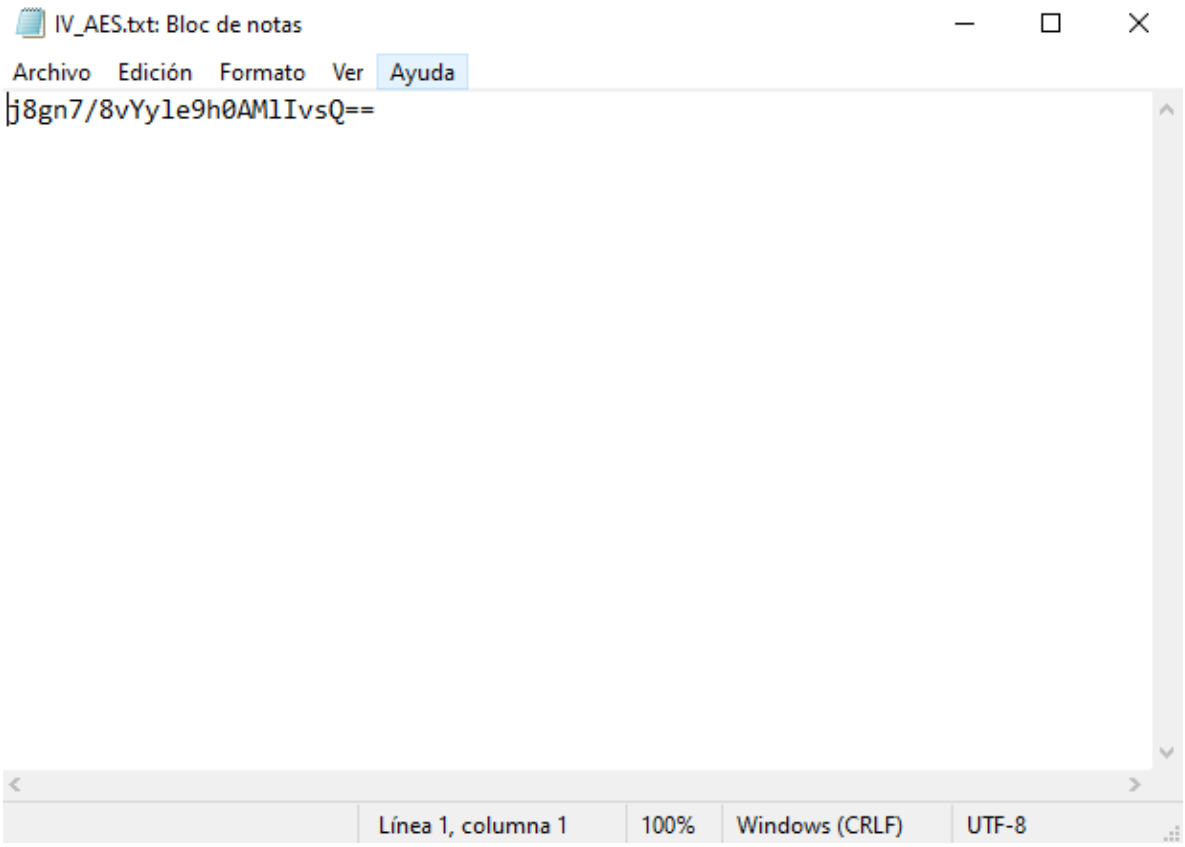


Cifrado

Llave



Vector de inicialización

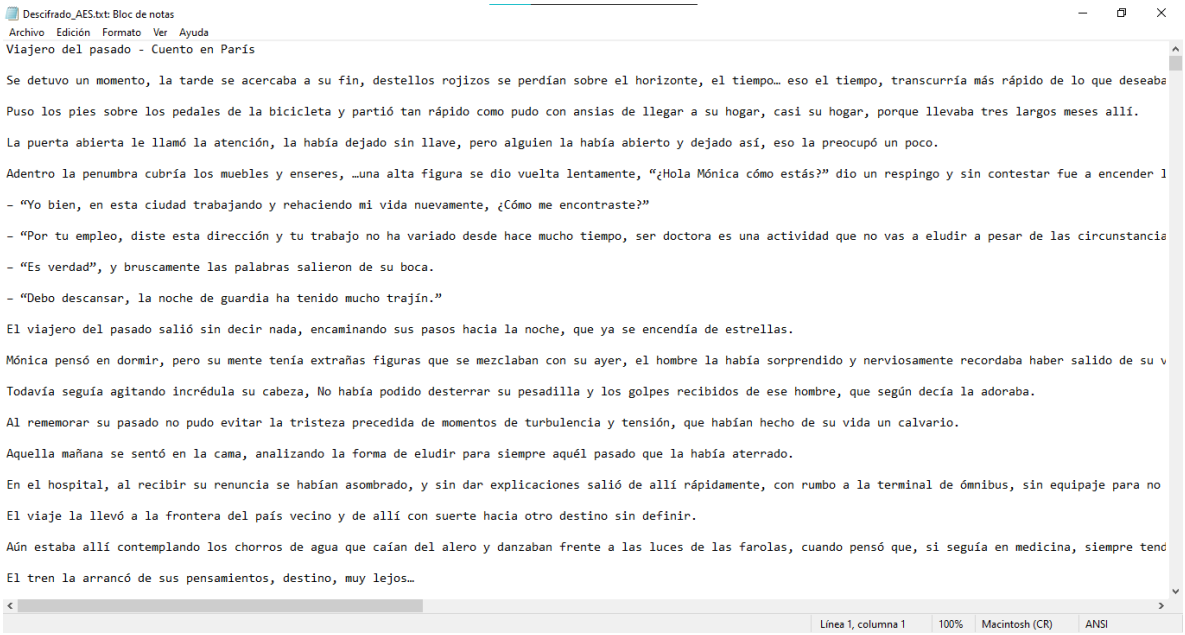


Sexto punto

Ejecución

```
Instrucciones ingrese los nombres con extencion .txt


Nombre del archivo txt cifrado: Cifrado_AES.txt

Nombre del archivo con la llave: Key_AES.txt

Nombre del archivo con el vector de inicializacion:
IV_AES.txt
```

Descifrado


Descifrado_AES.txt: Bloc de notas
Archivo Edición Formato Ver Ayuda
Viajero del pasado - Cuento en París
Se detuvo un momento, la tarde se acercaba a su fin, destellos rojizos se perdían sobre el horizonte, el tiempo… eso el tiempo, transcurría más rápido de lo que deseaba
Puso los pies sobre los pedales de la bicicleta y partió tan rápido como pudo con ansias de llegar a su hogar, casi su hogar, porque llevaba tres largos meses allí.
La puerta abierta le llamó la atención, la había dejado sin llave, pero alguien la había abierto y dejado así, eso la preocupó un poco.
Adentro la penumbra cubría los muebles y enseres, …una alta figura se dio vuelta lentamente, "¿Hola Mónica cómo estás?" dio un respingo y sin contestar fue a encender l
– "Yo bien, en esta ciudad trabajando y rehaciendo mi vida nuevamente, ¿Cómo me encontraste?"
– "Por tu empleo, diste esta dirección y tu trabajo no ha variado desde hace mucho tiempo, ser doctora es una actividad que no vas a eludir a pesar de las circunstancia
– "Es verdad", y bruscamente las palabras salieron de su boca.
– "Debo descansar, la noche de guardia ha tenido mucho trajín."
El viajero del pasado salió sin decir nada, encaminando sus pasos hacia la noche, que ya se encendía de estrellas.
Mónica pensó en dormir, pero su mente tenía extrañas figuras que se mezclaban con su ayer, el hombre la había sorprendido y nerviosamente recordaba haber salido de su v
Todavía seguía agitando incrédula su cabeza, No había podido desterrar su pesadilla y los golpes recibidos de ese hombre, que según decía la adoraba.
Al rememorar su pasado no pudo evitar la tristeza precedida de momentos de turbulencia y tensión, que habían hecho de su vida un calvario.
Aquella mañana se sentó en la cama, analizando la forma de eludir para siempre aquél pasado que la había aterrado.
En el hospital, al recibir su renuncia se habían asombrado, y sin dar explicaciones salió de allí rápidamente, con rumbo a la terminal de ómnibus, sin equipaje para no
El viaje la llevó a la frontera del país vecino y de allí con suerte hacia otro destino sin definir.
Aún estaba allí contemplando los chorros de agua que caían del alero y danzaban frente a las luces de las farolas, cuando pensó que, si seguía en medicina, siempre tend
El tren la arrancó de sus pensamientos, destino, muy lejos…
Línea 1, columna 1
100%
Macintosh (CR)
ANSI