Escuela Superior
de Ingeniería y Tecnología
Universidad de La Laguna

Cifrado simétrico con OpenSSL:

Seguridad de Sistemas Informáticos

Cheuk Kelly Ng Pante
alu0101364544@ull.edu.es

1. Comprobar lista de algoritmos simétricos soportados por OpenSSL

Para comprobar la lista de algoritmos simétricos soportados por OpenSSL hacemos uso del comando

```
Unset
openssl enc -list
```

Los cifrados que hay:

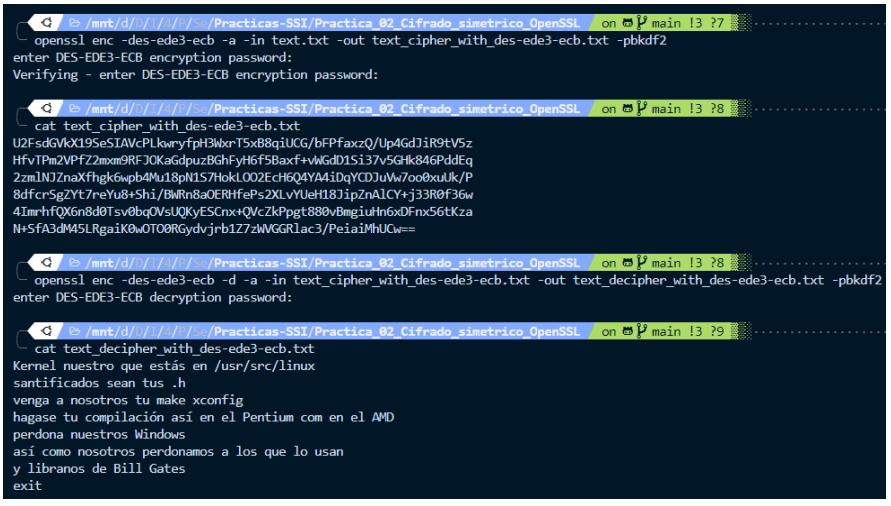
- Cifrado en flujo: RC, Chacha20
- Cifrado en bloque: AES, CAST, DES, RC2

2. Generación de un documento de texto y cifrar.

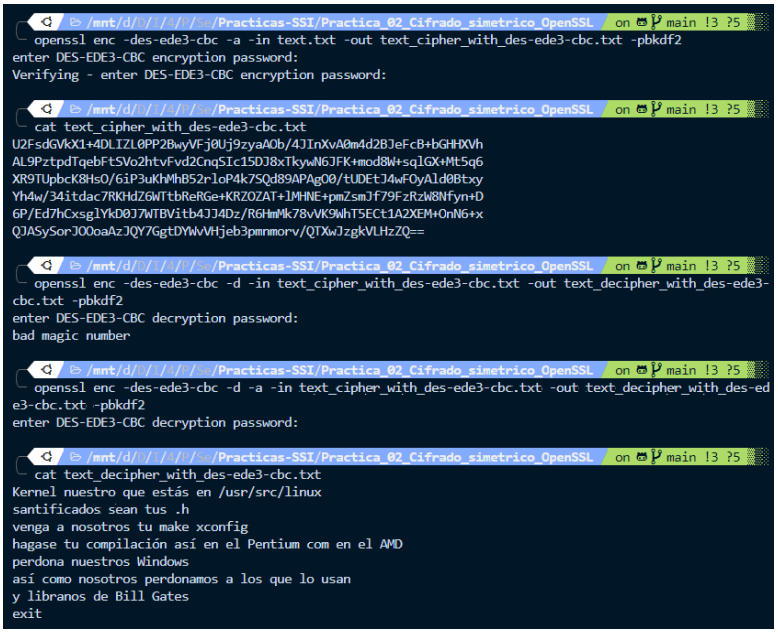
```
Kernel nuestro que estás en /usr/src/linux
santificados sean tus .h
venga a nosotros tu make xconfig
hagase tu compilación así en el Pentium con el AMD
perdona nuestros Windows
así como nosotros perdonamos a los que lo usan
y libranos de Bill Gates
exit
```

2.1. Cifrar con triple des EDE en modo cifrado ECB y CBC

- Cifrado con `des-ede3-ecb`:

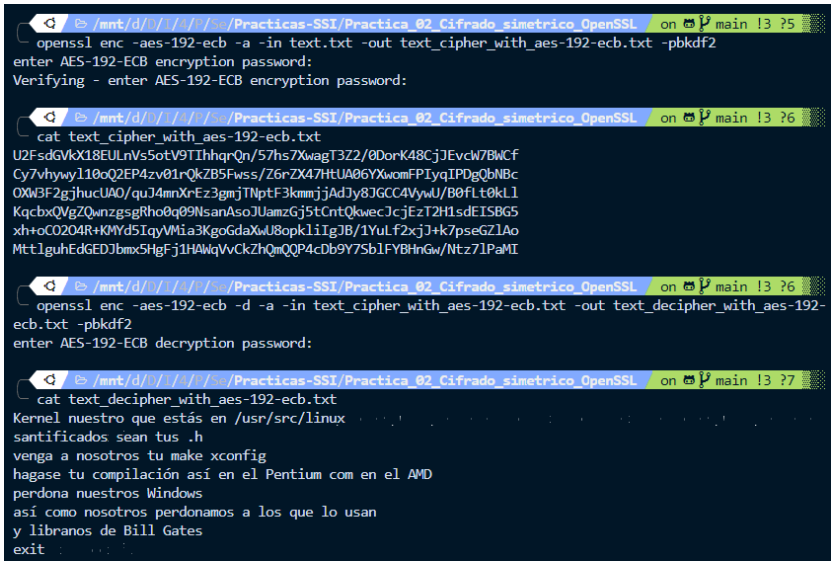


- Cifrado con `des-ede3-cbc`:

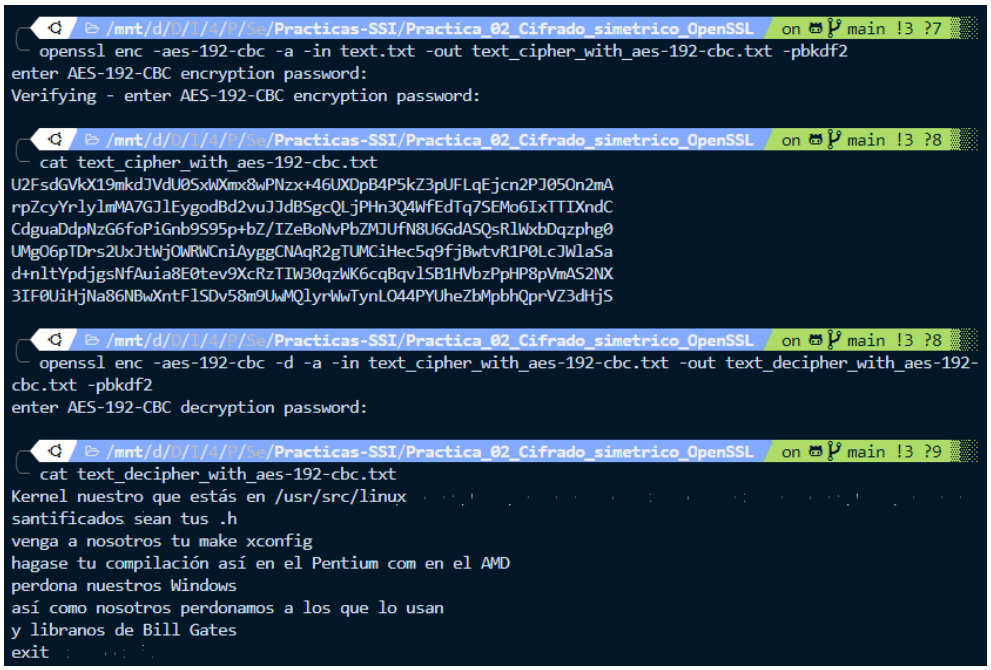


2.2. Cifrar con AES 192 en modo cifrado ECB y CBC

- Cifrado con `aes-192-ecb`:



- Cifrado con `aes-192-cbc`:



2.3. Analiza el comportamiento de los cifrados DES y AES usando todas las longitudes de clave posibles y todos los modos de cifrado implementados y medimos el tiempo.

Algoritmo	**Tiempo**
-aes-128-cbc	0m2.778s
-aes-128-ecb	0m1.968s
-aes-192-cbc	0m1.784s
-aes-192-ecb	0m1.554s
-aes-256-cbc	0m1.665s
-aes-256-ecb	0m1.500s
-des	0m1.569s
-des-cbc	0m3.421s
-des-cfb	0m2.246s
-des-ecb	0m1.592s

-des-ede	0m1.570s
-des-ede-cbc	0m1.604s
-des-ede-cfb	0m1.607s
-des-ede-ofb	0m2.374s
-des-ede3	0m2.574s
-des-ede3-cbc	0m2.345s
-des-ede3-cfb	0m2.193s
-des-ede3-ofb	0m2.724s
-des-ofb	0m3.738s

2.4. Haz el mismo análisis para las versiones de RC4 implementadas en OpenSSL.

Algoritmo	**Tiempo**
-rc4	0m2.370s
-rc-40	0m2.370s

3. Genera los parámetros necesarios para cifrar con el cifrado AES usando el modo CFB y una longitud de clave de 192.

Para generar los parámetros necesarios para cifrar con el cifrado AES usando el modo CFB y una longitud de clave de 192:

```
Unset
openssl rand -out key.txt 32
```

Este comando generará un archivo `key.txt` con una clave aleatoria de 32 bytes, que es la longitud necesaria para el cifrado AES-192.

Una vez que tengamos la clave, podemos utilizarla para cifrar los datos:

```
Unset
openssl enc -aes-192-cfb -in data.txt -out encrypted.txt -key
key.txt
```

Este comando cifrará el contenido del archivo `data.txt` y lo guardará en el archivo `encrypted.txt`.

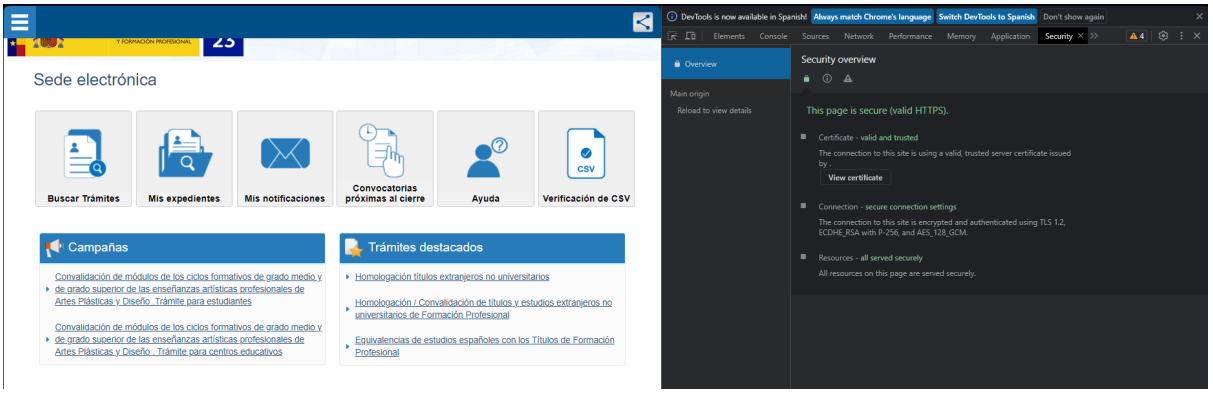
Para descifrar los datos, podemos utilizar el siguiente comando:

```
Unset
openssl enc -aes-192-cfb -in encrypted.txt -out decrypted.txt -key
key.txt
```

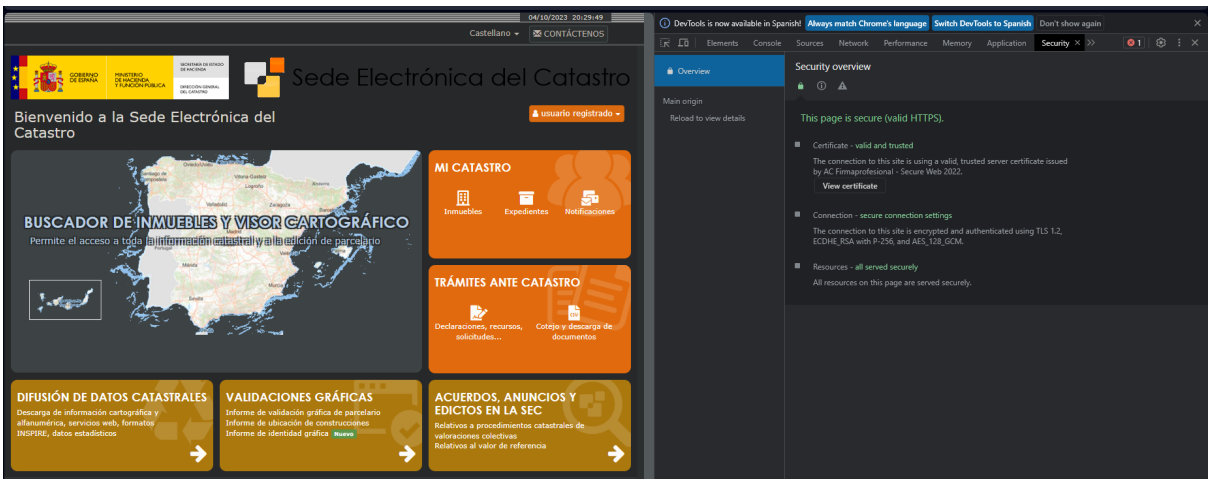
Este comando descifrará el contenido del archivo `encrypted.txt` y lo guardará en el archivo `decrypted.txt`.

4. Cifrado en HTTPs (estas conexiones usan TSL):

4.1. Accede a las página https://sede.educacion.gob.es y https://www1.sedecatastro.gob.es/, ¿qué algoritmo simétrico se utiliza para cada conexión?



- Protocolo de cifrado: TLS 1.2
- Algoritmo de intercambio de claves: ECDHE_RSA
- Algoritmo de cifrado: AES-128-GCM
- Modo de cifrado: GCM



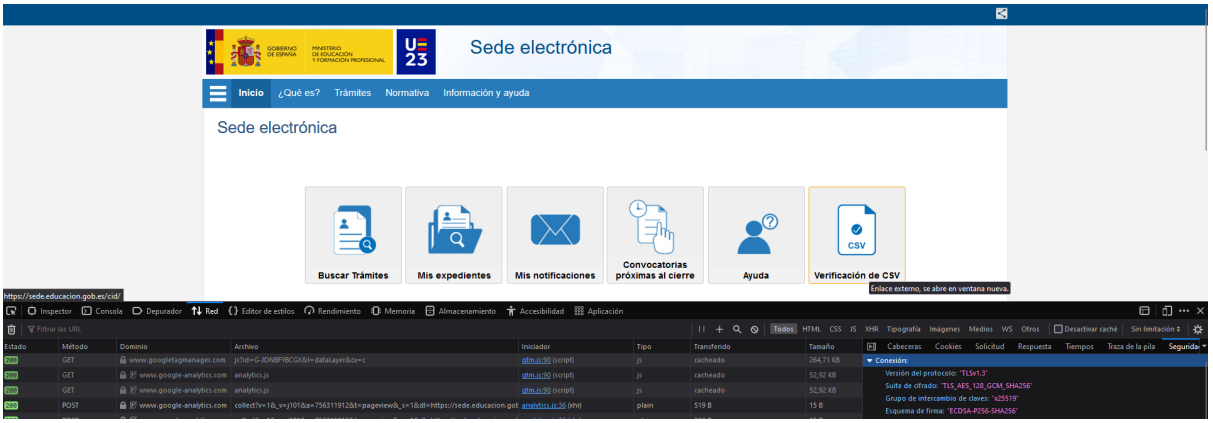
- Protocolo de cifrado: TLS 1.2
- Algoritmo de intercambio de claves: ECDHE_RSA
- Algoritmo de cifrado: AES-256-GCM
- Modo de cifrado: GCM

4.2. Probar distintos navegadores (Firefox, IE, etc), ¿existen diferencias entre las especificaciones de cifrado?

- Desde navegador Microsoft Edge:

Podemos observar que desde la página de la sede de educación y la sede electrónica del castro no ha cambiado nada con el navegador Microsoft Edge.

- Desde navegador Firefox:

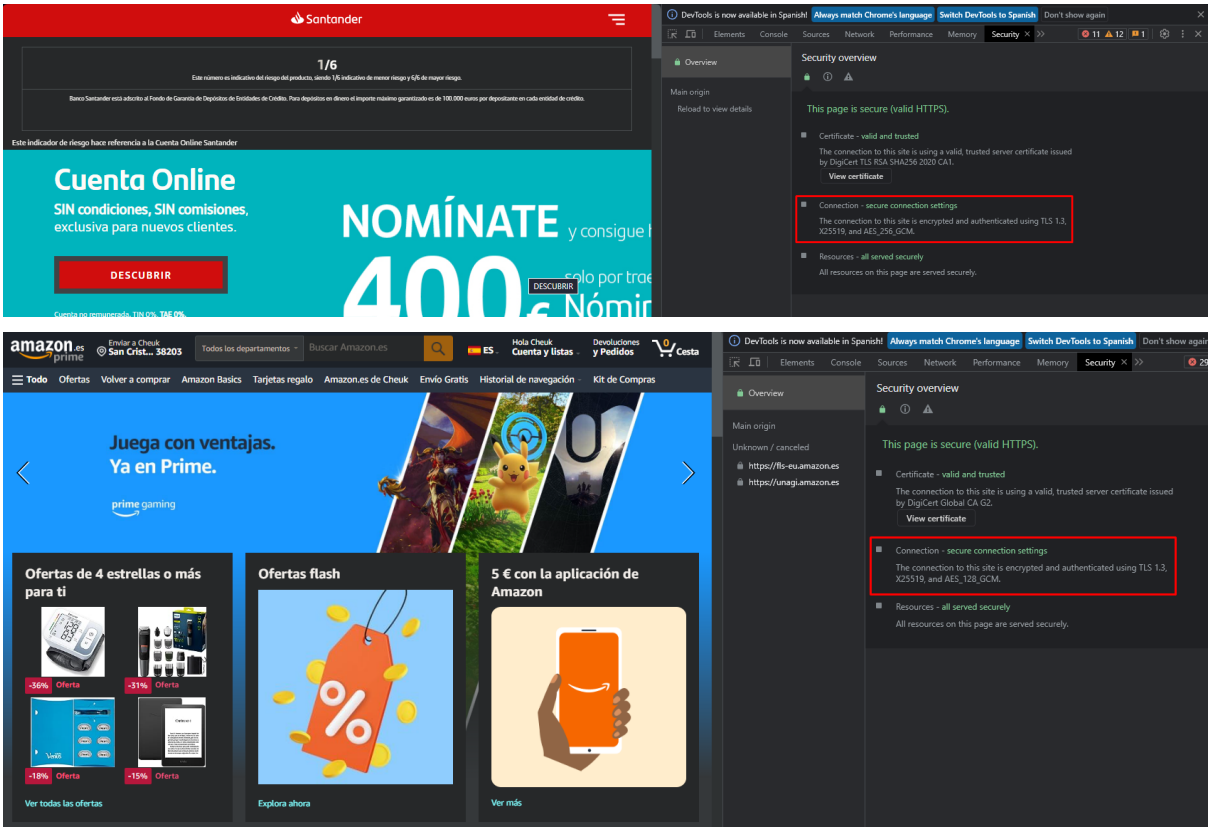


- Protocolo de cifrado: TLSv 1.3
- Algoritmo de intercambio de claves: x25519
- Algoritmo de cifrado: TLS_AES_128_GCM_SHA256
- Modo de cifrado: GCM

- Protocolo de cifrado: TLSv 1.2
- Algoritmo de intercambio de claves: P256
- Algoritmo de cifrado: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- Modo de cifrado: GCM

Ahora aquí en el navegador Firefox podemos observar diferencia hacia al navegador Microsoft Edge y al del navegador usado en el apartado anterior (Opera).

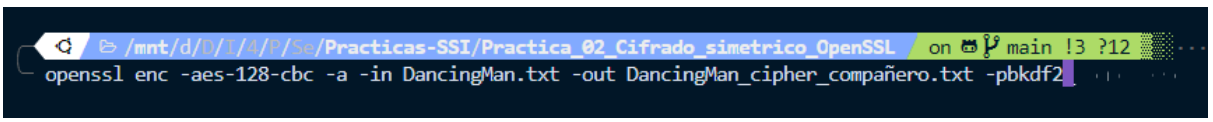
4.3. Busca otros sitios seguros y comprueba la configuración asociada a los esquemas de cifrado que se utilizan



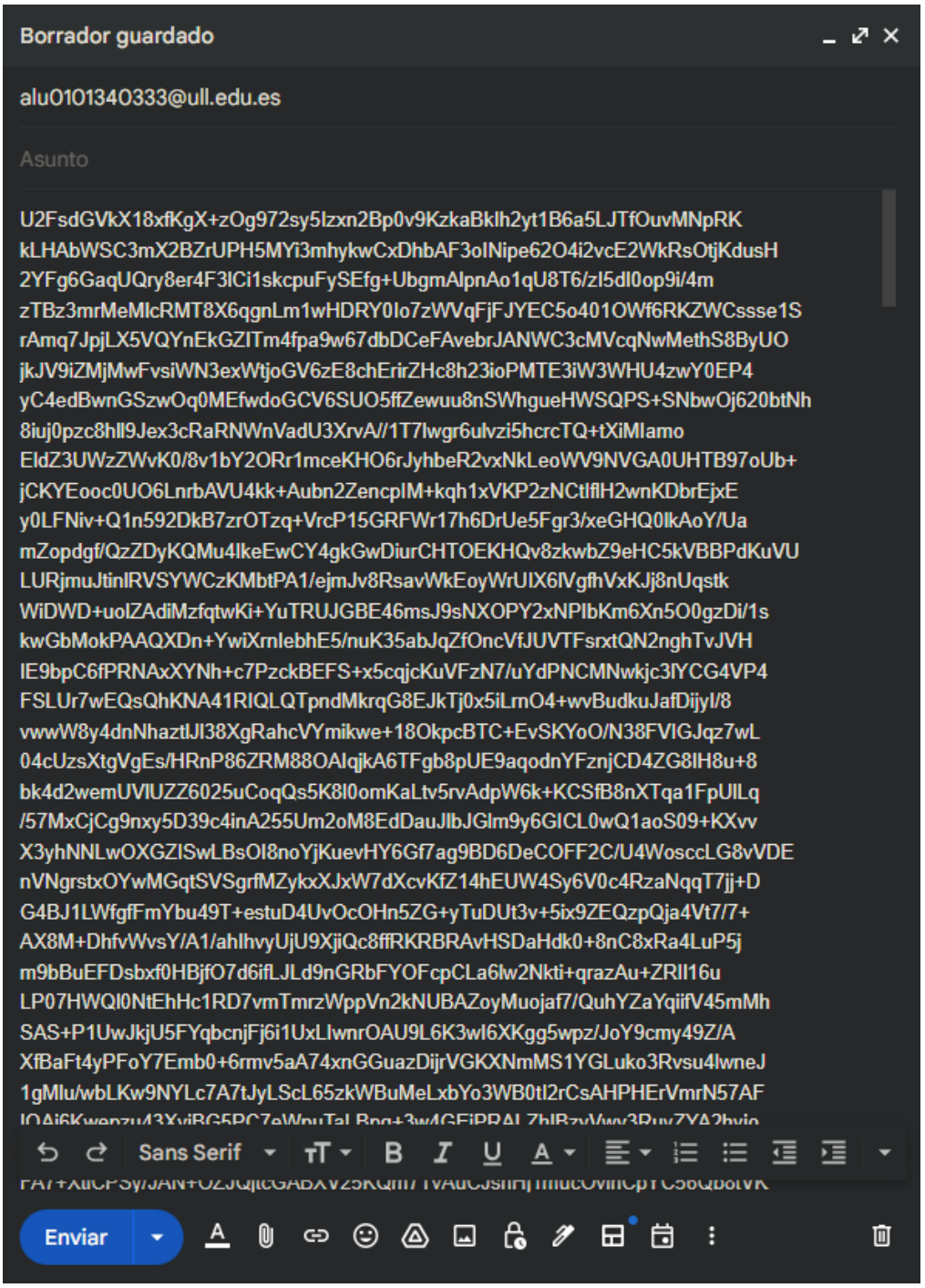
5. Prueba de correo electrónico

Para este ejercicio mi compañero y yo elegimos usar el algoritmo AES de 128 bits en modo CBC. Para cifrar el texto de Dancing Man hicimos lo siguiente:

```
Unset
openssl enc -aes-128-cbc -a -in DancingMan.txt -out crypted.txt
-pbkdf2
```



Aqui una captura de pantalla enviando el texto de DancingMan cifrado a través de Gmail:



Y por último recibo el texto cifrado por mi compañero y lo descifro usando el siguiente comando:

```
Unset
openssl enc -aes-128-cbc -a -d -in DancingMan_cipher.txt -out
decrypted.txt -pbkdf2
```

Con conocer la clave basta para descifrar el fichero, en mi caso, mi compañero y yo no tuvimos ningún problema al descifrar el DancingMan cifrado con el algoritmo AES de 128 bits en modo CBC.

6. Bibliografía.

https://openssl.cicei.com/index.php?title=Página_principal#Cifrado_en_bloqueGú
Apuntes OpenSSL Cifrado
Guión de la práctica 02 OpenSSL cifrado simétrico