



**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	2
2. Generación de un documento de texto y cifrar.	2
2.1. Cifrar con triple des EDE en modo cifrado ECB y CBC	2
2.2. Cifrar con AES 192 en modo cifrado ECB y CBC	3
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.	4
2.4. Haz el mismo análisis para las versiones de RC4 implementadas en OpenSSL.	5
3. Genera los parámetros necesarios para cifrar con el cifrado AES usando el modo CFB y una longitud de clave de 192.	5
4. Cifrado en HTTPs (estas conexiones usan TSL):	6
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?	6
4.2. Probar distintos navegadores (Firefox, IE, etc), ¿existen diferencias entre las especificaciones de cifrado?	7
4.3. Busca otros sitios seguros y comprueba la configuración asociada a los esquemas de cifrado que se utilizan	9
5. Prueba de correo electrónico	9
6. Bibliografía.	12



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:

```
on main l3 p7 .....  
openssl enc -des-ede3-ecb -a -in text.txt -out text_cipher_with_des-ede3-ecb.txt -pbkdf2  
enter DES-EDE3-ECB encryption password:  
Verifying - enter DES-EDE3-ECB encryption password:  
  
on main l3 p8 .....  
cat text_cipher_with_des-ede3-ecb.txt  
U2FsdGVkX19SeSIaVcPLowryfpH3WkrT5x8BqiUCG/bFPfaxzQ/Up4GdJiR9tV5z  
HfvIPm2VPFZ2mm9RF30KaGdpuz8GhFyH6f5Baxf+wGdD1S137v5GHk846PddEq  
2m1N0ZnaXfhgk6wp4M4d18pM157HokL002Ech6Q4YA4iDqYCD1uAw7co0xuJk/P  
8dfcrSgZYt7reYu0+Shi/BwRn8a0ERHfePs2XLvYUeH18JipZnALCY+j33R0F36w  
4ImrhfQXGn8d0Tsv0BqOVsUQkyESCnx+QVczkPpgt880vBmgiaHn6xDfmx56tKza  
N+SFA3dM4SLRgaiK0wOT08Rgydvjrb1Z7zWGRlac3/PeiaiMhUCw==  
  
on main l3 p8 .....  
openssl enc -des-ede3-ecb -d -a -in text_cipher_with_des-ede3-ecb.txt -out text_decipher_with_des-ede3-ecb.txt -pbkdf2  
enter DES-EDE3-ECB decryption password:  
  
on main l3 p9 .....  
cat text_decipher_with_des-ede3-ecb.txt  
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
```



- Cifrado con des-ede3-cbc:

```
➤ /mnt/d/ / / / / Practicas-SSI/Practica_02_Cifrado_simetrico_OpenSSL on main 13 75
openssl enc -des-ede3-cbc -a -in text.txt -out text_cipher_with_des-ede3-cbc.txt -pbkdf2
enter DES-EDE3-CBC encryption password:
Verifying - enter DES-EDE3-CBC encryption password:

➤ /mnt/d/ / / / / Practicas-SSI/Practica_02_Cifrado_simetrico_OpenSSL on main 13 75
cat text_cipher_with_des-ede3-cbc.txt
UZFsdGvKXl+4DLIZL0PP2BwyVFj0Uj9zyaA0b/4JInXvA0m4d2BjEfCb+bGH+XVh
AL9PztpdTqebFtSv02htvFvd2CnqSic15Dj8xTkywN6JFK+mod8W+sqLGx+Mt5q6
XR9TUpbck8Hs0/6iP3uKhMhB52r1oP4k75Qd89APag00/tUDEtJ4wFOyAlD0Btxy
Yh4w/34itdac7RKhdZGwTtbReRGe+KRZOZAT+1MhNE+pmZsmJf79fzRzW8Nfyn+D
6P/Ed7hCxsglyKd0J7WtBVitb4JJ4Dz/RGhMmK78vVK9NhT5ECT1A2XEM+OnN6+x
QJASySorJ00oaAzJQY7GgtDYwVHjeb3pnmorv/QTxwJzgkVLHzZQ==

➤ /mnt/d/ / / / / Practicas-SSI/Practica_02_Cifrado_simetrico_OpenSSL on main 13 75
openssl enc -des-ede3-cbc -d -in text_cipher_with_des-ede3-cbc.txt -out text_decipher_with_des-ede3-cbc.txt -pbkdf2
enter DES-EDE3-CBC decryption password:
bad magic number

➤ /mnt/d/ / / / / Practicas-SSI/Practica_02_Cifrado_simetrico_OpenSSL on main 13 75
openssl enc -des-ede3-cbc -d -a -in text_cipher_with_des-ede3-cbc.txt -out text_decipher_with_des-ed
e3-cbc.txt -pbkdf2
enter DES-EDE3-CBC decryption password:

➤ /mnt/d/ / / / / Practicas-SSI/Practica_02_Cifrado_simetrico_OpenSSL on main 13 75
cat text_decipher_with_des-ede3-cbc.txt
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 com en el AMD
perdona nuestros Windows
así como nosotros perdonamos a los que lo usan
y libranos de Bill Gates
exit
```

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

- Cifrado con aes-192-ecb:

```
➤ /mnt/d/ / / / / Practicas-SSI/Practica_02_Cifrado_simetrico_OpenSSL on main 13 75
openssl enc -aes-192-ecb -a -in text.txt -out text_cipher_with_aes-192-ecb.txt -pbkdf2
enter AES-192-ECB encryption password:
Verifying - enter AES-192-ECB encryption password:

➤ /mnt/d/ / / / / Practicas-SSI/Practica_02_Cifrado_simetrico_OpenSSL on main 13 76
cat text_cipher_with_aes-192-ecb.txt
UZFsdGvKXl8EULnVs5otV9TIhhqrQn/57hs7XwagT3Z2/0DorK48CjJEvcw7BwCf
Cy7vhywy110oQ2EP4zv01rQkZB5Fwss/Z6rZX47HtUA06YXwomFPIYqIPDgQbNBc
OXW3F2gjhucUA0/quJ4mnXr-Ez3gmjTNptF3kmmjjAdJy8JGCC4VywU/B0FLt0kL1
KqcbxQVgZQwnzsgRho0q09NsanAsoJUamzGj5tCntQkwecJcJezT2H1sdEISBG5
xh+oC0204R+KMYd5IqyVMia3KgoGdaXwU8opk1iIgJB/1YulF2xjJ+k7pseGZ1Ao
MttlguhEdGEDJbmXSHgFj1H4WqVvCkZhQmQP4cDb9Y7SblFYBhGw/Ntz71PaMI

➤ /mnt/d/ / / / / Practicas-SSI/Practica_02_Cifrado_simetrico_OpenSSL on main 13 76
openssl enc -aes-192-ecb -d -a -in text_cipher_with_aes-192-ecb.txt -out text_decipher_with_aes-192-ecb.txt -pbkdf2
enter AES-192-ECB decryption password:

➤ /mnt/d/ / / / / Practicas-SSI/Practica_02_Cifrado_simetrico_OpenSSL on main 13 77
cat text_decipher_with_aes-192-ecb.txt
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 com en el AMD
perdona nuestros Windows
así como nosotros perdonamos a los que lo usan
y libranos de Bill Gates
exit
```



- Cifrado con aes-192-cbc:

```
└─$ openssl enc -aes-192-cbc -a -in text.txt -out text_cipher_with_aes-192-cbc.txt -pbkdf2
enter AES-192-CBC encryption password:
Verifying - enter AES-192-CBC encryption password:

└─$ cat text_cipher_with_aes-192-cbc.txt
U2FsdGVkX19mkdJVdU0SxwXmx8wPNzx+46UXDpB4P5kZ3pUFLqEjcn2PJ050n2mA
rpZcyYrlylmMA7GJ1EygodBd2vuJJdBSgcQLjPHn3Q4WfEdTq7SEMo6IxTTIXndC
CdguaDdpNzG6foPiGnb9S95p+bZ/IZeBoNvPbZMJUfN8U6GdASQsRlWxbDqzphg0
UMg06pTDrs2UxJtWjOWRWCniAyggaCNAqR2gTUMCiHec5q9fjBwtvR1P0LcJWlaSa
d+nltYpdjgsNfAuia8E0tev9XcRzTIW30qzWK6cqBqv1SB1HVBzPpHP8pVmAS2NX
3IF0UihJNa86NBwXntF1SDv58m9UwMQ1yrWwTynL044PYUheZbMpbhQprVZ3dHjS

└─$ openssl enc -aes-192-cbc -d -a -in text_cipher_with_aes-192-cbc.txt -out text_decipher_with_aes-192-cbc.txt -pbkdf2
enter AES-192-CBC decryption password:

└─$ cat text_decipher_with_aes-192-cbc.txt
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 com en el AMD
perdona nuestros Windows
así como nosotros perdonamos a los que lo usan
y libranos de Bill Gates
exit
```

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
```

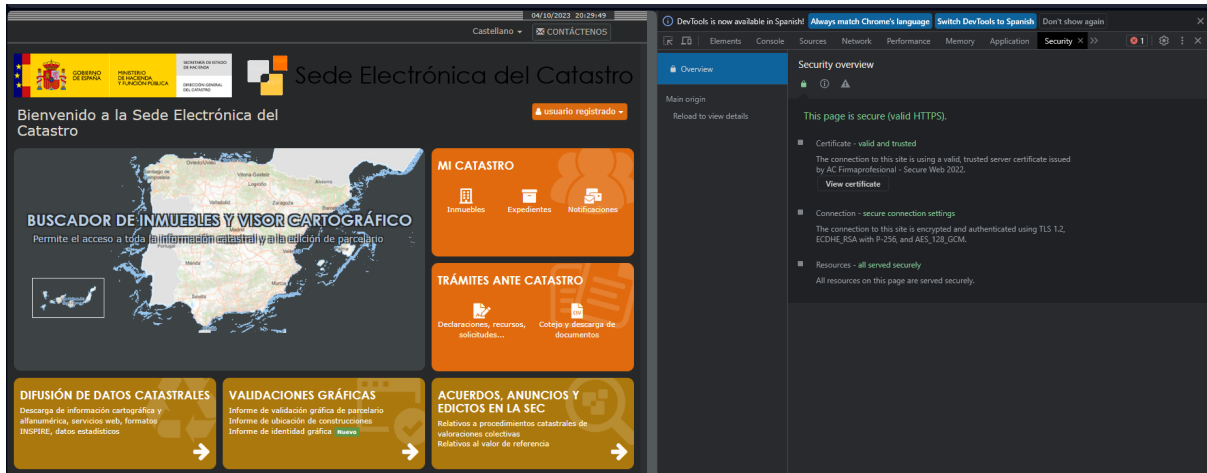
Este comando descifrará el contenido del archivo `encrypted.txt` y lo guardará en el archivo `decrypted.txt`.

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

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?

The screenshot shows a web browser window with the 'Sede electrónica' page. The page has a blue header with the text 'Sede electrónica' and a navigation bar with icons for 'Buscar Trámites', 'Mis expedientes', 'Mis notificaciones', 'Convocatorias próximas al cierre', 'Ayuda', and 'Verificación de CSV'. Below the navigation bar, there are two sections: 'Campanías' and 'Trámites destacados'. The 'Campanías' section lists several campaigns related to the validation of modules of the degree courses of medium and higher grade of the Artistic and Design cycles. The 'Trámites destacados' section lists several procedures related to the homologation and validation of foreign titles and studies. On the right side of the browser window, the Chrome DevTools 'Security' tab is open, showing the 'Security overview' for the current page. The overview indicates that the page is secure (valid HTTPS) and provides details about the certificate, connection, and resources.

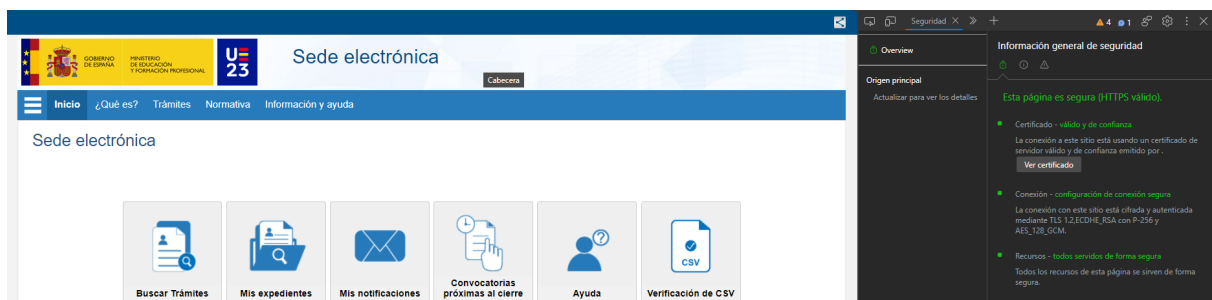
- Protocolo de cifrado: TLS 1.2
- Algoritmo de intercambio de claves: ECDHE_RSA
- Algoritmo de cifrado: AES-128-GCM
- Modo de cifrado: GCM



- 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?

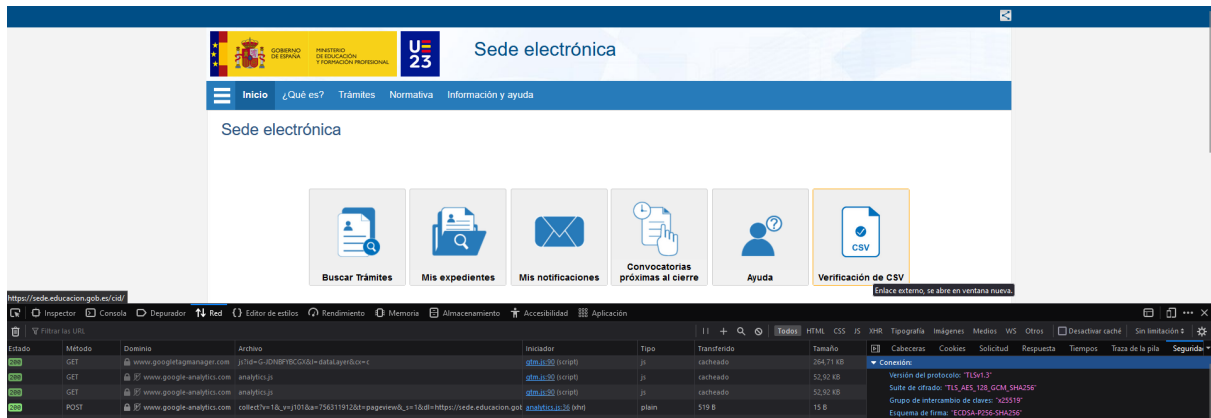
- Desde navegador Microsoft Edge:



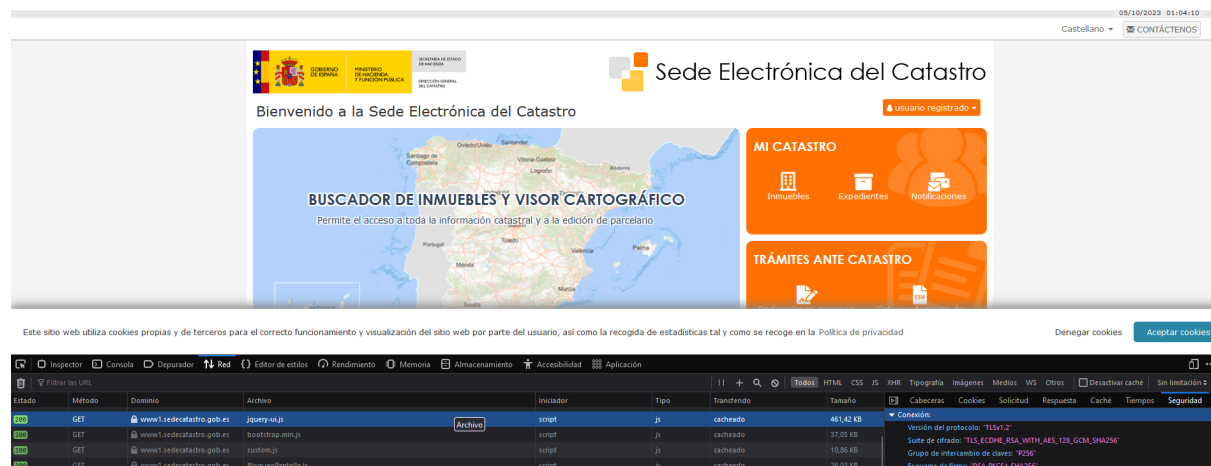


Podemos observar que desde la página de la sede de educación y la sede electrónica del catastro no ha cambiado nada con el navegador Microsoft Edge.

- 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

The top screenshot shows the Santander website. The security overview panel on the right indicates: 'This page is secure (valid HTTPS). Certificate - valid and trusted. The connection to this site is using a valid, trusted server certificate issued by DigiCert TLS RSA SHA256 2020 CA1. View certificate. Connection - secure connection settings. The connection to this site is encrypted and authenticated using TLS 1.3, X25519, and AES-256_GCM. Resources - all served securely. All resources on this page are served securely.'

The bottom screenshot shows the Amazon.es website. The security overview panel on the right indicates: 'This page is secure (valid HTTPS). Certificate - valid and trusted. The connection to this site is using a valid, trusted server certificate issued by DigiCert Global CA G2. View certificate. Connection - secure connection settings. The connection to this site is encrypted and authenticated using TLS 1.3, X25519, and AES-128_GCM. Resources - all served securely. All resources on this page are served securely.'

5. Prueba de correo electrónico

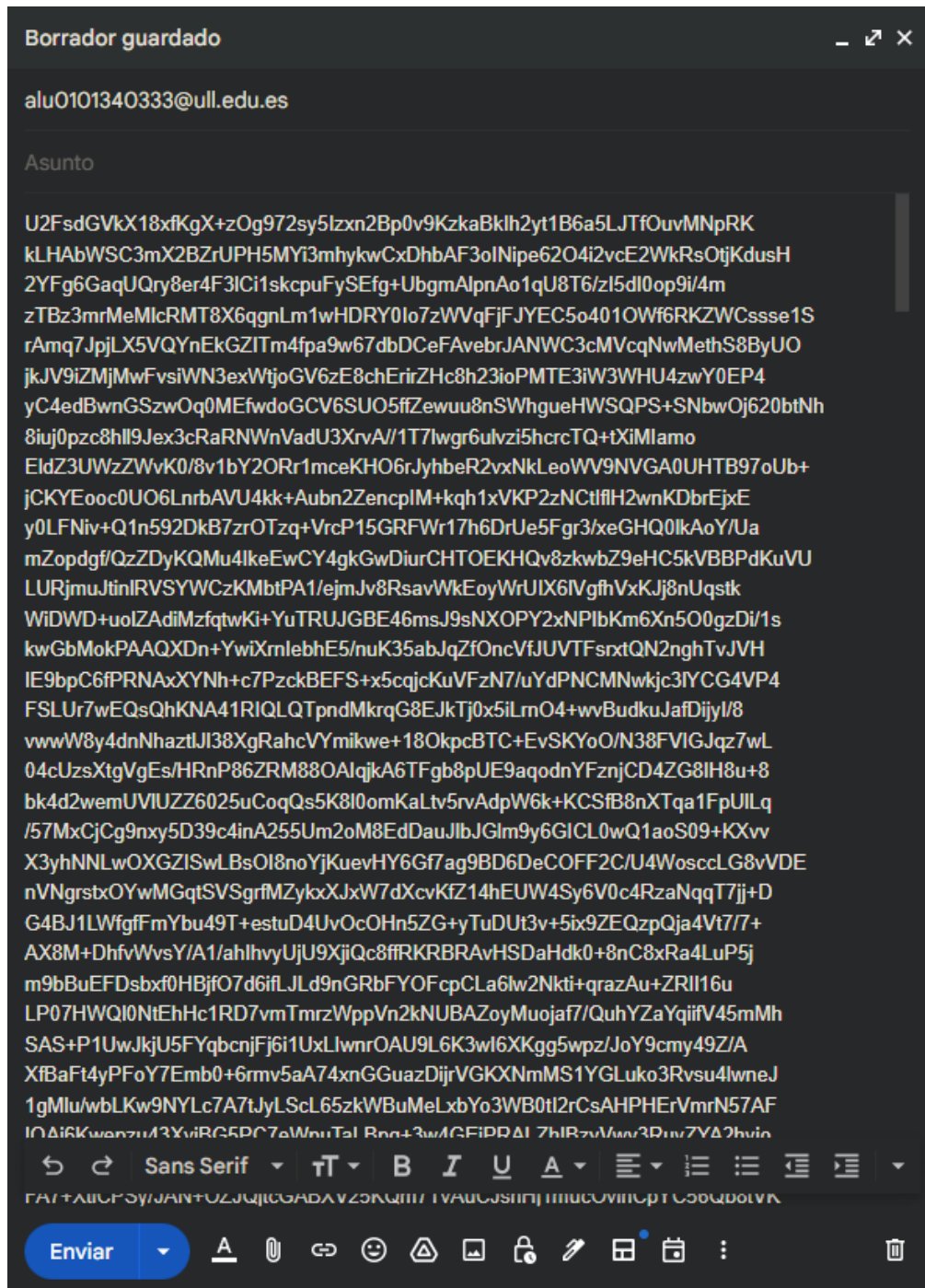
Para este ejercicio mi compañero y yo elegimos usar el algoritmo AES de 128 bits en modo CBC. Para cifrar el texto de Dancing Man hicimos lo siguiente:

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

```
on main !3 ?12  
openssl enc -aes-128-cbc -a -in DancingMan.txt -out DancingMan_cipher_compañero.txt -pbkdf2
```



Aquí 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
```

```
on P main !3 ?10
touch DancingMan_cipher_compañero.txt
on P main !3 ?11
vi DancingMan_cipher_compañero.txt
on P main !3 ?11
openssl enc -aes-128-cbc -d -a -in DancingMan_cipher_compañero.txt -out DancingMan_decipher_compañero.txt -pbkdf2
enter AES-128-CBC decryption password:
on P main !3 ?12
cat DancingMan_decipher_compañero.txt
Holmes had been seated for some hours in silence with his long, thin back curved over a chemical vessel in which he was brewing a particularly malodorous product. His head was sunk upon his breast, and he looked from my point of view like a strange, lank bird, with dull gray plumage and a black top-knot. "So, Watson," said he, suddenly, "you do not propose to invest in South African securities?" I gave a start of astonishment. Accustomed as I was to Holmes's curious faculties, this sudden intrusion into my most intimate thoughts was utterly inexplicable. "How on earth do you know that?" I asked. He wheeled round upon his stool, with a steaming test-tube in his hand, and a gleam of amusement in his deep-set eyes. "Now, Watson, confess yourself utterly taken aback," said he. "I am." "I ought to make you sign a paper to that effect." "Why?" "Because in five minutes you will say that it is all so absurdly simple." "I am sure that I shall say nothing of the kind." "You see, my dear Watson"-he propped his test-tube in the rack, and began to lecture with the air of a professor addressing his class-"it is not really difficult to construct a series of inferences, each dependent upon its predecessor and each simple in itself. If, after doing so, one simply knocks out all the central inferences and presents one's audience with the starting-point and the conclusion, one may produce a startling, though possibly a meretricious, effect. Now, it was not really difficult, by an inspection of the groove between your left forefinger and thumb, to feel sure that you did not propose to invest your small capital in the gold fields." "I see no connection." "Very likely not; but I can quickly show you a close connection. Here are the missing links of the very simple chain: 1. You had chalk between your left finger and thumb when you returned from the club last night. 2. You put chalk there when you play billiards, to steady the cue. 3. You never play billiards except with Thurston. 4. You told me, four weeks ago, that Thurston had an option on some South African property which would expire in a month, and which he desired you to share with him. 5. Your check book is locked in my drawer, and you have not asked for the key. 6. You do not propose to invest your money in this manner." "How absurdly simple!" I cried. "Quite so!" said he, a little nettled. "Every problem becomes very childish when once it is explained to you. Here is an unexplained one. See what you can make of that, friend Watson." He tossed a sheet of paper upon the table, and turned once more to his chemical analysis. I looked with amazement at the absurd hieroglyphics upon the paper. "Why, Holmes, it is a child's drawing," I cried. "Oh, that's your idea!" "What else should it be?" "That is what Mr. Hilton Cubitt, of Riding Thorpe Manor, Norfolk, is very anxious to know. This little conundrum came by the first post, and he was to follow by the next train. There's a ring at the bell, Watson. I should not be very much surprised if this were he." A heavy step was heard upon the stairs, and an instant later there entered a tall, ruddy, clean-shaven gentleman, whose clear eyes and florid cheeks told of a life led far from the fogs of Baker Street. He seemed to bring a whiff of his strong, fresh, bracing, east-coast air with him as he entered. Having shaken hands with each of us, he was about to sit down, when his eye rested upon the paper with the curious markings, which I had just examined and left upon the table. "Well, Mr. Holmes, what do you make of these?" he cried. "They told me that you were fond of queer mysteries, and I don't think you can find a queerer one than that. I sent the paper on ahead, so that you might have time to study it before I came." "It is certainly rather a curious production," said Holmes. "At first sight it would appear to be some childish prank. It consists of a number of absurd little figures dancing across the paper upon which they are drawn. Why should you attribute any importance to so grotesque an object?" "I never should, Mr. Holmes. But my wife does. It is frightening her to death. She says nothing, but I can see terror in her eyes. That's why I want to sift the matter to the bottom."
```

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_bloqueGu

Apuntes OpenSSL Cifrado

Guión de la práctica 02 OpenSSL cifrado simétrico