**Universidad Nacional Autónoma de Nicaragua**

**UNAN-León**

**Facultad de Ciencias y Tecnología**

**Departamento de Computación**

**Ingeniería en Telemática**

**V año**

****

**Componente: Laboratorio de Seguridad de Redes**

**Tema: Cifrado con OpenSSL**

**Realizado por:**

**Br. Jhonatan Uziel Espinoza Ortega Carnet: 15-00737-0**

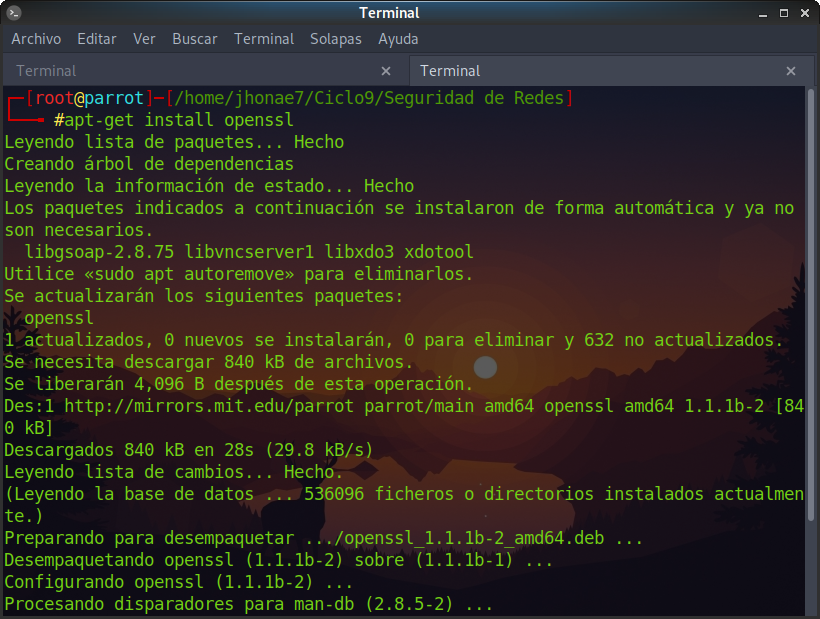
**Dirigido a:**

**MSc. Aldo Martinez**

**León, Nicaragua lunes 8 de julio del 2019.**

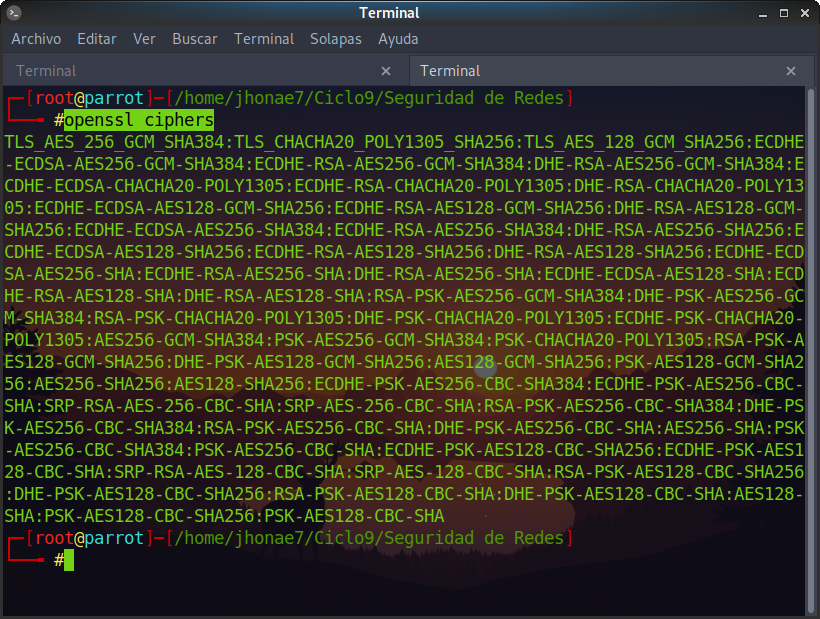
**Cifrado con OpenSSL**

**1. Instalar OpenSSL**



**2. Utilizacion de algoritmos simetricos**

**2.1 Comando ciphers**

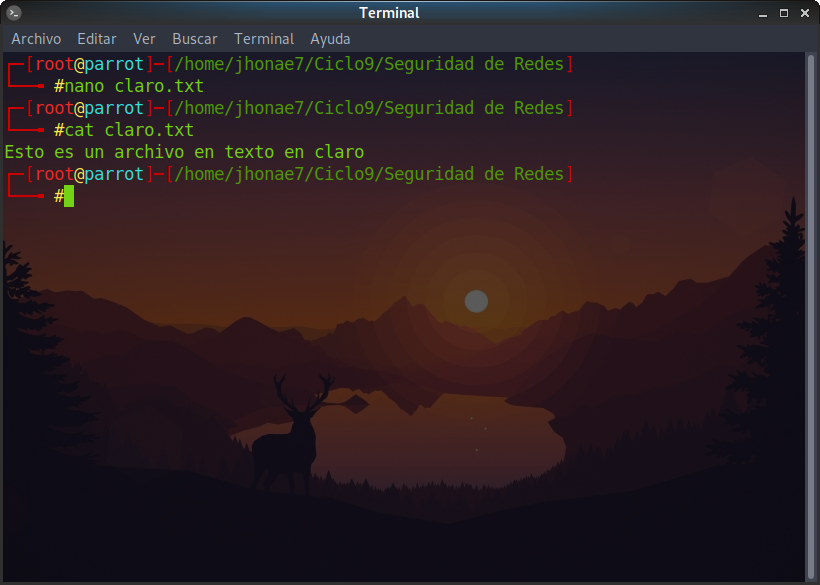
Para comprobar la lista de algoritmos simetricos soportados ejecutar:

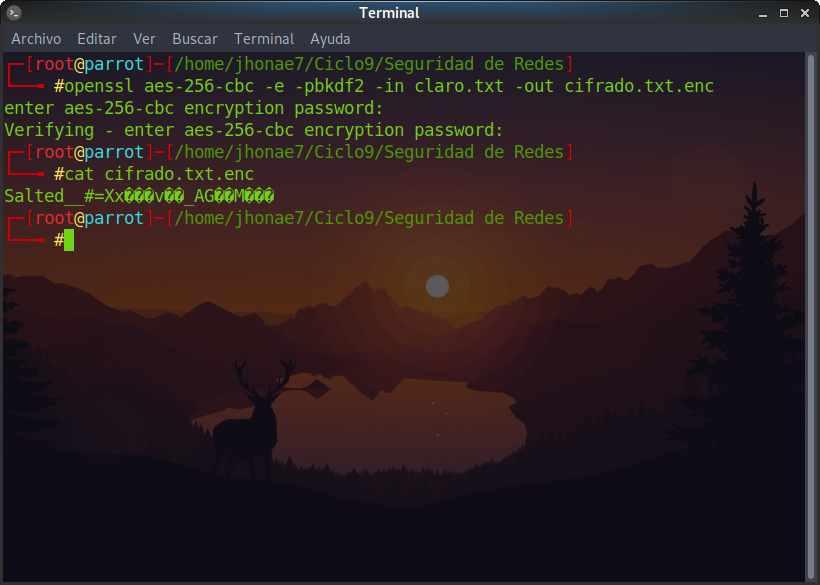
**2.2 Cifrar un mensaje de prueba**

Seguir los siguientes pasos para crear un documento de texto cifrado con openssl.

- Mirar en la documentacion de OpenSSL como se utiliza el comando enc para cifrar y descifrar.

- Crear un archivo de texto

- Cifrarlo con un algoritmo simetrico

Donde:

\* aes-256-cbc: indica que se usa el algoritmo aes con un tamaño de clave de 256 bits y el modo de cifrado de bloque (la secuencia de bits se encripta como una sola unidad o bloque con una clave de cifrado

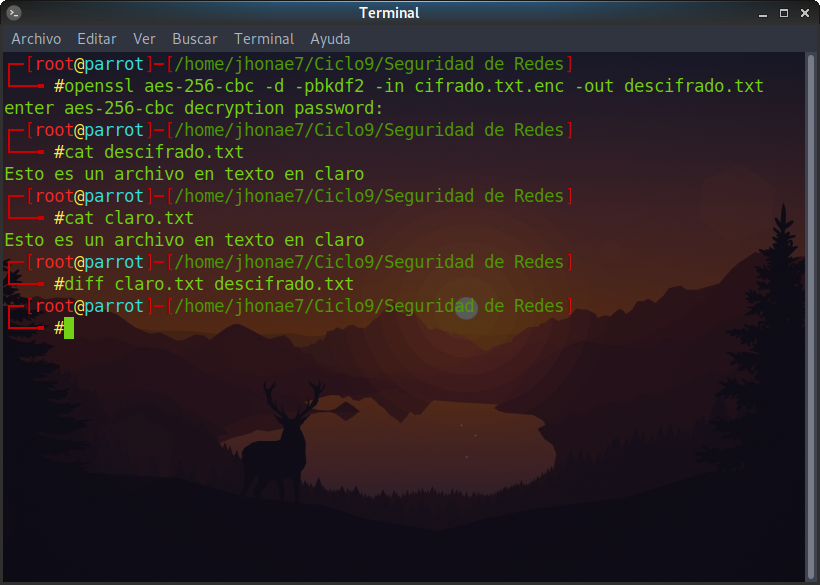
\* e: con este parametro se indica que la operación a realizar es de cifrado

\* pbkdf2: funcion de derivacion de clave que se utiliza para reducir la vulnerabilidad a ataques de fuerza bruta.

\* in: para indicar los datos que seran cifrados

\* out: para indicar el archivo donde se guardaran los datos cifrados

- Descifrarlo y comprobar el resultado



Donde:

\* aes-256-cbc: indica que se usa el algoritmo aes con un tamaño de clave de 256 bits y el modo de cifrado de bloque (la secuencia de bits se encripta como una sola unidad o bloque con una clave de cifrado

\* d: con este parametro se indica que la operación a realizar es de descrifrado

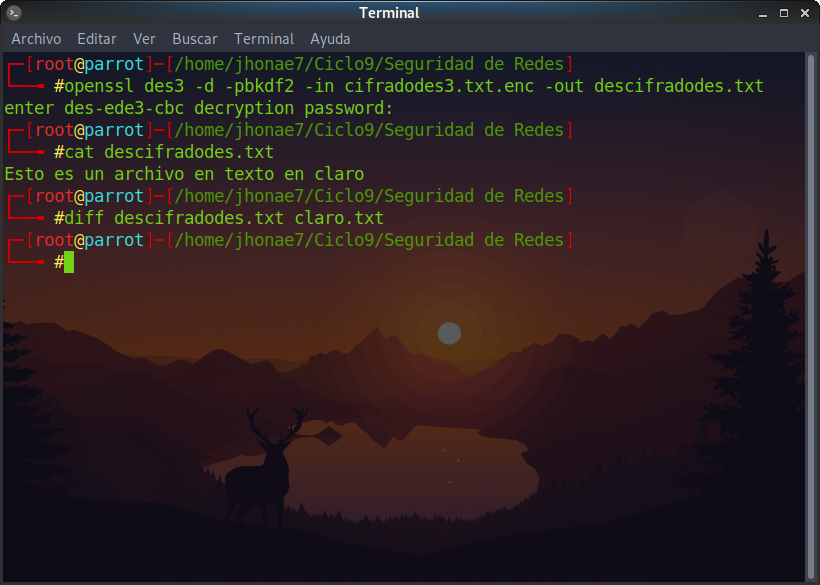
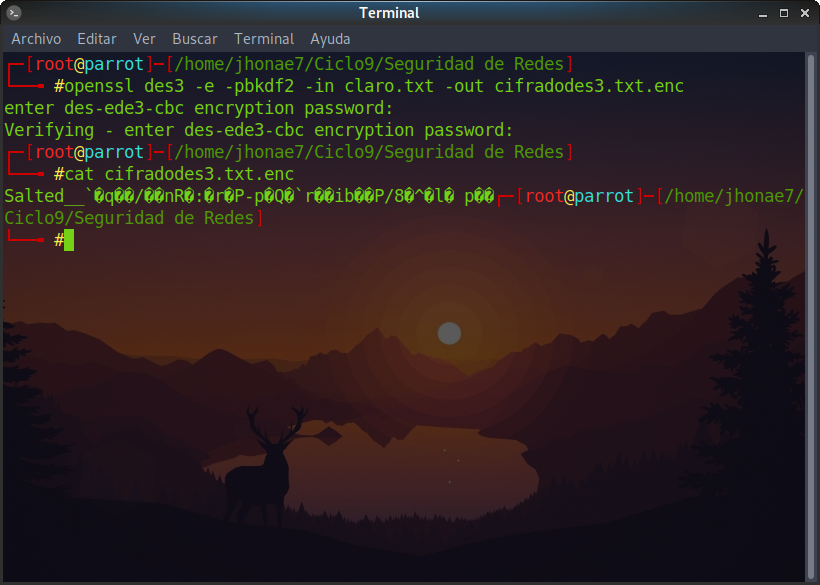
\* pbkdf2: funcion de derivacion de clave que se utiliza para reducir la vulnerabilidad a ataques de fuerza bruta.

\* in: para indicar los datos que seran descrifrados

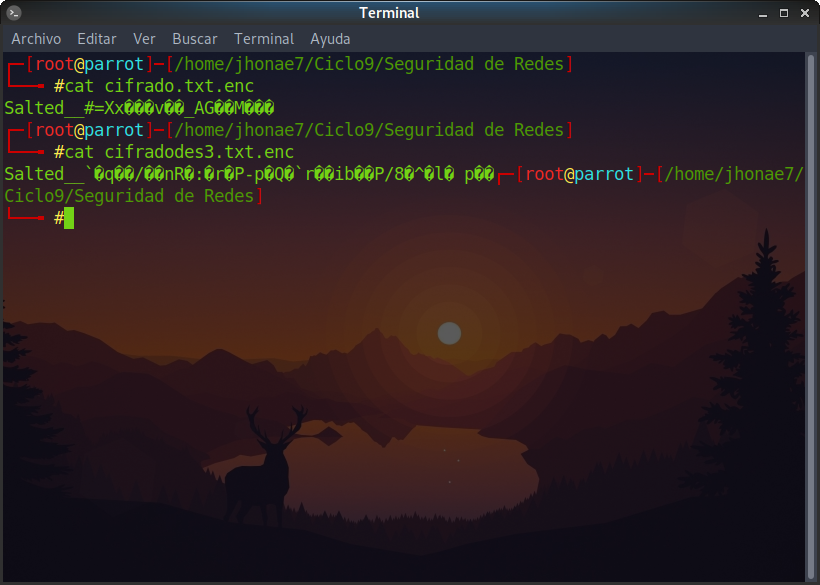
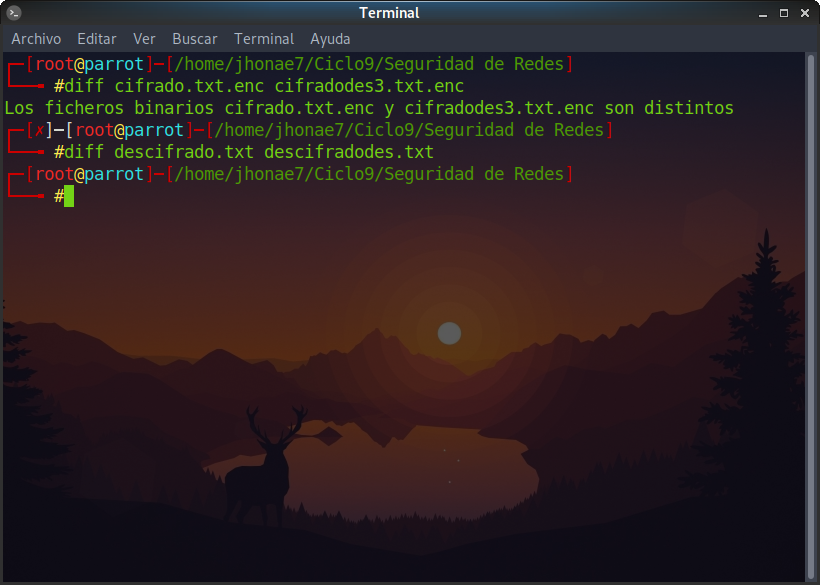
\* out: para indicar el archivo donde se guardaran los datos descifrados

- Analizar el comportamiento para diferentes longitudes de mensaje y diferentes algoritmos de cifrado.

Mismo archivo “claro.txt” ahora con des3



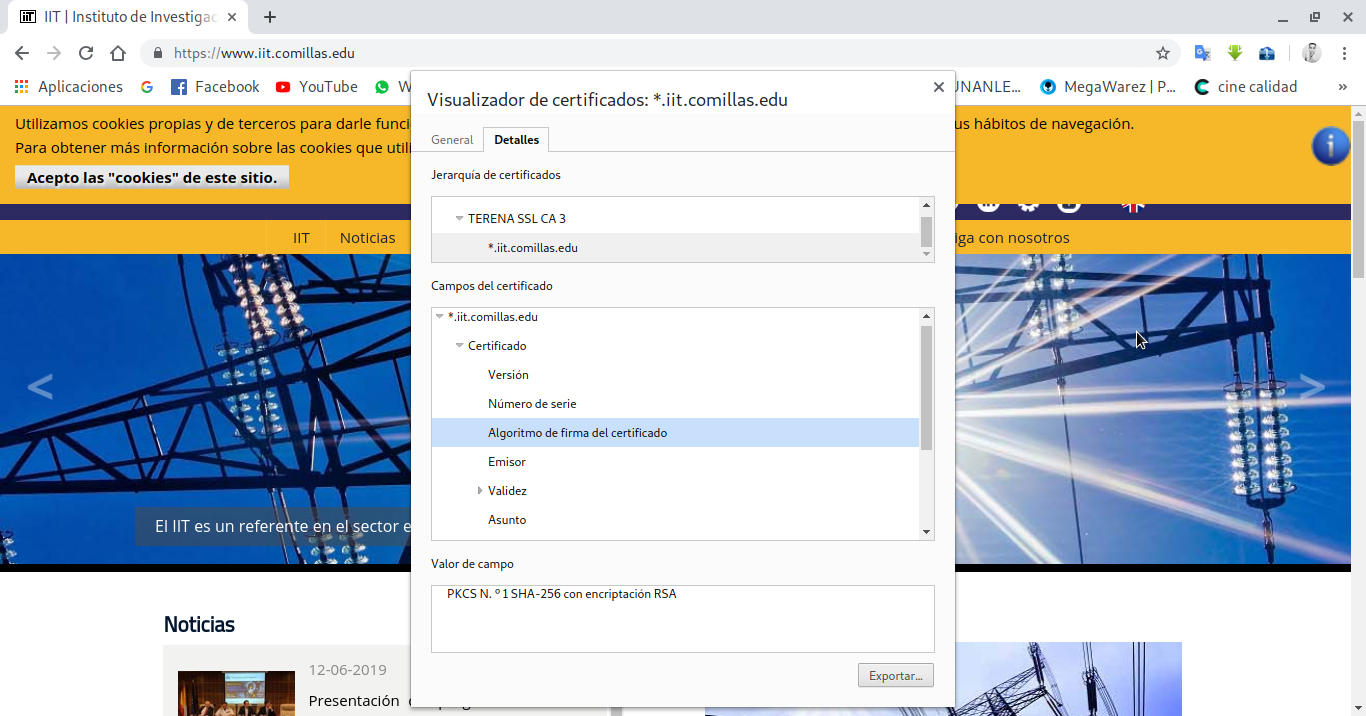
Diferencias en los ficheros encriptados



**3. Cifrado en HTTPs**

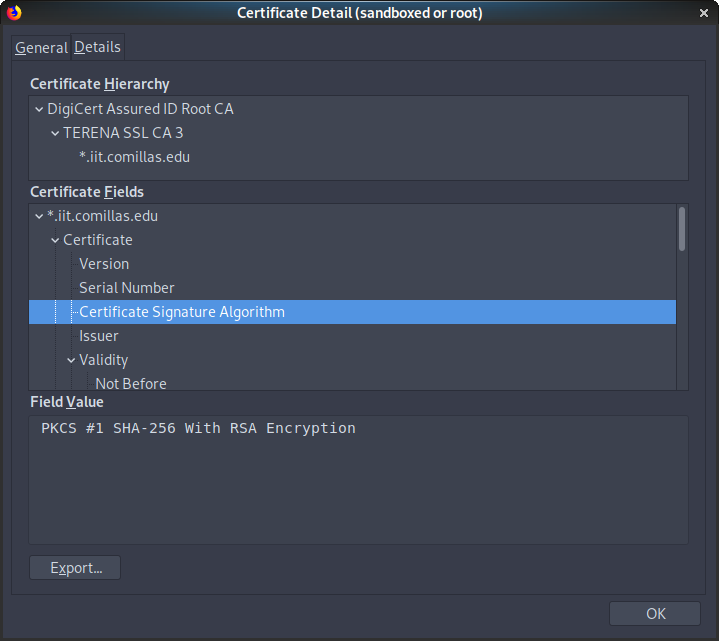
- Acceder a la página https://www.iit.upcomillas.es/

- ¿qué algoritmo simétrico se utiliza para conexión?

- Probar distintos navegadores (Firefox, IE, Safari…)

**Google Chrome**

**Moxilla Firefox**

****

- Acceder a la página https://www.upcomillas.es/

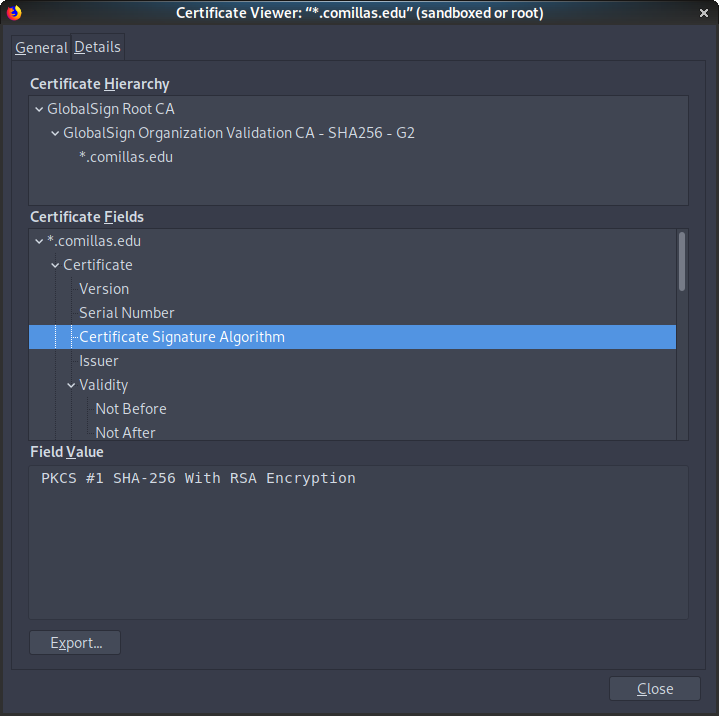
- ¿qué algoritmo simétrico se utiliza para conexión?

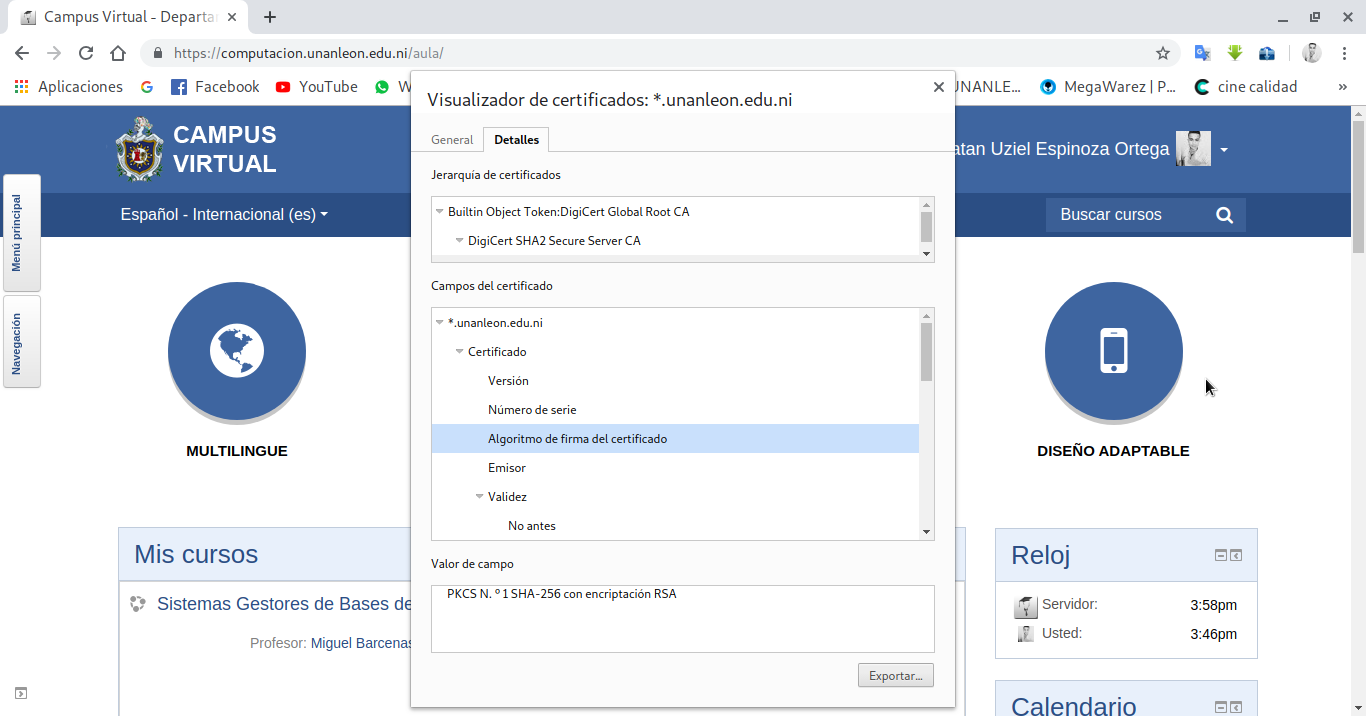
- Probar distintos navegadores (Firefox, IE, Safari…)

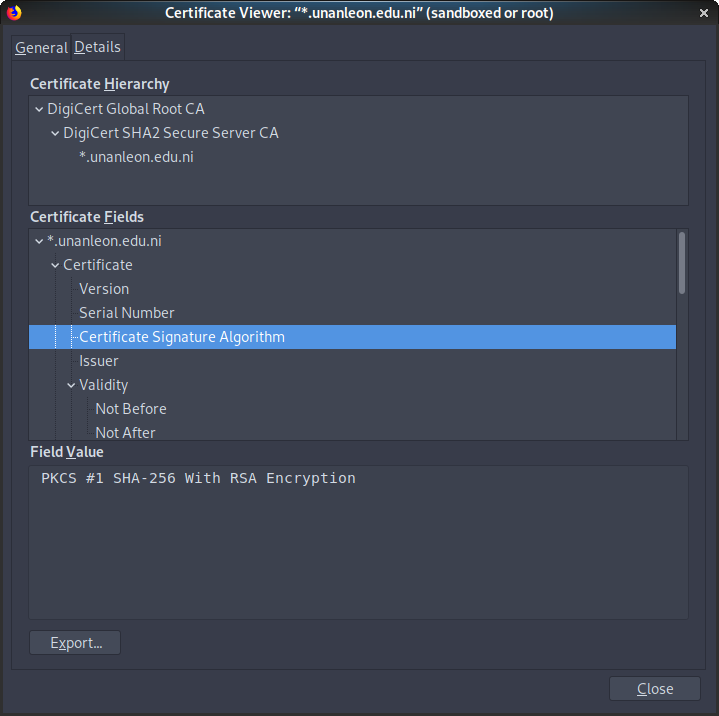
**Google Chrome**



**Mozilla Firefox**





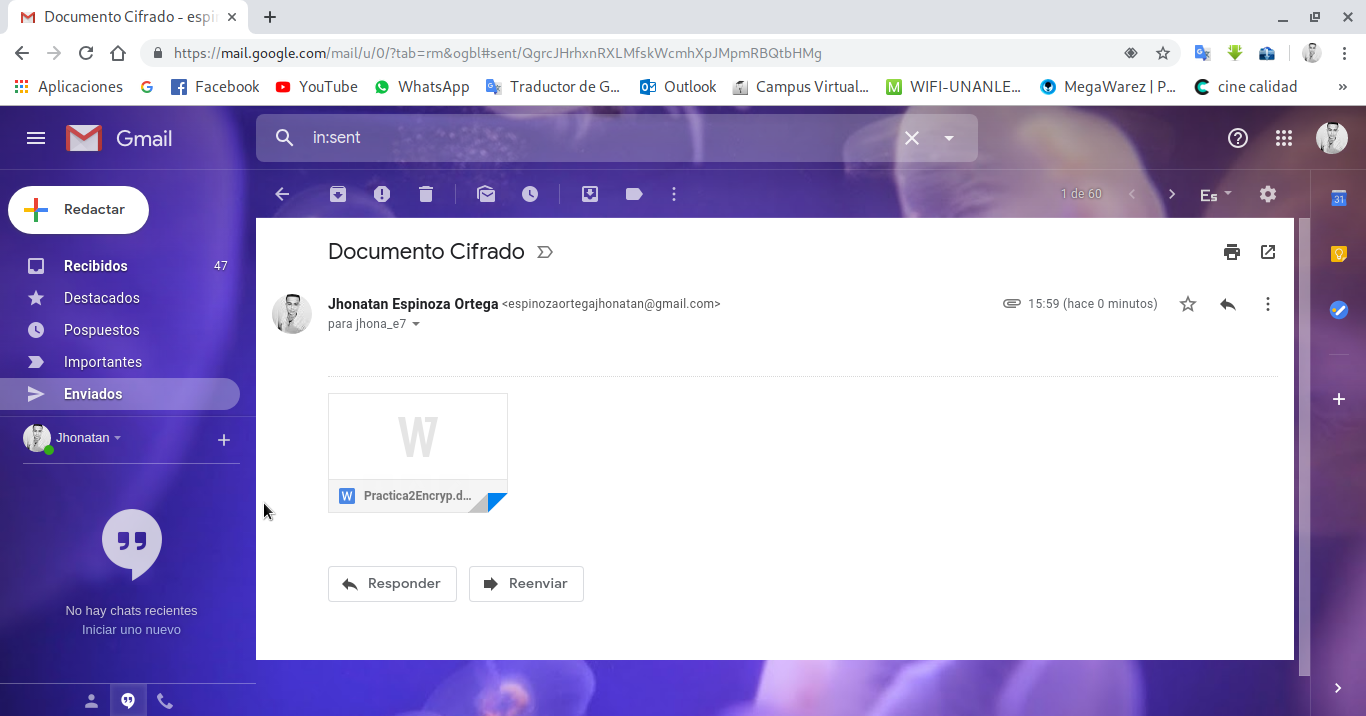


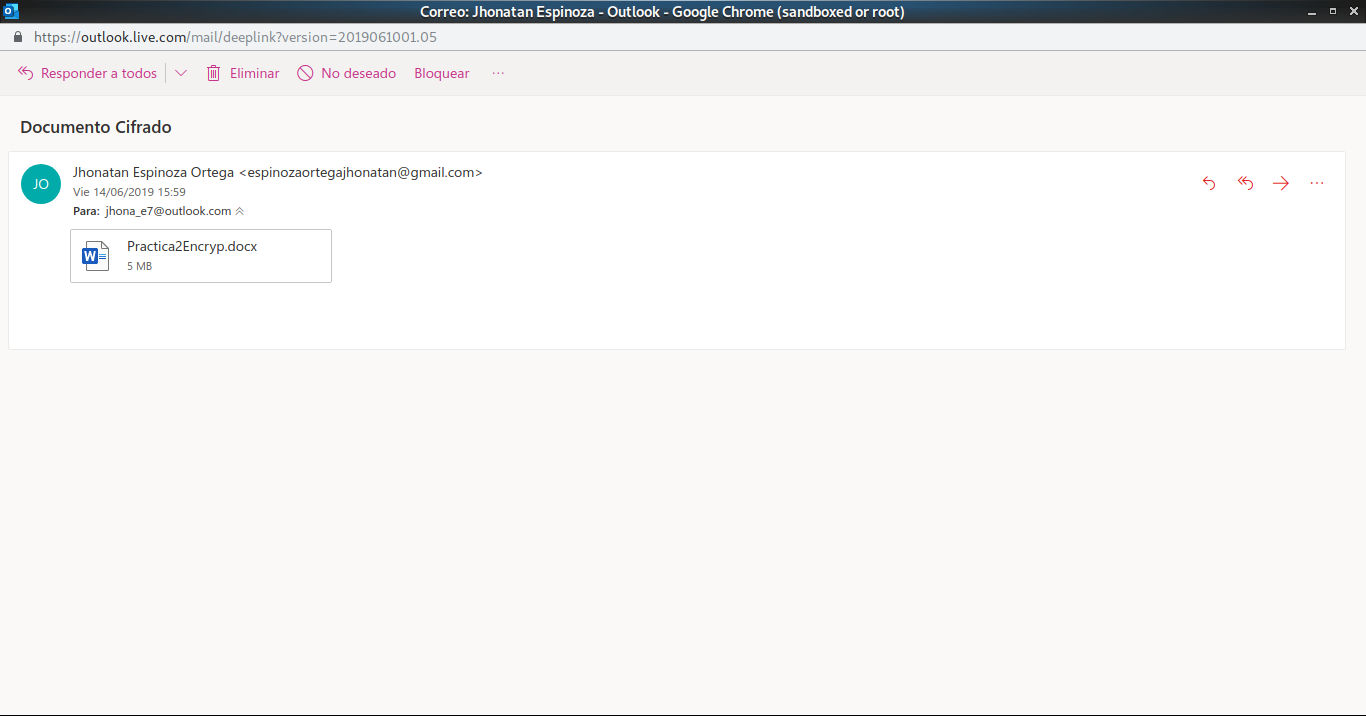
**4. Prueba de Correo Electronico**

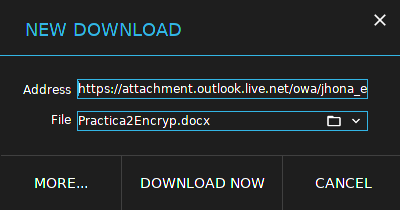
- Cifrar documentos con comandos openssl

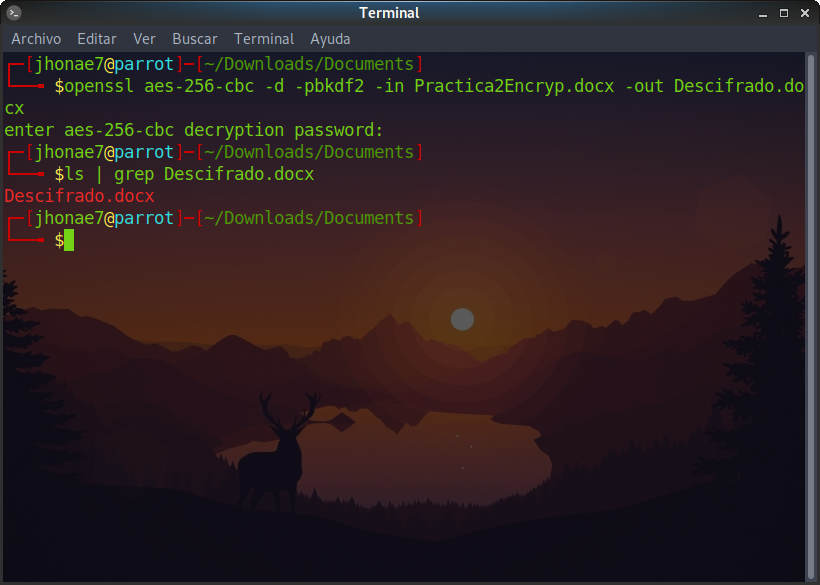


- Enviar el documento cifrado por correo electronico







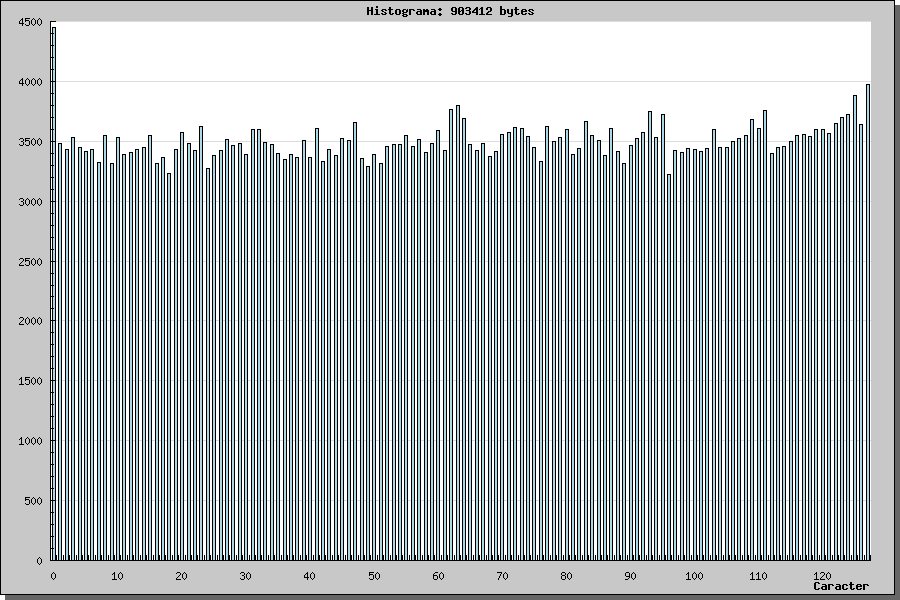


**5. Analisis por histograma**

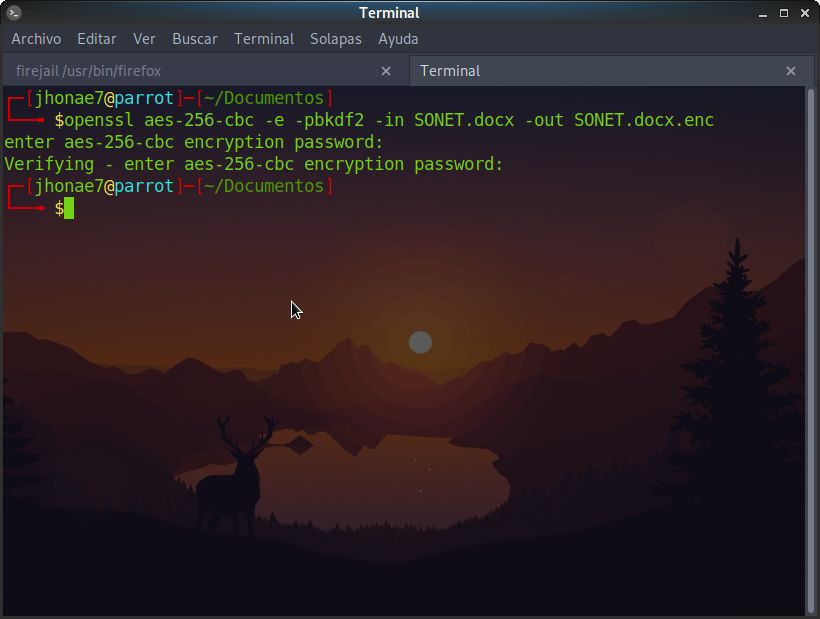
El histograma de un fichero representa, mediante un gráfico de barras, la frecuencia de repetición de cada carácter del fichero.

Utilizar la página http://www.iit.upcomillas.es/palacios/seguridad/histograma/ para obtener vía web el histograma de cualquier fichero, y hacer pruebas con los siguientes tipos de fichero:

Fichero de texto (ejemplo correo electrónico o documento word)

 El mismo fichero pero comprimido

El mismo fichero pero cifrado con AES (utilizar openssl)



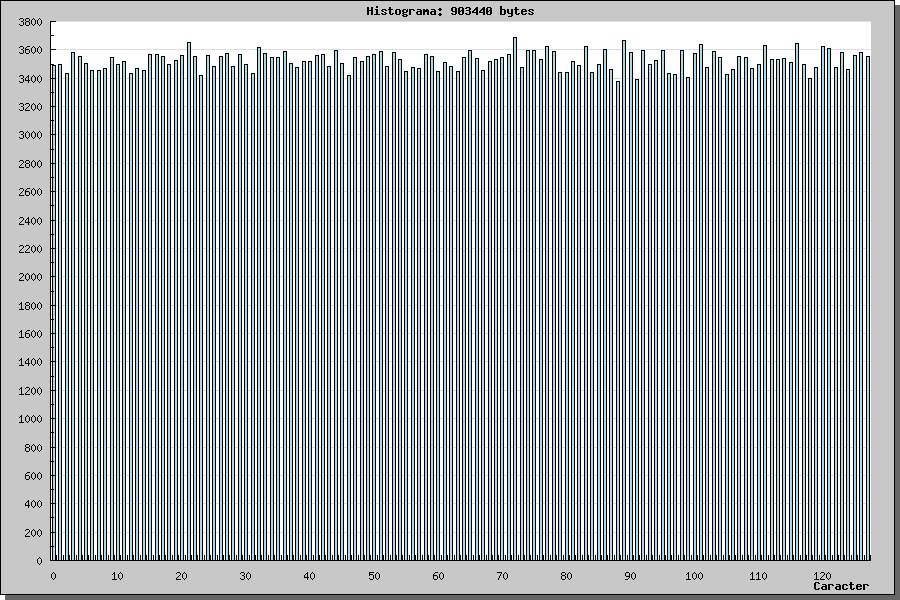
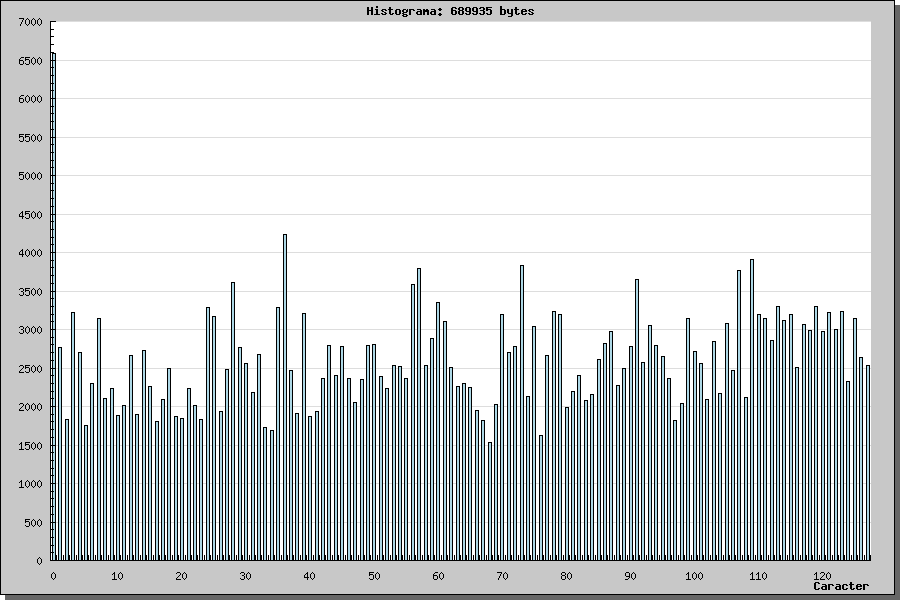


Imagen JPEG



Fichero aleatorio generado mediante openssl con el comando rand

**5.1 Tamaño de ficheros**

Anotar el tamaño origininal de un fichero y el tamaño resultante de:

- Cifrar

- Comprimir

- Cifrar + comprimir

- Comprimir + cifrar

Tamaño: 11.0 kb

Cifrar: 11.1 kb

Comprimir: 10.5 kb

Cifrar + Comprimir: 11.2 kb

Comprimir + Cifrar: 10.6 kb