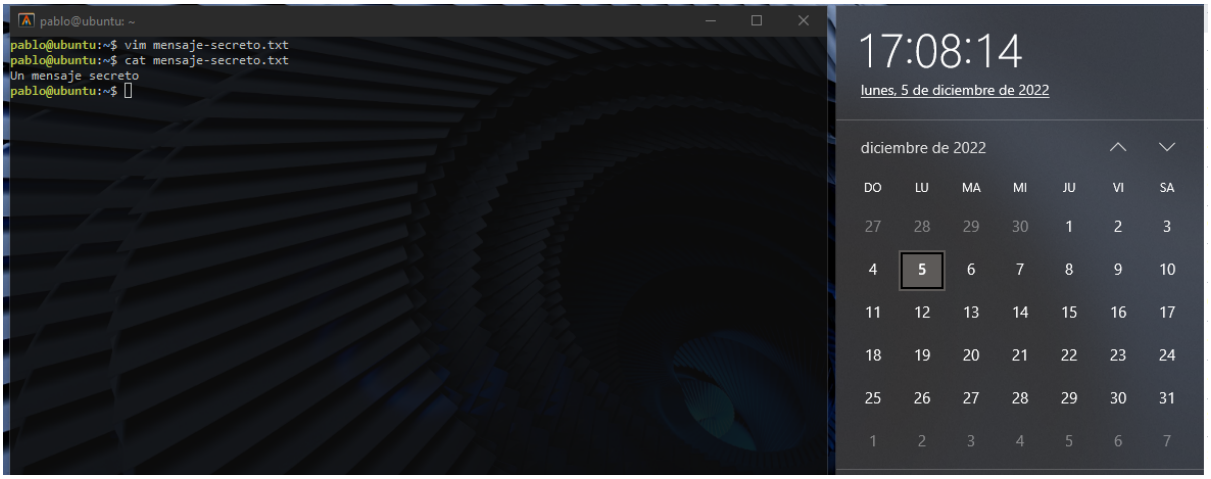
Actividad 5

Pablo Sanchez Galdamez (21001135)

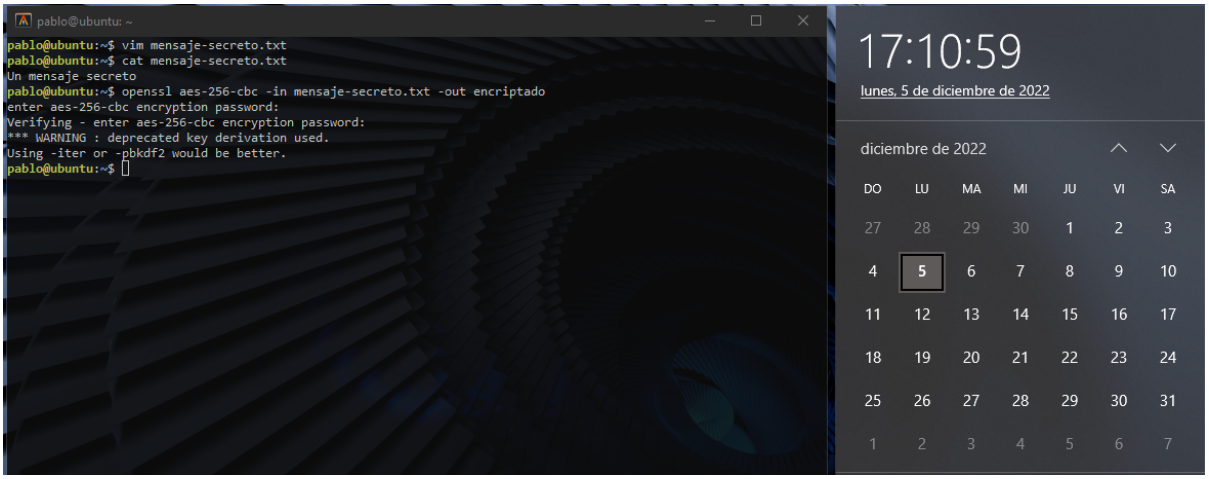
Cifrado simétrico

Algoritmo seleccionado: AES
Implementación: Usando OpenSSL en linux

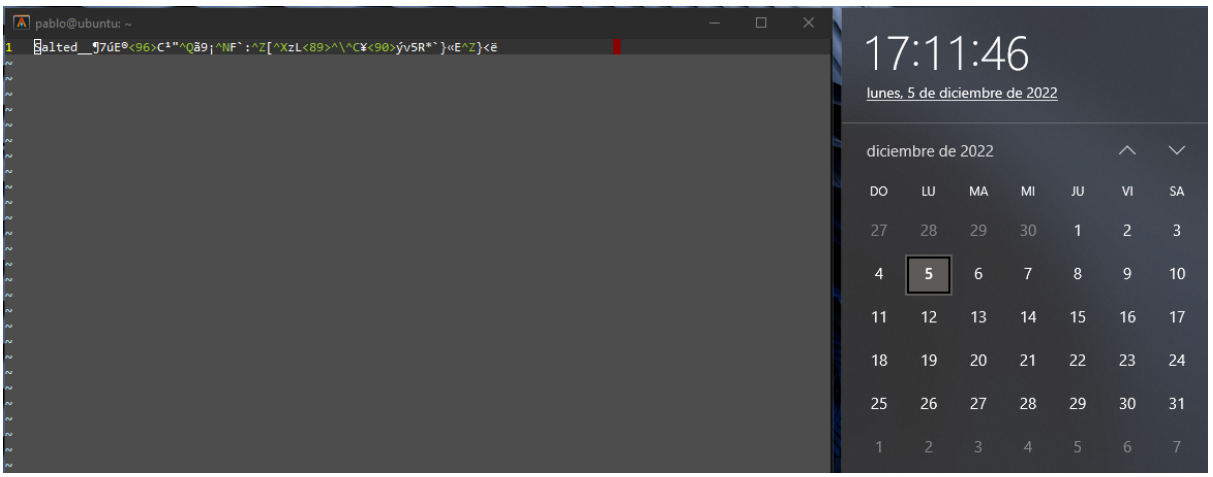
Primero crearemos un mensaje para encriptar:



Luego encriptamos el mensaje:



Lo que nos dará el siguiente mensaje encriptado:



Por si no se lee bien en la imagen:

Salted__¶7úE®<96>C¹'^Qã9¡^NF`:^Z[^XzL<89>^\^C¥<90>ýv5R*`}«E^Z}<ë

Justificación

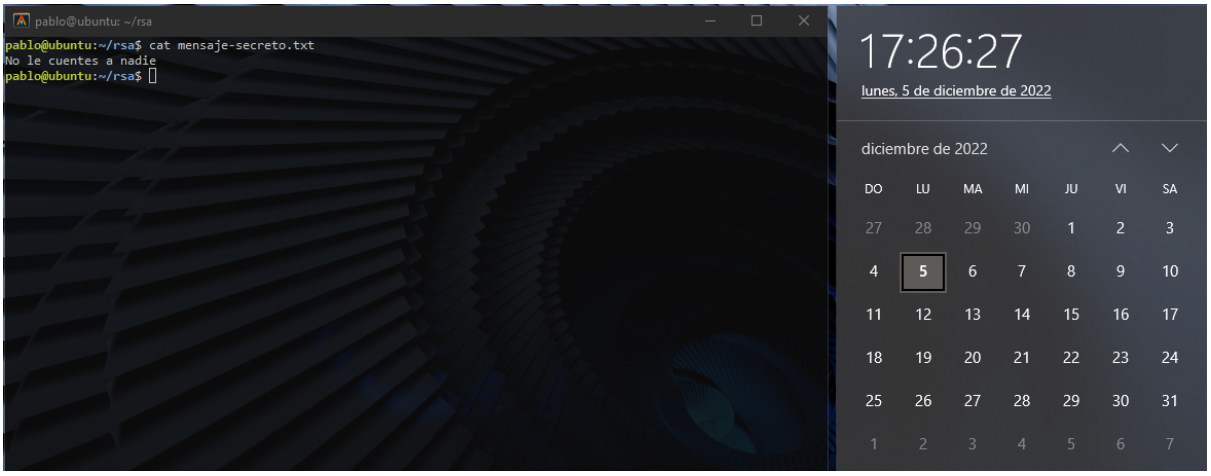
Leí que los más seguros que se pueden utilizar son AES, o DES con 3 pasadas.

Luego de investigar un poco, parece que no solo AES es el más seguro, sino que también es más rápido que 3DES, así que decidí usar ese.

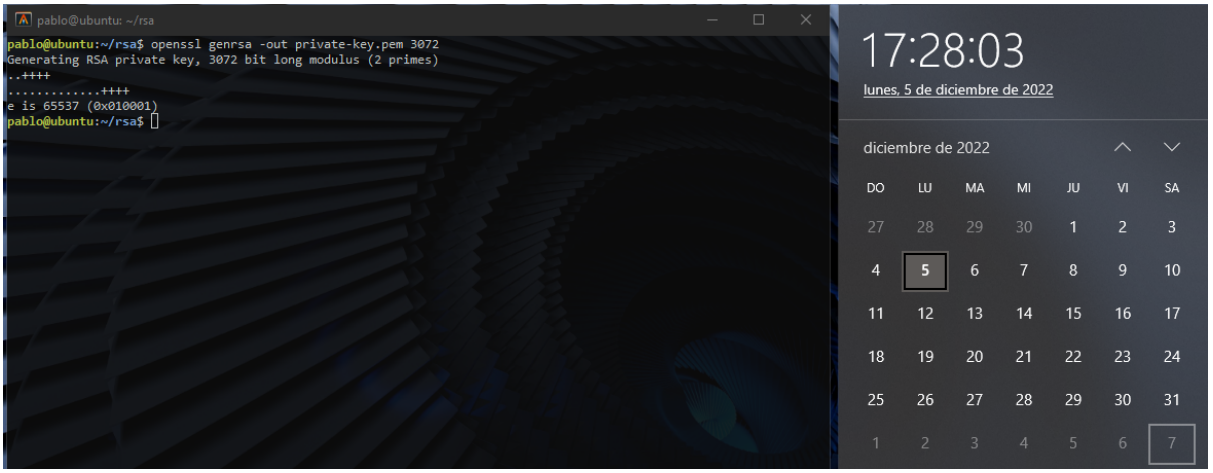
Cifrado asimétrico

Algoritmo seleccionado: RSA
Implementación: Usando OpenSSL en linux

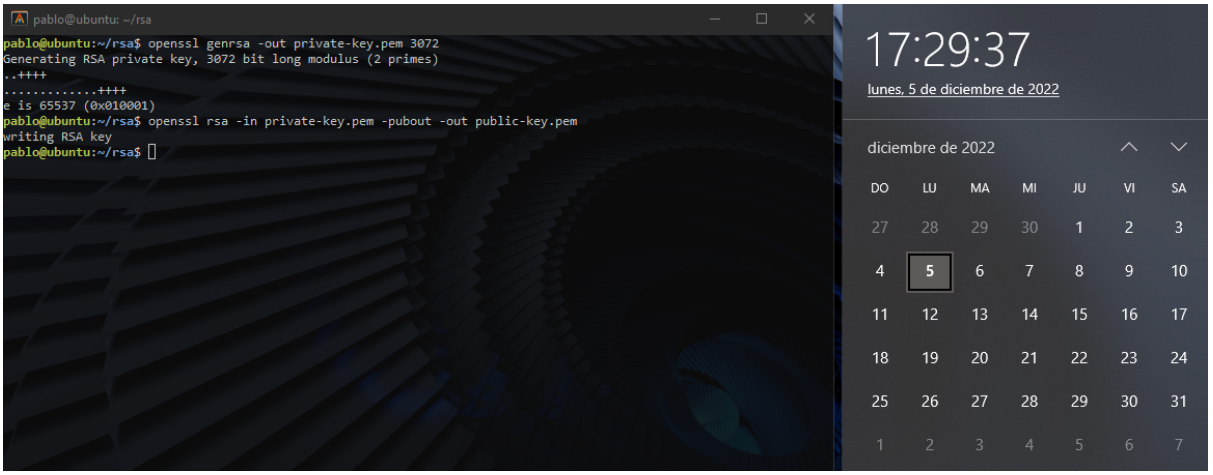
Primero crearemos un mensaje a encriptar:



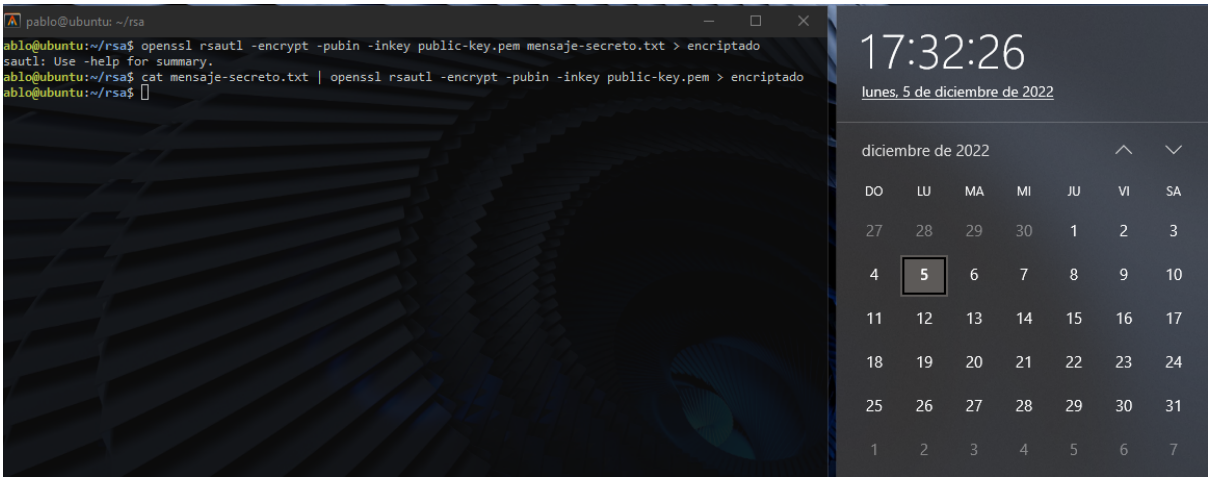
Luego crearemos la llave privada:



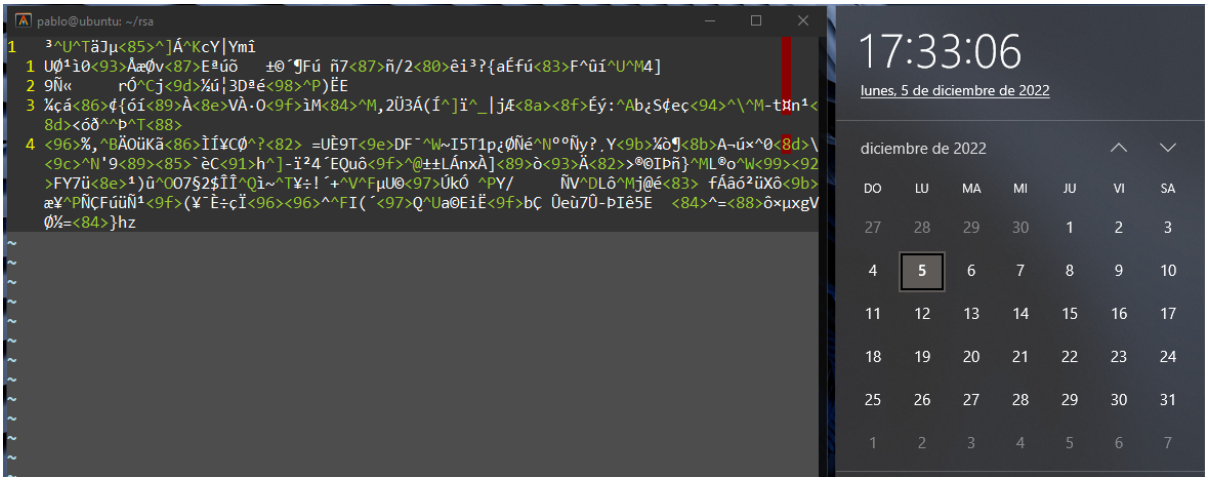
Y usando la llave que recién creamos crearemos la llave pública:



Y usando la llave pública encriptamos el mensaje:



Lo cual nos generará el siguiente mensaje encriptado:



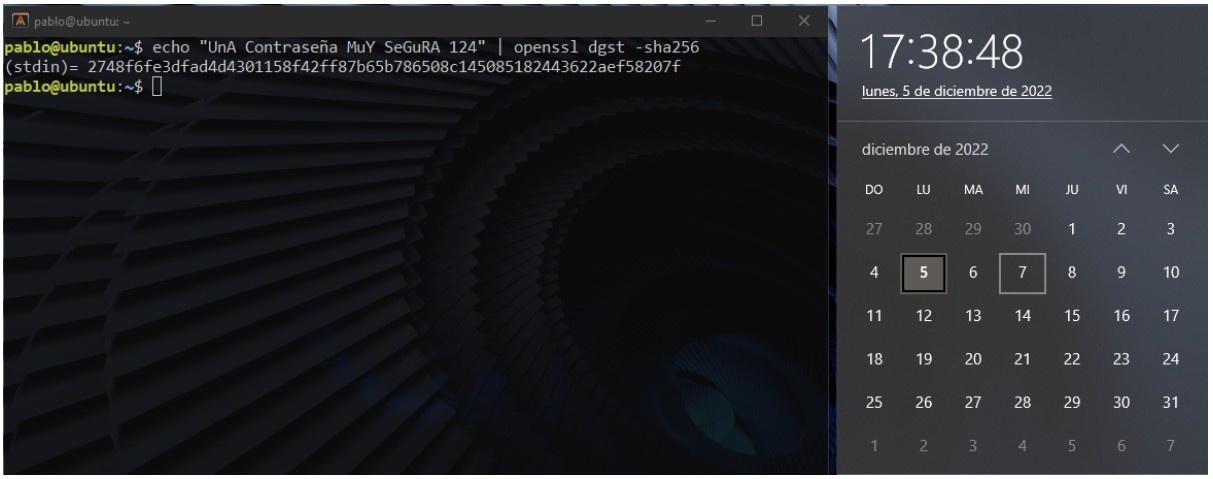
Justificación

Según investigue RSA es el más seguro, se le considera de grado militar, así que me pareció el más apropiado para utilizar.

Función hash

Algoritmo seleccionado: SHA-256
Implementación: Usando OpenSSL en linux

Simplemente pasamos el contenido que necesitemos a la funcionalidad digest de openssl



Justificación

Siempre que escucho sobre funciones hash se menciona SHA-256, así que me pareció apropiado usar este algoritmo.