SEGURIDAD INFORMÁTICA

TEMAS 3 Y 4

2ºA - PARTE PRÁCTICA

**EJERCICIO 1 (1,5 PUNTOS)**

Hay un mensaje, que codificado tiene la siguiente salida:

NDUgNGUgNDggNGYgNTIgNDEgNDIgNTUgNDUgNGUgNDEgMmMgMjAgNGMgNGYgMjAgNDggNDEgNTMgMjAgNDMgNGYgNGUgNTMgNDUgNDcgNTUgNDkgNDQgNGY=

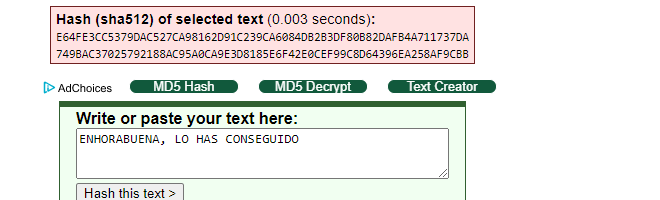
Obtén el mensaje. **ENHORABUENA, LO HAS CONSEGUIDO**

Una vez decodificado el mismo, tiene el siguiente hash:

e34fe3cc5379dac527ca98162d91c239ca6084db2b3df80b82dafb4a711737da749bac37025792188ac95a0ca9e3d8185e6f42e0cef99c8d64396ea258af9ccb

¿Es correcto? Si la respuesta es NO, muestra el correcto.

Ese es el hash.



**EJERCICIO 2 (3,5 PUNTOS)**

Necesitas dos máquinas virtuales, ambas con Linux. En una tiene que tener un usuario que se llame TuNombre y en otra un usuario que se llame TuApellido.

Cambiamos los nombres a las maquinas.



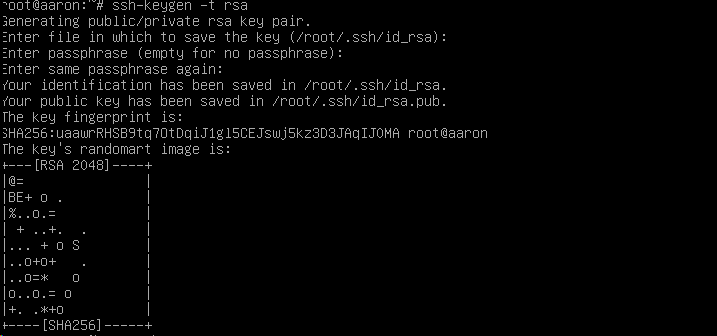




Utilizando la herramienta openssl:

Creamos las claves

* Crea un par de claves rsa



Vamos al directorio .ssh

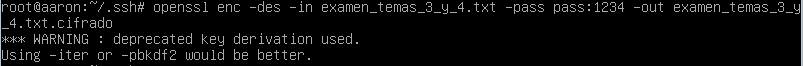


* Cifra un fichero de texto que te debes de crear con el nombre “examen temas 3 y 4”

Creamos el archivo con NANO y escribimos algo dentro, luego un ls.



Encryptamos en fichero con des.



Vemos que se ha encriptado.

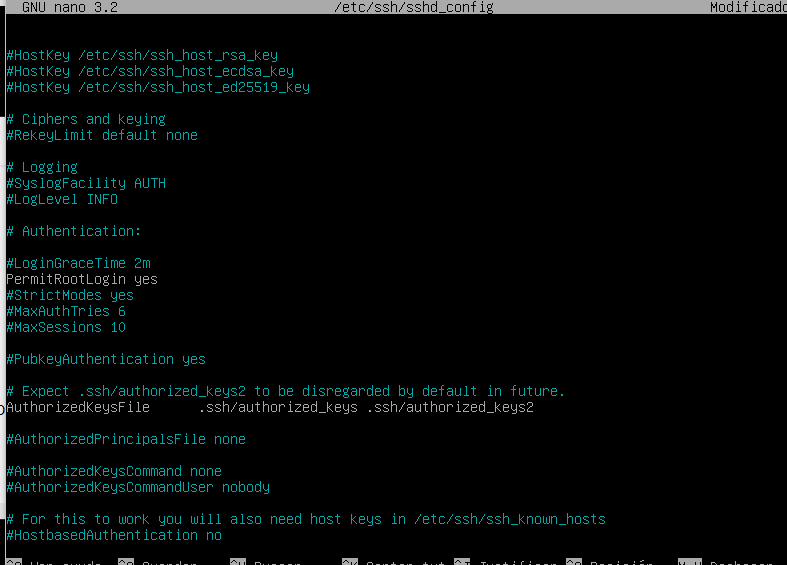


* Para el fichero del usuario TuNombre de la MV 1 al usuario TuApellidos de la MV2

Instalamos ssh server.



Configuramos el ssh server, para que tenga un archivo de claves y permita entrar con root.



Vemos que nos permite refrescar y ver cómo está el servicio.



Creamos el archivo y hacemos un ls, archivo que vamos a copiar.



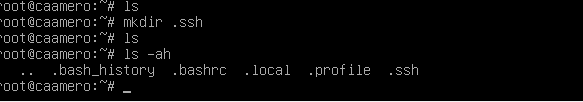
Encryptamos este archivo como hemos hecho anteriormente.



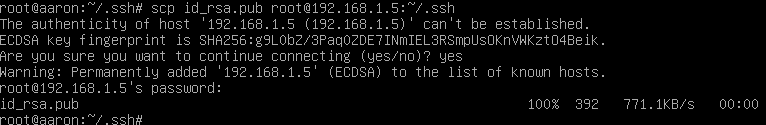
Vemos como este encriptado.



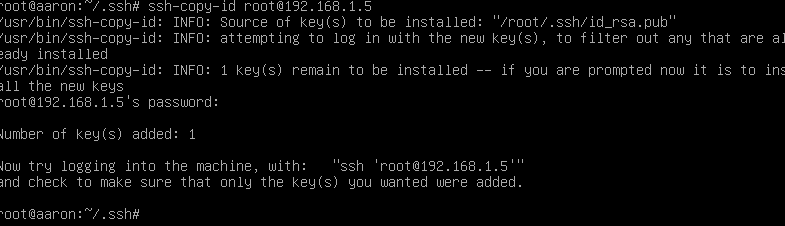
En el servidor creamos el directorio .ssh.



Copiamos la publica al servidor.



Después el identificador de clave, para que pueda descryptar el archivo que vamos a pasar.



Copiamos el archivo a la otra máquina.



Vemos que se ha copiado correctamente.



Comprobamos que está cifrado.



Creamos la privada del servidor.



Creamos la publica.



* Descifra el fichero desde el usuario

Se descifra con el comando OPENSSL RSAULT –DECRYPT –IN ARCHIVO1.TXT.CIFRADO –OUT ARCHIVO1.TXT.DESCIFRADO – INKEY PRIVADA.KEY.

Cifras con su publica y descifras con tu privada.

Nota: En todas las capturas debes de dejar claro en que máquina y con qué usuario estás trabajando. Explica lo que haces brevemente, incluso los pasos que faltan para realizar este proceso correctamente. ESTAS NORMAS SON DE OBLIGADO CUMPLIMIENTO PARA DAR EL EJERCICIO POR BUENO.