# Ejercicio 1

La herramienta gpg viene instalada en distribuciones Linux, y nos permite

utilizar tanto criptografía simétrica como asimétrica. En este ejemplo veremos

la simétrica.

Abriremos la terminal Linux y crearemos un directorio llamado cifrado donde

trabajaremos. También puedes crear dentro carpetas dentro en función del tipo

de ejercicio: simetrico para ejercicios sobre cifrados simétrico etc. Lo primero

será crear un fichero de prueba. Podemos utilizar la herramienta fortune, que

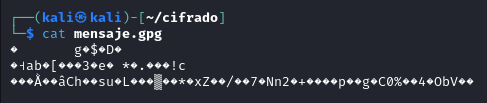
ofrece aleatoriamente refranes, chistes, etc. Para ello, nos hará falta instalarla

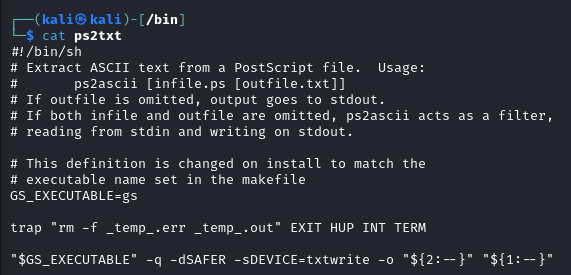
previamente.

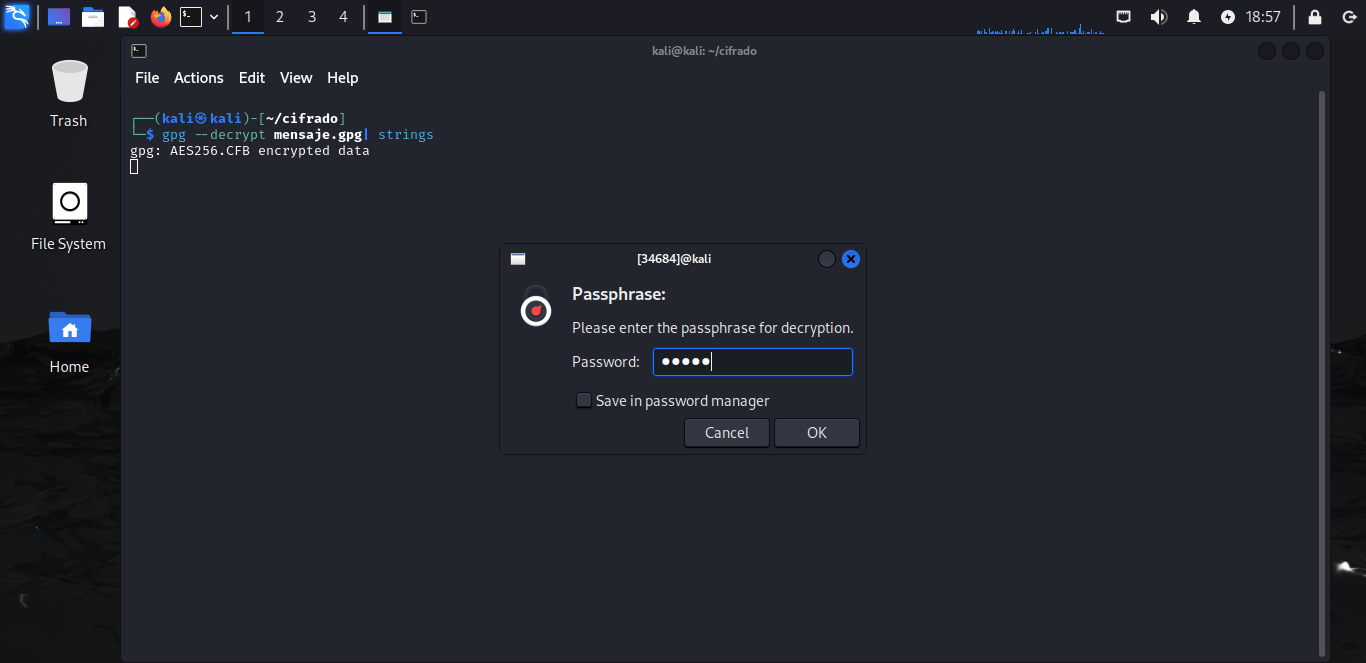
1. Redirige la salida del programa fortune a un fichero de texto plano.



1. Cifra el mensaje generado anteriormente mediante el uso del comando gpg y un parámetro que indique que el cifrado sea simétrico. ¡RECUERDA LA CONTRASEÑA! Nota: Sería conveniente que te guardaras el manual de gpg para saber qué parámetros utilizar en los distintos apartados y ejercicios. Esto puedes hacerlo con: man gpg > manual También interesaría ir anotando los diferentes comandos utilizados, junto con su función para así poder reutilizarlos más adelante.  
   
2. Intenta sacar por pantalla el contenido del mensaje cifrado. ¿Qué aparece? Intenta sacar por pantalla alguno de los ficheros contenidos en /bin.

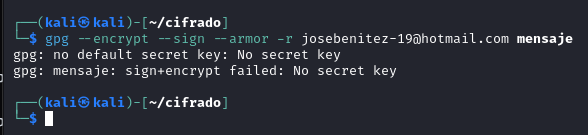




1. Repite el paso anterior pero esta vez usando el comando strings para obtener la salida del fichero cifrado. Utiliza man para saber qué hace este comando.  
   
2. Ahora cifra el mensaje pero añadiendo también el parámetro -a. ¿Qué diferencias hay con respecto al mensaje cifrado de la forma anterior?  
   

Ahora usa ascii

1. Intenta transmitir ambos mensajes cifrados por correo electrónico. ¿Qué ocurre?



No tengo llave privada

1. Borra el mensaje en claro y transfiere mediante FTP el mensaje cifrado al cliente Windows, y desde Windows, descifra y vuelca el mensaje transmitido a otro fichero de texto plano. Te harán falta los siguientes preliminares:
   1. Descargar e instalar la aplicación Gpg4win: Esta aplicación cuenta con una interfaz gráfica llamada Kleopatra. Pero desde línea de comandos se puede utilizar de la misma manera que en Linux, y así no será necesario que aprendamos en este momento a usar la interfaz gráfica. No obstante, utilícese lo que se considere más oportuno.

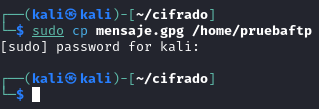
Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente

* 1. Mover el mensaje cifrado al directorio de trabajo de usuarioftp



1. Una vez descifrado el mensaje, elabora una respuesta al mismo, cífrala y transfiérela de nuevo a Linux. Desde Linux, vuelve a comprobar la respuesta en claro transmitida

Interfaz de usuario gráfica

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

1. Con la herramienta gpg podemos cifrar ficheros binarios, no solo ficheros de texto. Por tanto, lo primero que haremos será hacer una copia del propio ejecutable fortune a la que llamaremos refranes. Hará falta saber la ruta en la que se encuentra el ejecutable. Averigua qué comando hace esto de manera directa.

Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente

1. Cifra el ejecutable refranes. ¿Qué formato de cifrado será el más adecuado?

Texto

Descripción generada automáticamente



1. Ahora descífralo y redirige la salida (mediante el parámetro -o) a un nuevo fichero llamado dichos

Texto

Descripción generada automáticamente

1. Prueba a ejecutar dichos. Te hará falta otorgarle los permisos adecuados.

Texto

Descripción generada automáticamente

## Ejercicio 2

Como habrás podido comprobar en el ejercicio anterior, los ficheros binarios .gpg no siempre son adecuados. No sirven para incluirlos dentro de un texto (por ejemplo, en un script o un correo electrónico). Para resolverlo tenemos el parámetro -a, que genera un fichero cifrado pero compuesto solo de caracteres ASCII. Estos ficheros ya no tienen extensión. gpg, sino .asc. Dentro está el contenido cifrado, y alrededor un par de cabeceras informativas. Además, existe otro parámetro para cambiar el algoritmo de cifrado utilizado. Investiga cuál es, y compara los cifrados efectuados en el Ejercicio 1, con los logrados con cualquier otro algoritmo de cifrado simétrico de entre todos los disponibles en gpg. Para ver con qué algoritmos contamos, puedes usar el parámetro --version. Explica también toda la información que obtienes al ahcer esto último.



