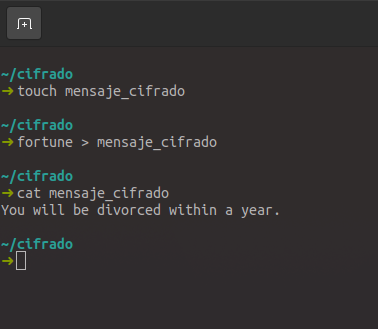
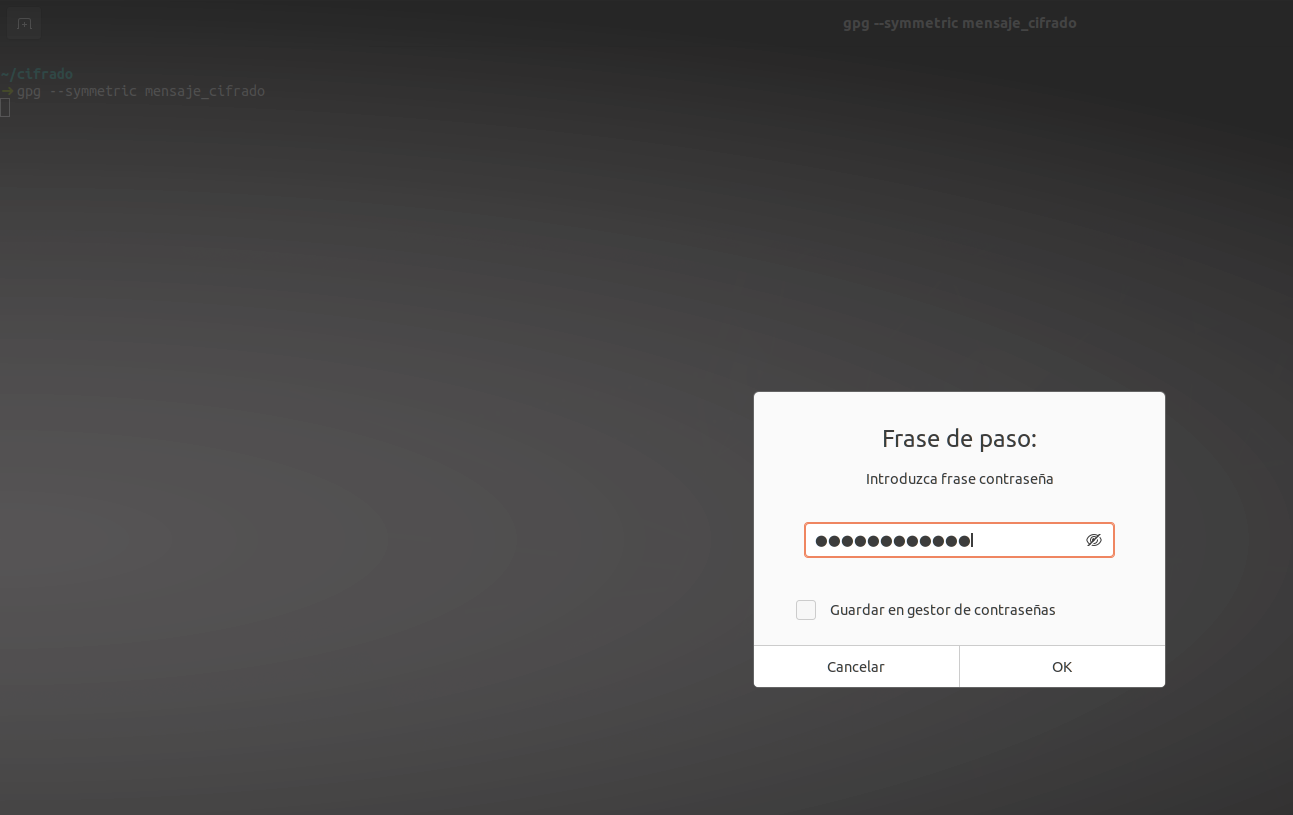
**Juan Carlos Navidad García**

**Seguridad Informática**

CIFRADO SIMETRICO EN LINUX



1. **Proceso de instalación de Webmin en Ubuntu:**
2. **La herramienta gpg nos permite utilizar tanto criptografía simétrica como asimétrica. En este ejemplo veremos la simétrica.**
3. **Nos presentamos en Ubuntu y creamos un directorio llamado cifrado donde vamos a trabajar. Lo primero será crear un fichero de prueba.**
   * Podemos utilizar la herramienta **fortune**, que ofrece aleatoriamente refranes, chistes, etc.
   * Creamos un archivo de texto cualquiera.
   * Ejecutamos*:* ***“fortune > archivo”***
4. **Para cifrarlo con clave simétrica el comando es:**

* *“gpg –-symmetric archivo”*
* El comando nos pedirá la clave que queremos utilizar
* El resultado del comando es un nuevo fichero con la extensión. gpg. Es un fichero cifrado: si intentamos ver qué hay dentro con el comando cat, no aparece nada inteligible.
* Aquí podemos ver que se ha cifrado:

1. **Cuando se necesite leerlo, se descifrará con el comando:**

* *“gpg -–decrypt documento.gpg”*
* El comando pedirá la clave que habíamos utilizado para cifrar. Si la introducimos correctamente, aparecerá en pantalla el contenido del fichero.

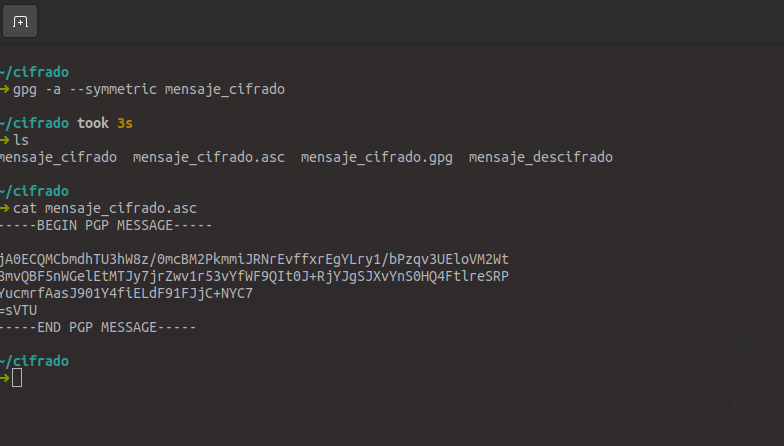
1. **Si no queremos verlo por pantalla, sino volcarlo a un fichero, podemos redirigir la salida estándar con el comando:**

* “gpg –-decrypt documento.gpg > documento2”

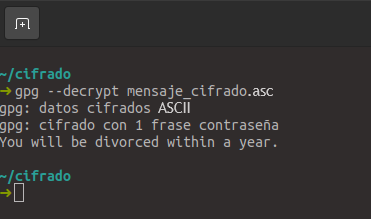


1. **Los ficheros binarios.gpg no siempre son adecuados. No sirven para incluirlos dentro de un texto. Para resolverlo tenemos el parámetro -a, que genera un fichero cifrado pero compuesto solo de caracteres ASCII. Estos ficheros ya no tienen extensión.gpg, sino .asc. El comando en cuestión sería:**

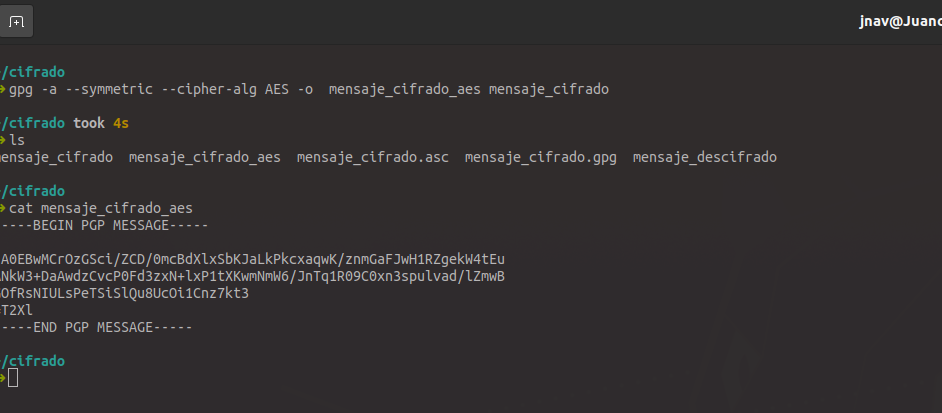
* *“gpg –a -–symmetric mensaje”*



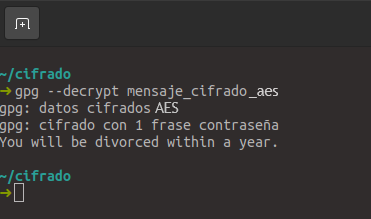
1. **El fichero .asc ofrece las mismas garantías que el .gpg y se utiliza igual. Para descifrar sería:**

* *“gpg –-decrypt mensaje.asc”*

1. **La herramienta por defecto utiliza el algoritmo de cifrado CAST5. Podemos cambiarlo con el parámetro cipher-alg. Por ejemplo, para utilizar AES ejecutaríamos:**

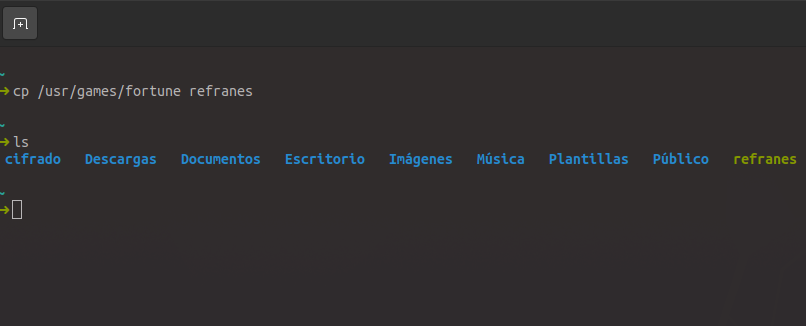
* *“gpg –a –-symmetric –-cipher-alg AES –o mensaje.aes mensaje”*
* En este ejemplo hemos utilizado **-a** para tener el fichero en ASCII y el parámetro **-o** para indicar el fichero de salida (es equivalente a redirigir la salida estándar).

1. **El descifrado se hace como siempre:**

* **“*gpg -–decrypt documento.aes”***
* Ahora, el mensaje de la pantalla nos avisa de que el fichero estaba cifrado con **AES** (ya no es **CAST5**).

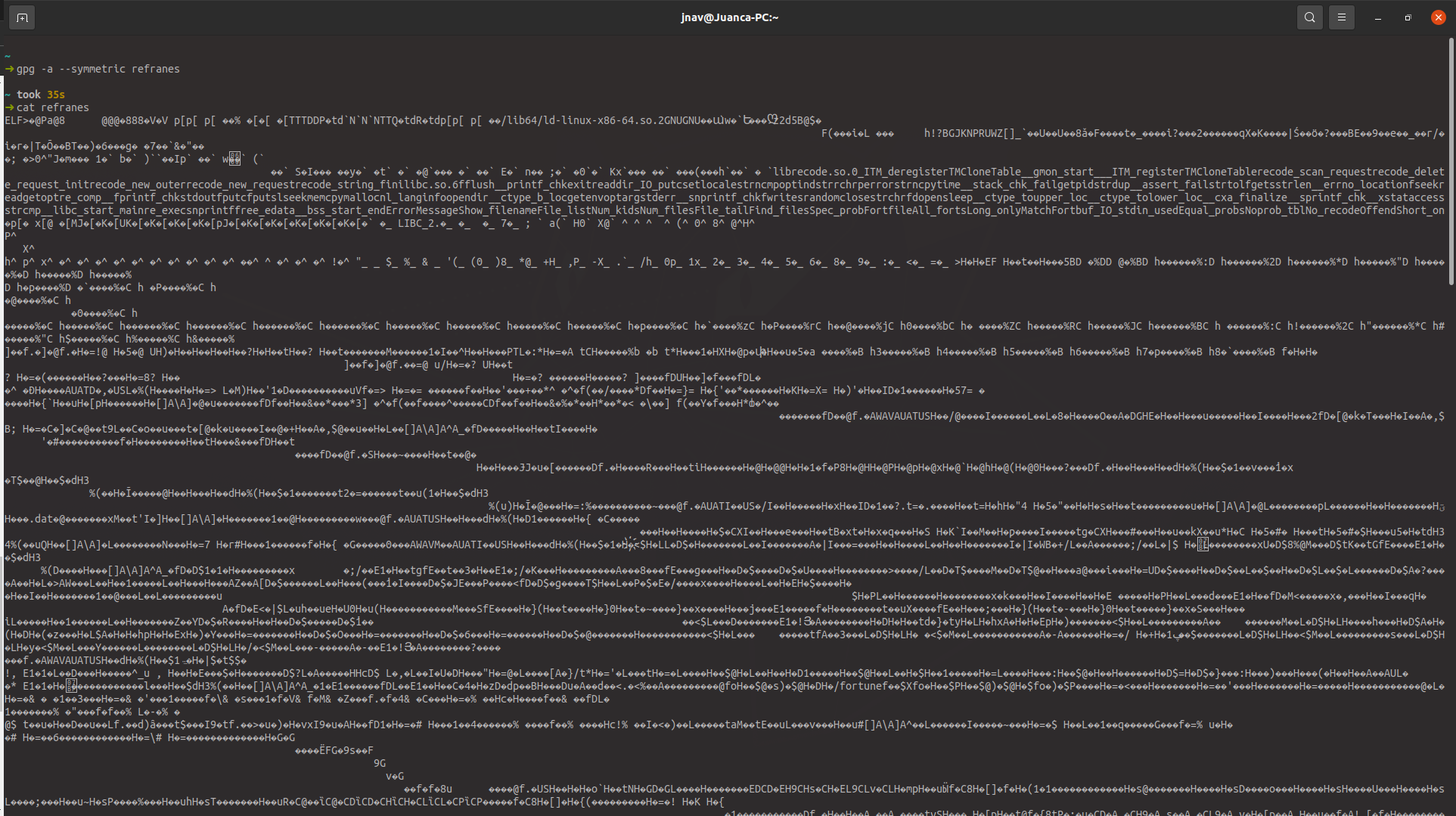
1. **Con esta herramienta podemos cifrar ficheros binarios, no solo ficheros de texto. Vamos a trabajar sobre una copia del propio ejecutable fortune y le llamaremos refranes. Los comandos serían:**

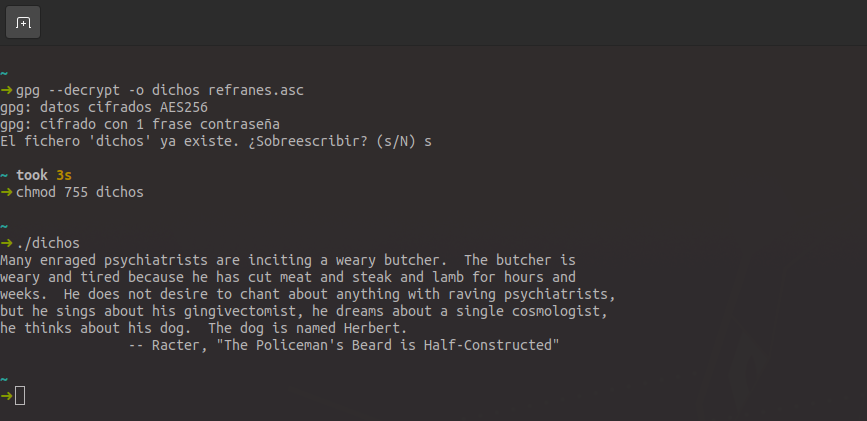
* *“cp /usr/games/fortune refranes”*
* *“./refranes”*



1. **Lo ciframos en modo ASCII:**

* *“gpg –a -–symmetric refranes”*



1. **Podemos recuperarlo descifrando el fichero refranes.asc con las opciones conocidas. Por ejemplo, podemos dejar el resultado en un nuevo fichero dichos. Después de introducir la contraseña, solo necesitamos darle permisos de ejecución y estará disponible. Los comandos son:**
   * *“gpg –-decrypt –o dichos refranes.asc”*
   * *“chmod 755 dichos dichos”*