CICLO FORMATIVO DE GRADO SUPERIOR - TÉCNICO EN ADMINISTRACIÓN DE SISTEMAS INFORMÁTICOS EN REDES

SEGURIDAD Y ALTA DISPONIBILIDAD

TEMA 5

Nombre y apellidos:
-Wuke Zhang

ACTIVIDAD 5.1. Cifrado

En esta actividad vamos a utilizar los dos métodos de cifrado vistos en la terminal de Ubuntu.

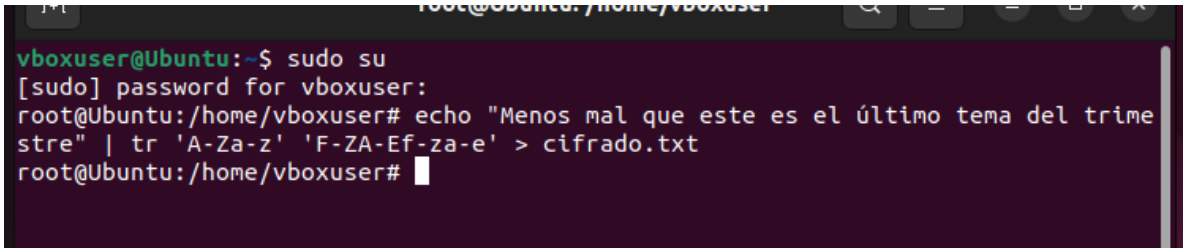
Añade capturas de pantalla de toda la ventana de la terminal en las preguntas en las que haya que ejecutar comandos. Se comprobará que el nombre del usuario sea el tuyo.

Responde a las siguientes preguntas:

1. Realiza en la terminal un cifrado cesar con clave 5 de la siguiente frase:

"Menos mal que este es el último tema del trimestre"

El cifrado deberá guardarse automáticamente en un fichero llamado ***cifrado.txt*** **(1 pto)**

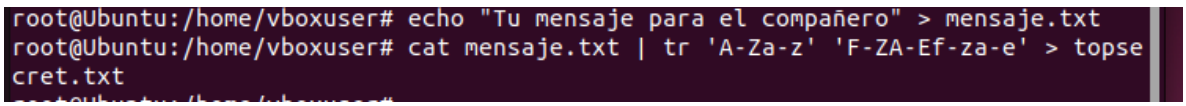


2. Responde a las siguientes preguntas (1 pto)

- ¿Cómo se le llama al texto anterior? Texto plano si te refieres al original
- Una vez que lo hemos cifrado, ¿qué tipo de texto obtenemos? Texto cifrado(criptograma)
- ¿A qué grupo de algoritmo de cifrado pertenece? Cifrado simétrico

3. Mensaje oculto con cifrado simétrico (4 ptos)

- Crea un fichero de texto con el nombre ***mensaje.txt***.
- Escribe una frase para enviarla a tu compañero/a de clase.
- Cifra el fichero con cifrado cesar y guárdalo directamente en un fichero llamado ***topsecret.txt.***



- Envía o pasa el fichero a tu compañero/a para que lo descifre. Además del fichero, ¿qué necesitará para poder descifrar el texto?

  La clave
- Al mismo tiempo, descifra el mensaje que tu compañero/a ha preparado para ti.

  cat "nombre y extension del archivo" | tr 'F-ZA-Ef-za-e' 'A-Za-z'

4. Cifrado asimétrico (4 ptos)

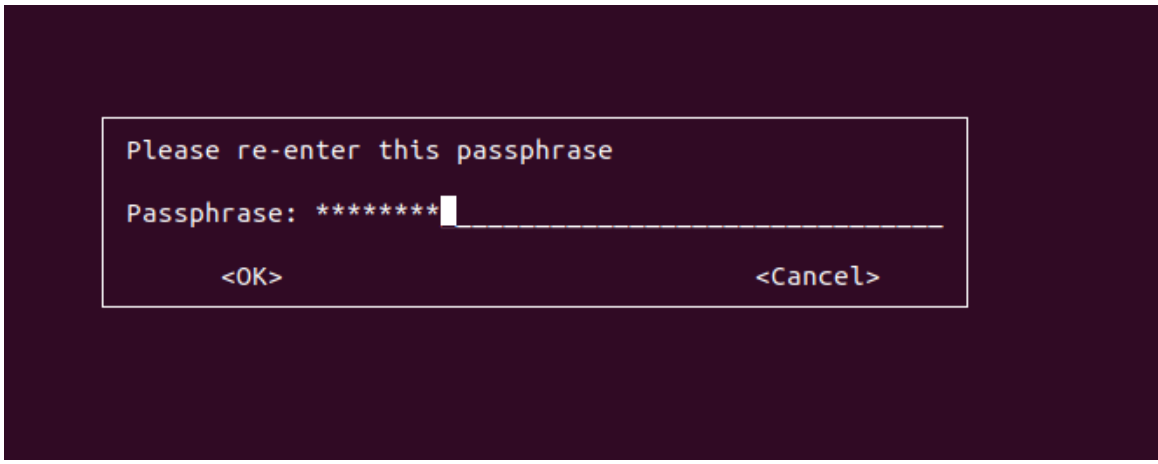
- Modifica el fichero ***mensaje.txt*** y añade una nueva frase.

```
root@Ubuntu:/home/vboxuser# echo "Frase nueva para cifrar asimétricamente" >> me
nsaje.txt
```

- Utiliza el comando gpg --full-gen-key para crear un par de claves. Las llaves deben cumplir las siguientes características:

  - ***o*** Algoritmos RSA (permite cifrar y firmar archivos)
  - ***o*** Tamaño de llave: 4096 (a mayor cantidad de bits, mayor seguridad)
  - ***o*** Caducidad de la clave: 0 (esto es para que la llave se mantenga siempre vigente, aunque en ocasiones es recomendarle ponerle una fecha de expiración)
  - ***o*** Real name: Escribe tu nombre y primer apellido
  - ***o*** Correo: invéntate uno o déjalo en blanco
  - ***o*** Contraseña: Escribe una contraseña que cumpla con las características ideales de seguridad vistas en el curso (tamaño, combinación de caracteres, etc)

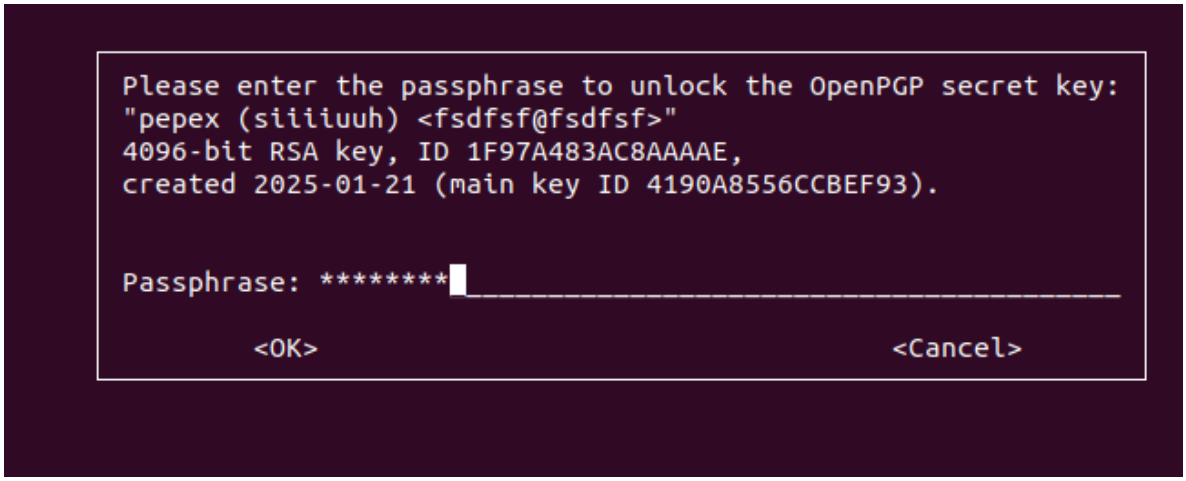
```
root@Ubuntu:/home/vboxuser# gpg --full-gen-key
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

gpg: directory '/root/.gnupg' created
gpg: keybox '/root/.gnupg/pubring.kbx' created
Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
  (14) Existing key from card
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (3072) 4096
Requested keysize is 4096 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 0
```



- Cifra el fichero ***mensaje.txt*** y muestra el cifrado en la terminal.

```
root@Ubuntu:/home/vboxuser# gpg --encrypt --recipient "pepex" mensaje.txt
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
```

- Ahora descífralo con la clave privada.




```
root@Ubuntu:/home/vboxuser# gpg --decrypt mensaje.txt.gpg
gpg: encrypted with 4096-bit RSA key, ID 1F97A483AC8AAAAE, created 2025-01-21
      "pepex (siiiiuuh) <fsdfsf@fsdfsf>"
Tu mensaje para el compañero
Frase nueva para cifrar asimétricamente
```

Envía el documento en formato **.pdf** con el nombre '**Actividad5.1. NombreyApellidos**'.