**Universidad Nacional de la Patagonia San Juan Bosco**

**Licenciatura en Sistemas O.P.C.G.P.I.**


# Administracion de Redes y Seguridad

## TP N.º 3

**Docentes: Mg. Ing. Ricardo Antonio López**
**Lic. Cristian Javier Parise**

**Alumnos: Aguila Maximiliano**
**Krmpotic Lucas**

# Guía de Trabajos Prácticos 3

## Criptografía y sus aplicaciones

### 3.1.Conceptos básicos

1. Dados los siguientes casos, determine cuál de los sistemas de cifrado resulta más adecuado (simétrico y asimétrico). Si decide utilizar el sistema de cifrado asimétrico, determine qué clave usaría para realizar el proceso de encriptado. Justifique brevemente su elección:

a) Juan quiere mandarle un mensaje a Julio. A Julio no le importa asegurarse que el mensaje fue enviado por Juan, sin embargo Juan quiere estar seguro de que el mensaje no podrá ser leído ni alterado por un tercero. Juan trabaja en una empresa en Argentina y Julio es empleado de una empresa ubicada en España.

_Utilizaria un sistema de cifrado ASIMETRICO, ya que no es necesario efectuar ningun tipo de intercambio de claves.
_Ademas Juan podria encriptar por modo de ENCRIPCION, en el cual Juan encriptaria con la clave publica del receptor (Julio), y el mismo podria desencriptar el mensaje utilizando su clave privada.

b) Adriana y Leandro quieren comunicarse en forma segura. Para ellos resulta fácil conseguir un medio seguro para intercambiar información que luego necesiten para realizar esta comunicación segura. En este caso lo que importa es que nadie pueda espiar los datos involucrados en dicha comunicación.

_Utilizaria un sistema de cifrado SIMETRICO, ya que es un sistema de clave compartida (o privada) en el cual solo ellos dos sabrian la llave o clave para encriptar/desencriptar.

c) Analía usará el correo electrónico para enviar la aceptación de un contrato al Estudio en el cual trabaja. Para la persona que lo reciba es importante tener la garantía de que el mismo fue enviado efectivamente por Analía.

_ Utilizaria un sistema de cifrado ASIMETRICO, en modo de AUTENTIFICACION.

2. Para cada afirmación determine si es verdadera o falsa:

a) En los criptosistemas simétricos no puede garantizarse el no repudio porque ambas partes de la transacción conocen la clave utilizada. Verdadero.

b) Si únicamente me importara la eficiencia del método que uso para encriptar, debería optar por un algoritmo de cifrado asimétrico. Falso, utilizaria Simetrico.

c) Con ambos tipos de criptosistemas necesito contar con un mecanismo seguro para transmitir la clave. Falso, solo en sistemas de cifrados Asimetricos.

### 3.2. Aplicaciones de criptografía
Herramientas necesarias: Un Navegador (Chrome, firefox, Iceweasel, etc.), Cliente de correo. (Thanderbird, Icedove, etc.), GnuPG, Enigmail y Steghide.

### 3.2.1. Primera parte: PKI
3. ¿Que información es necesaria para que quien recibe un mail firmado, pueda verificar la firma del mismo?

_La tecnología PKI permite a los usuarios autenticarse frente a otros usuarios y usar la información de los certificados de identidad para cifrar y descifrar mensajes, firmar digitalmente información, garantizar el no repudio de un envío, y otros usos.
En este caso, para verificar la firma del mail firmado se necesita el certificado con la CLAVE PUBLICA.

4. ¿Que información necesito para poder enviar un mail encriptado?

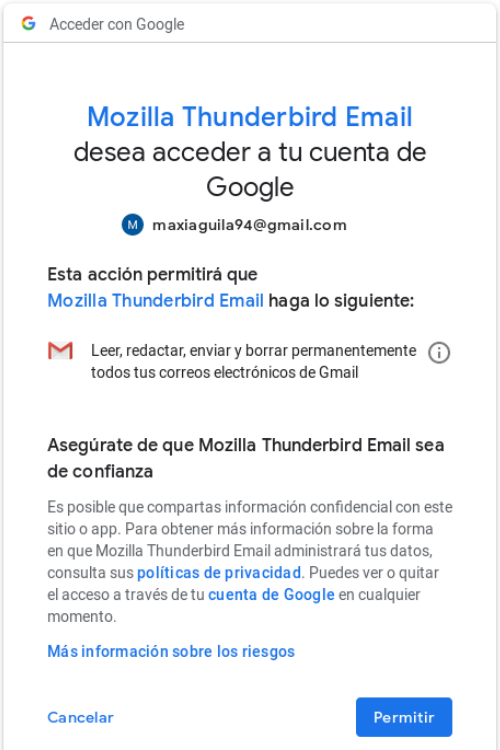
_Para enviar un mail encriptado se necesita es la CLAVE PRIVADA.

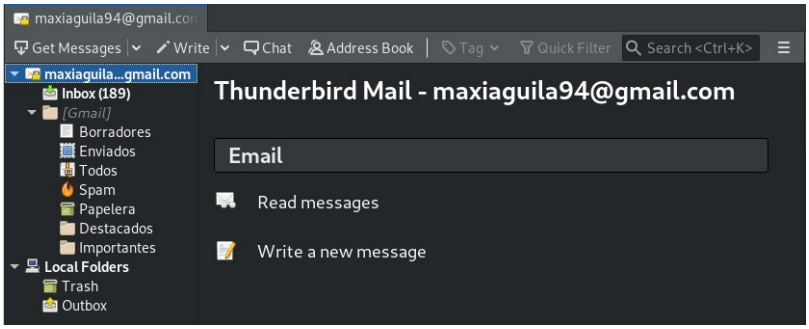
5. ¿Que información es necesaria para que quien recibe un mail encriptado, pueda abrirlo?

_ Para poder abrir un mail encriptado necesito la CLAVE PUBLICA

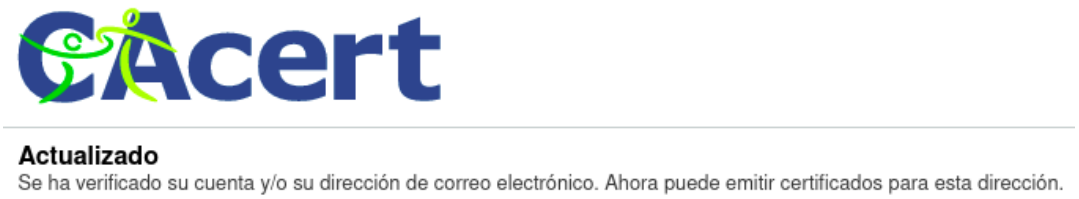
6. Realice la siguiente práctica, efectuando los pasos en el orden que se proponen.

a) Configure el cliente de correo Thunderbird para acceder a su correo personal. Estos programas permite envio/recepción de mails cifrados/firmados.
Nota: Verificar que esté seteada la opción de mantener correo en el servidor

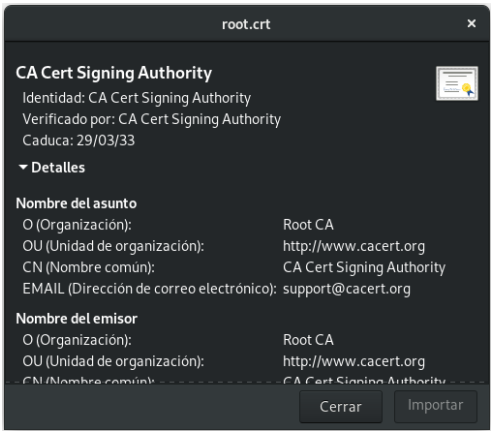


b) Diríjase al Sitio https://www.cacert.org/ e instale el certificado de la Autoridad de certificación en su navegador.




1) A través de la opción Certificado raíz, descargar el Certificado Raíz (Formato PEM) su disco local.




2) Antes de instalarlo, vea el certificado de la Autoridad de Certificación y mencione:

3) El algoritmo de firma que utiliza.

_Algoritmo de firma: MD5 con RSA

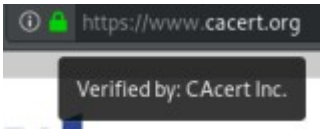
4) La cantidad de bits de cifrado.
5) El período de validez del mismo.

_Caduca: 29/03/33

6) Otras observaciones que le parezcan importantes.

_ Parámetros de la firma: 05 00
_ Identidad: CA Cert Signing Authority
_ Verificado por: CA Cert Signing Authority
_ Información de la clave pública
_ Parámetros de la clave
_ Tamaño de la clave
_ Huella de la clave SHA1

7) Instale el certificado y establezca que se confiará en esa Autoridad para verificar otros sitios y para certificar otros usuarios de correo.
8) Verifique que el certificado de la CA fue instalado correctamente en su navegador.
c) Una vez instalado, debería entrar sin que el navegador le advierta que el sitio no es seguro o confiable en el sitio de la CA https://www.cacert.org/




d) Ingrese nuevamente al sitio mencionado (con el certificado instalado, según el paso anterior), solicite un certificado de correo electrónico para Ud. Para ello, ingrese sus datos y siga las instrucciones que se le indiquen en el Sitio. A través de la opción: Darse de alta, luego “Iniciar sesión con contraseña” y usar la opción “Certificado de cliente”.
La dirección de email que especifique en el certificado, deberá ser la que esté configurada en el cliente de correo.

**Nuevo Certificado de Cliente**

| Agregar | Dirección |
|---|---|
| ☑ | maxiaguila94@gmail.com |
| ☑ | Permitir iniciar sesión con este certificado<br>Al permitir la autenticación mediante certificado, éste puede utilizarse para acceder a esta cuenta desde https://secure.cacert.org/ . |
| Comentario opcional, se utiliza únicamente en la vista rápida del certificado | |
| ☐ | Mostrar opciones avanzadas |
| ☑ | **Acepto el Acuerdo de la Comunidad de CAcert (CCA).**<br>Por favor, observe que: Necesita aceptar el CCA para continuar. |
| | Siguiente |

7. Instale y verifique que su certificado haya sido correctamente instalado en su Navegador.

**Información acerca del certificado**

| | |
|---|---|
| Estado | Válido |
| Dirección e-mail | maxiaguila94@gmail.com |
| Número de Serie | 13E08D |
| Revocado | No Revocado |
| Caduca | 2019-05-06 17:37:14 |
| Iniciar sesión | ☑ |
| Comentarios | |

a) Enviar el certificado al foro de consultas del aula así todos tienen los certificados de sus compañeros para hacer esta practica (o enviarlo por email al profesor asi los publica)

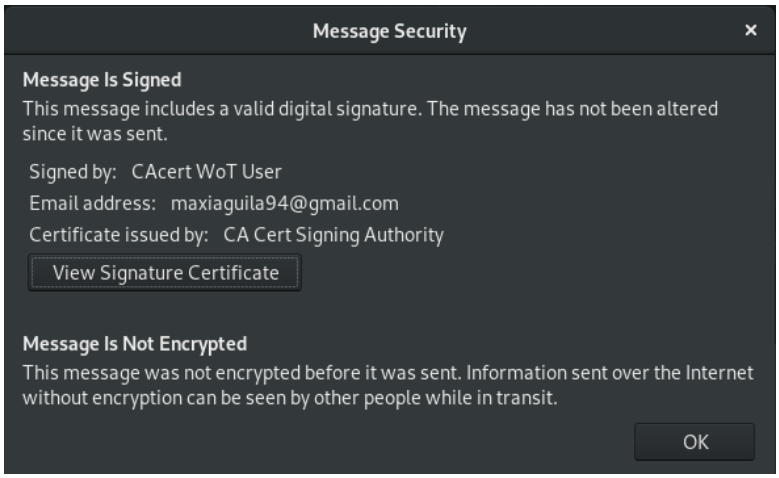
b) procesa a instalar el mismo en su navegador. Verifique que el mismo haya sido instalado correctamente.

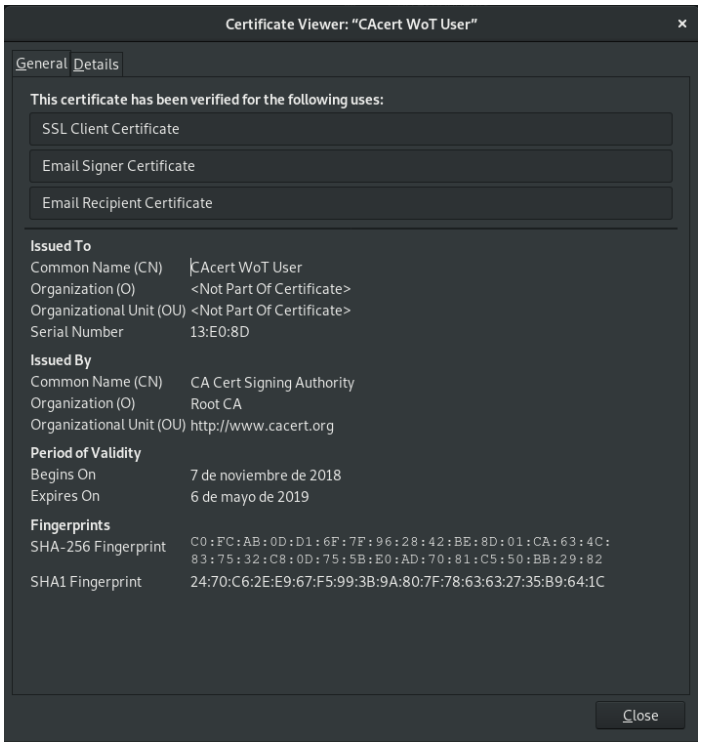
c) Exporte su certificado personal y el certificado de la autoridad de certificación en una carpeta de su PC y luego impórtelos en su cliente de mail, en el caso de Thunderbird a través de las siguientes opciones:
1) El certificado de la CA impórtelo desde la opción: Editar → Preferencias → Avanzadas → Certificados → Ver Certificados → Autoridades → Importar. . .

2) Su certificado impórtelo desde la opción: Editar → Preferencias → Avanzadas → Certificados → Ver Certificados → Sus certificados → Importar. . .

8. Envíe un mail firmado a un compañero y analice cómo llega el mismo a la cuenta personal de dicho usuario. Nota: deberá usar la opción Firmar Mensaje (S/MIME)). ¿Qué información es necesaria en el destino para verificar la firma?

_ Para verificar la firma se necesita la CLAVE PUBLICA


9. Envíe un mail encriptado a un compañero y analice cómo llega el mismo a la cuenta personal de dicho usuario. Nota: deberá usar la opción Cifrar Mensaje (S/MIME)). ¿Qué información es necesaria en el destino para abrir el correo?
Nota: puede ser necesario que tenga que instalar el certificado de la persona a la que le desea enviar mails cifrado

_ En el destino, para abrir el correo se necesita su CLAVE PRIVADA

10. Envíe un mail encriptado y firmado a un compañero. ¿Qué información es necesaria en el destino para abrir el correo y verificar la firma?

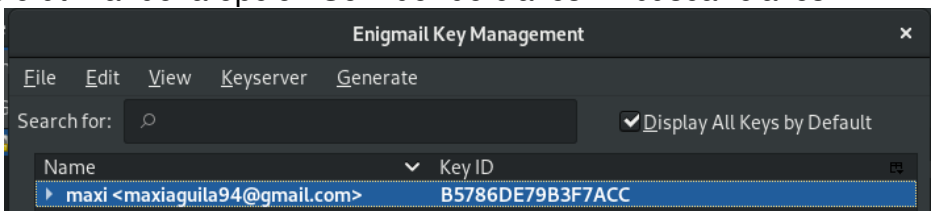
_ Se necesita que la firma este verificada y la CLAVE PUBLICA

### 3.2.2. Segunda parte: PGP

Creando anillos de claves y cifrando/firmando correo electrónico:

12. Cree su par de claves PGP, si usan Thinderbir, instalen el complemento Enigmail.
13. Dentro del administrador de claves, publique su clave en el Servidor de claves
a) Utilice la opción “Servidor de Clave” → “Subir Claves Públicas”

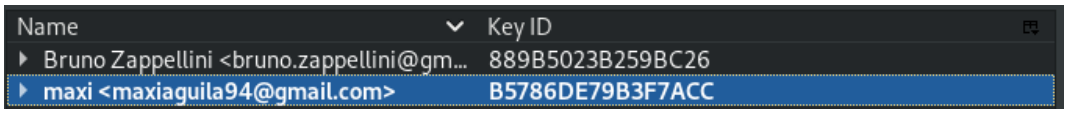
b) Compruébelo utilizando la opción Servidor de claves → buscar claves




14. Dentro del administrador de claves, incorpore la clave de su compañero a su anillo de claves, para ello:

a) “Servidor de Claves” → “Buscar Claves” e ingresando la dirección de mail que corresponda a su compañero.

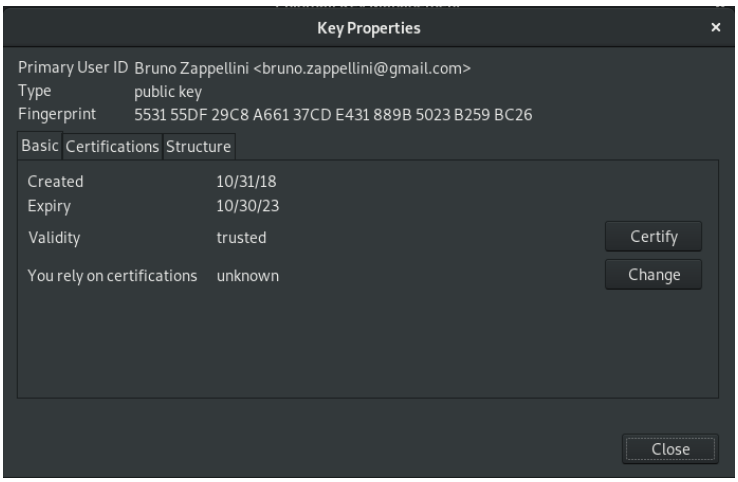
b) Importe la misma a su anillo de claves.




c) Firme la clave de su compañero, a través de la opción “Firmar”.

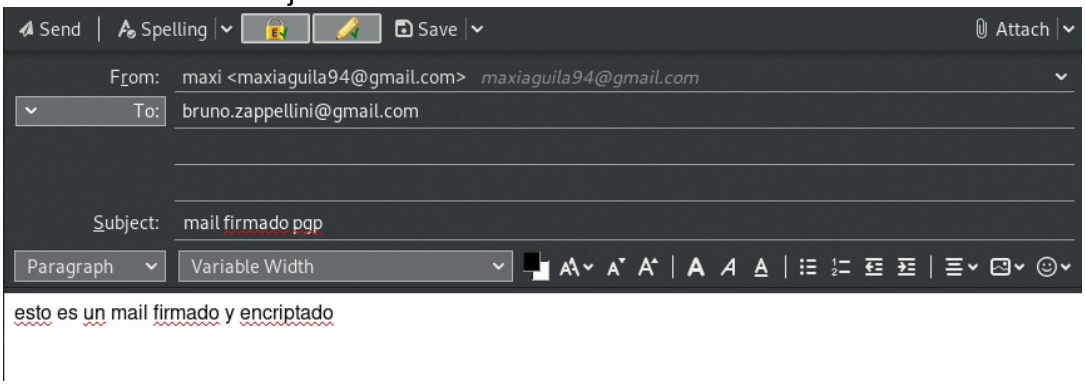
14. Dentro del administrador de claves, incorpore la clave de su compañero a su anillo de claves, para ello:
a) “Servidor de Claves” → “Buscar Claves” e ingresando la dirección de mail que corresponda a su compañero.

b) Importe la misma a su anillo de claves.
c) Firme la clave de su compañero, a través de la opción “Firmar”.



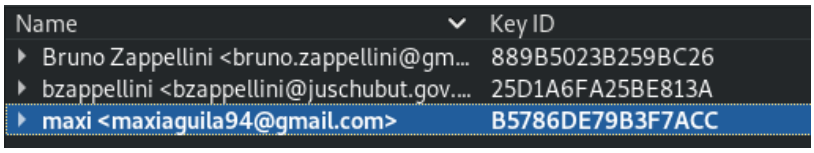
15. Utilizando el cliente de mail intercambie mails firmados y encriptados con su compañero usando las opciones:

“OpenPGP” → “Firmar Mensaje” y
“OpenPGP” → “Cifrar Mensaje”

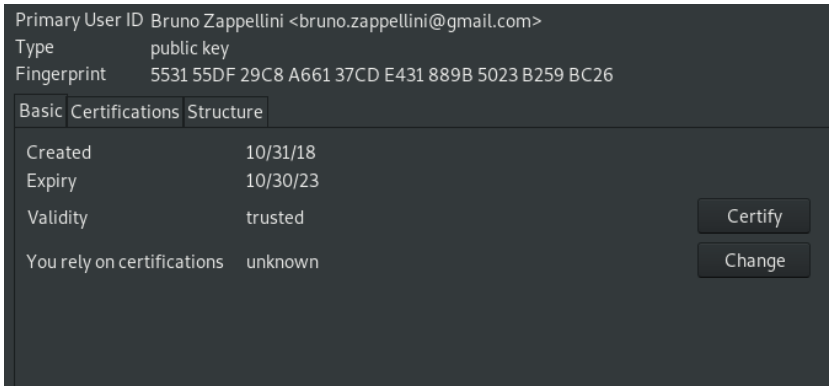


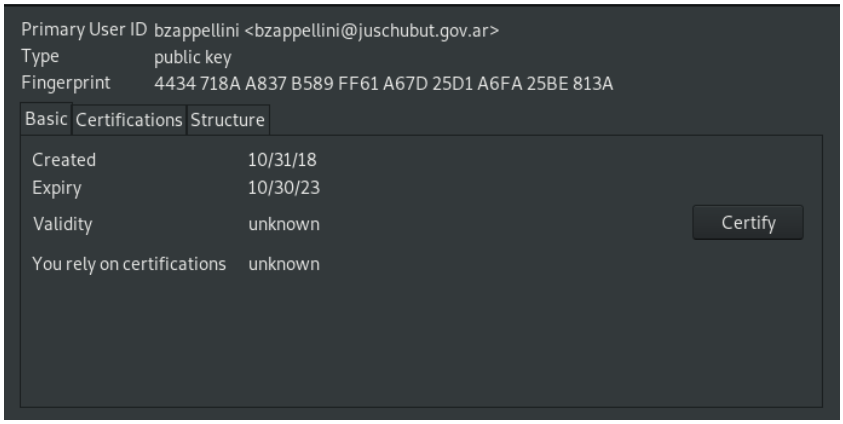

16. Trabajando con relaciones de confianza. Para ello se plantearán distintos casos a probar, teniendo en cuenta que:

a) En el Servidor de claves se encuentran publicadas las claves de:
1) bruno.zappellini@gmail.com
2) bzappellini@juschubut.gov.ar, la cual está firmada por bruno.zappellini@gmail.com (indicando que este último usuario confía en que la clave pública de bzappellini@juschubut.gov.ar es de quien dice ser)




b) Dentro del administrador de claves busque e incorpore ambas claves.
Ahora confíe en el usuario bruno.zappellini@gmail.com, dándole el mayor nivel de confianza posible.






c) ¿Qué ocurre con respecto a la validez de la otra cuenta bzappellini@juschubut.gov.ar? Para comprenderlo seleccione dicha clave e elija la opción ”Ver Firmas”

_ Una cuenta (bruno.zappellini@gmail.com) esta verificada y validada con el maximo nivel de confianza posible. Mientras que la otra (bzappellini@juschubut.gov.ar) no esta validada.

17. Analice distintos resultados que se obtienen al cambiar la confianza que ha establecido respecto a la clave de algún compañero (haga las pruebas usando la opción “Establecer confianza del propietario”).

18. ¿Qué información es necesaria para que quien recibe un mail firmado, pueda verificar la firma del mismo?

_ El receptor necesita la CLAVE PUBLICA

19. ¿Qué información necesito para poder enviar un mail encriptado?

_ La CLAVE PUBLICA del receptor

20. ¿Qué información es necesaria para que quien recibe un mail encriptado, pueda abrirlo?

_ Su CLAVE PRIVADA para desencriptar el mail

### 3.2.3. Tercera parte: Criptografía Simétrica y esteganografía

**Cifrando archivos con gpg(GnuPG) en forma simétrica:**

23. Cree un archivo y encríptelo:

a) Genere un archivo cualquiera, por ejemplo con:
echo ‘‘Mensaje secreto para Alberto’’ >archivo.txt

b) Para encriptar el archivo, desde una terminal y parado en el mismo directorio, ejecutar:
*gpg -c archivo.txt*
Introduzca una clave para cifrar el archivo y la confirmación de la clave.

d) Ahora archivo.txt esta en texto claro y archivo.txt.gpg esta cifrado.


mensaje.txt

```
Este es mi mensaje secreto y que nadie puede ver :O
```

mensaje encriptado con gpg

```
Ë
<0x04><0x07><0x03><0x02>M<0x1e>éÇ=ÆIÕïÒo<0x01>ÞT    «®Ş<0x16><0x15><0x14>®]BžP~ý)
â<0x81>†ªõ"$Æõrc¸HÚ©ß•úM½ÞÂÒû·Š<0x1f><0x05><ó‰—ÉE<0x8d>UÍ°
î–È³yî¿<0x8d>]Ù±<0x1b><0x03>¨<0x1f>+è|²Ž<0x15>â"g<0x14>\×è=ù?G‰<0x0e>4k<0x13><0x0b>V%2SÒÖB:˜¿tN<0x0f>
```

e) Haga las pruebas que considere necesarias. Lea las páginas del manual para obtener información acerca del algoritmo de cifrado.

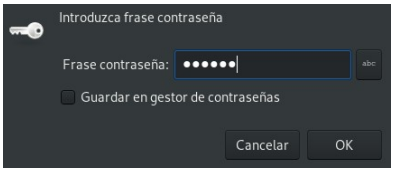
_ GPG no usa algoritmos de software que están restringidos por patentes. En su lugar usa una serie de algoritmos no patentados como ElGamal, CAST5, Triple DES (3DES), AES y Blowfish.

f ) Intercambie archivos cifrados con sus compañeros.

g) Para desencriptar pruebe:

*gpg -d archivo.txt.gpg*

```
➜ TP3 gpg -d mensaje.txt.gpg
gpg: datos cifrados AES
```



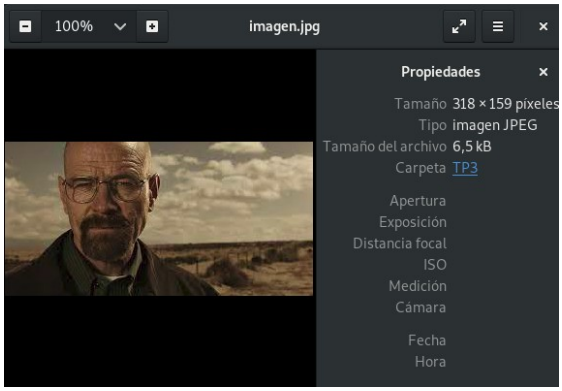

```
➜ TP3 gpg -d mensaje.txt.gpg
gpg: datos cifrados AES
gpg: cifrado con 1 frase contraseña
Este es mi mensaje secreto y que nadie puede ver :O
```

**Esteganografía**

24. Oculte un archivo de texto en una imagen a través del siguiente comando:
steghide embed -cf[nombre imagen ]-ef [nombre archivo a ocultar ]

```
➜  TP3 ls
Certificados  imagen.jpg  mensaje.txt  mensaje.txt.gpg  PracticaARyS.pdf  TP3.odt
➜  TP3 steghide embed -cf imagen.jpg -ef mensaje.txt
Anotar salvoconducto:
Re-ingresar salvoconducto:
adjuntando "mensaje.txt" en "imagen.jpg"... hecho
```

25. Visualice la imagen que contiene el archivo oculto




26. Extraiga el archivo oculto de la imagen a través del siguiente comando:
steghide extract -sf [imagen con steganografia ]

```
➜  TP3 steghide extract -sf imagen.jpg
Anotar salvoconducto:
anot❓los datos extra❓os e/"mensaje.txt".
➜  TP3
```