

# Práctica 1.1 - Retos de cifrado simétrico y asimétrico

## Incidentes de Ciberseguridad



C.E. en Ciberseguridad en Entornos de las Tecnologías de la Información  
IES Mar de Cádiz - El Puerto de Santa María  
2024/2025



- [Enunciado](#)
  - [Ejercicio 1: Hay dos archivos con mensajes cifrados de forma algorítmica. Descífralos.](#)
  - [Ejercicio 2: En este ejercicio vamos a trabajar en grupos de dos personas. El objetivo es usar gpg para el envío de mensajes cifrados. Concretamente vamos a realizar lo siguiente:](#)
- [Resolución](#)
  - [Ejercicio 1: Hay dos archivos con mensajes cifrados de forma algorítmica. Descífralos.](#)
    - [Reto 1](#)
    - [Solución](#)
    - [Reto 2](#)
    - [Solución](#)
  - [Ejercicio 2: En este ejercicio vamos a trabajar en grupos de dos personas. El objetivo es usar gpg para el envío de mensajes cifrados. Concretamente vamos a realizar lo siguiente:](#)
    - [1. Generar unas claves para nuestro equipo.](#)
    - [2. Exportar nuestra clave.](#)
    - [3. Importar las claves de gpg de otro compañero.](#)
    - [4. Listar todas las claves privadas y listar todas las claves publicas](#)
    - [5. Crea un archivo .txt y escribe un texto fácil en él. Cifra dicho archivo con la clave pública del receptor \(tu compañero\). Envíale ese archivo cifrado.](#)
    - [6. Descifra el archivo recibido con nuestra clave privada.](#)
- [Bonus](#)
- [Conclusión](#)
- [Bibliografía](#)



# Enunciado

**Ejercicio 1: Hay dos archivos con mensajes cifrados de forma algorítmica. Descífralos.**

**Ejercicio 2: En este ejercicio vamos a trabajar en grupos de dos personas. El objetivo es usar gpg para el envío de mensajes cifrados. Concretamente vamos a realizar lo siguiente:**

1. Generar unas claves para nuestro equipo.
2. Exportar nuestra clave.
3. Importar las claves de gpg de otro compañero.
4. Listar todas las claves privadas.
5. Listar todas las claves públicas.
6. Crea un archivo .txt y escribe un texto fácil en él. Cifra dicho archivo con la clave pública del receptor (tu compañero). Envíale ese archivo cifrado.
7. Descifra el archivo recibido con nuestra clave privada.

Si no hubiera grupos de dos personas, se puede realizar en grupos de 3, pero cada uno debe generar sus claves.



# Resolución

## Ejercicio 1: Hay dos archivos con mensajes cifrados de forma algorítmica. Descífralos.

### Reto 1

#### Descripción

Desde la creación del instituto, algunos alumnos se han encargado de la gestión del periodico local, "El noticiero", donde se intercambian mensajes y escriben artículos didácticos. En uno de los artículos alguien anónim@ ha lanzado un reto. Asegura haber escondido un mensaje en el libro más universal de la literatura castellana. En su mensaje advierte que para empezar, nos proporciona algunas coordenadas para que las mentes mas brillantes del instituto puedan resolverlo.

#### Pregunta

¿Cuál es el mensaje secreto que ha enviado el alumno anónimo y ha escondido este alumn@?

#### Datos proporcionados

Libro: "El quijote de la mancha"

10:8:2

23:11:1

30:8:2

30:26:7

35:1:7

151:19:10

151:11:8

152:11:5

### Solución

Para solucionar este reto tenemos que coger las coordenadas que nos ofrecen, estas son La pagina, la linea de texto y la palabra, dando como resultado:

10:8:2 - Querer

23:11:1 - Saber

30:8:2 - noticia

30:26:7 - sobre

35:1:7 - conocer

151:19:10 - misterio



151:11:8 - quien

152:11:5 - hizo

Querer saber noticia sobre conocer misterio quien hizo

## Reto 2

### Descripción

Después de muchos años recopilando documentación, fotos y artículos, se ha decidido realizar una limpieza y llevar la documentación antigua a una nueva sala que le ha cedido el instituto.

En esta sala se pueden archivar de una forma sencilla por fecha todos los documentos del periodico.

### Pregunta

Durante este proceso moviendo documentos, una hoja extraña se cae entre los documentos que llevais. Contiene un texto ilegible junto a la referencia del emperador Julio César.

¿Podrás sacar en claro que quería decir la nota?

Datos proporcionados:

Yn fvthvragr vasbeznpvba rf pbasvqrapvny. Gr nlhqnen n cebfrthve ra yn vairfgvtnpvba. Ab gr pbasvrf, ab gbqnf ynf vasbeznpvbarf qr ynf dhr qvfcbazbf fba gna snpvyrf pbzb rfgn ebgnpvba qr pnenpgrerf. Sveznqb: ha nzvtb.

`synt{rfgnzbf_rzcrmnaqb_n_pbabpre_nytb_qr_uvfgbev}`

## Solución

Nos hablan de que el texto estaba junto a una referencia de julio cesar, si buscamos en Google "código cesar" o similares nos aparecerá el Cifrado Cesar, una vez con esta información podemos buscar un descodificarlo online y nos dará el siguiente resultado una vez introduzcamos el texto.

El texto estaba cifrado en Cesar 13

La siguiente información es confidencial. Te ayudara a proseguir en la investigacion. No te confies, no todas las informaciones de las que disponemos son tan faciles como esta rotacion de caracteres. Firmado: un amigo.

`flag{estamos_empezando_a_conocer_algo_de_historia}`

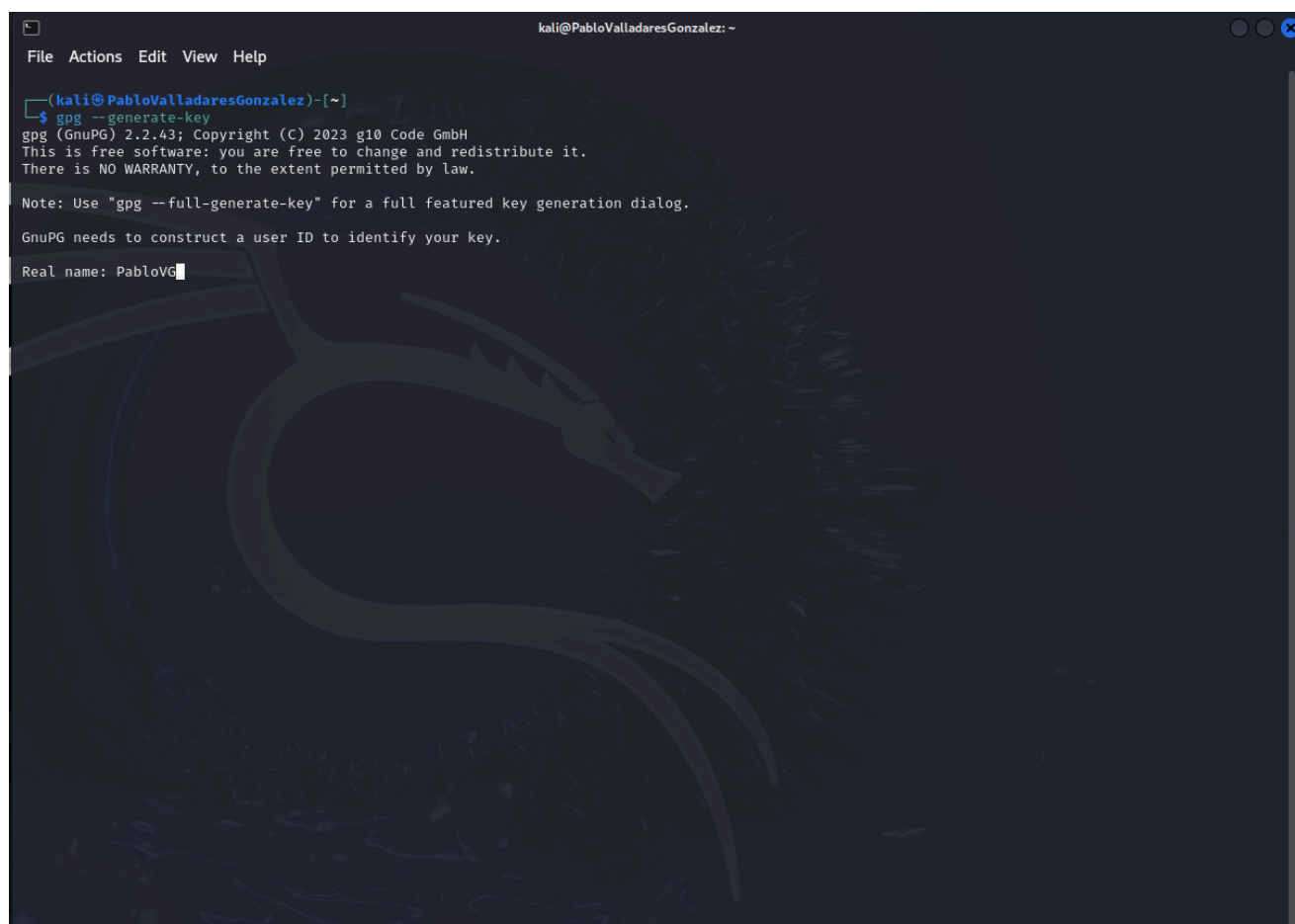


**Ejercicio 2: En este ejercicio vamos a trabajar en grupos de dos personas. El objetivo es usar gpg para el envío de mensajes cifrados. Concretamente vamos a realizar lo siguiente:**

## **1. Generar unas claves para nuestro equipo.**

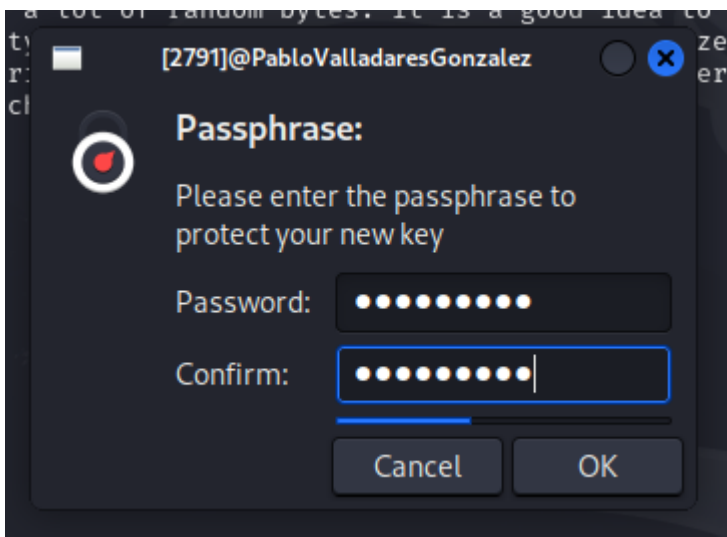
Para generar nuestras claves utilizaremos el comando `gpg --generate-key`

Una vez usemos dicho comando, nos pedira: Nombre y correo, despues de eso podremos ponerle una contraseña de manera opcional para mayor seguridad, en mi caso he puesto una contraseña para mayor seguridad ya que estamos en un ciclo relacionado con eso y hay que concienciar a la gente sobre ello.



```
kali@PabloValladaresGonzalez: ~  
File Actions Edit View Help  
  
(kali@PabloValladaresGonzalez)-[~]  
$ gpg --generate-key  
gpg (GnuPG) 2.2.43; Copyright (C) 2023 g10 Code GmbH  
This is free software: you are free to change and redistribute it.  
There is NO WARRANTY, to the extent permitted by law.  
  
Note: Use "gpg --full-generate-key" for a full featured key generation dialog.  
  
GnuPG needs to construct a user ID to identify your key.  
  
Real name: PabloVG
```





## 2. Exportar nuestra clave.

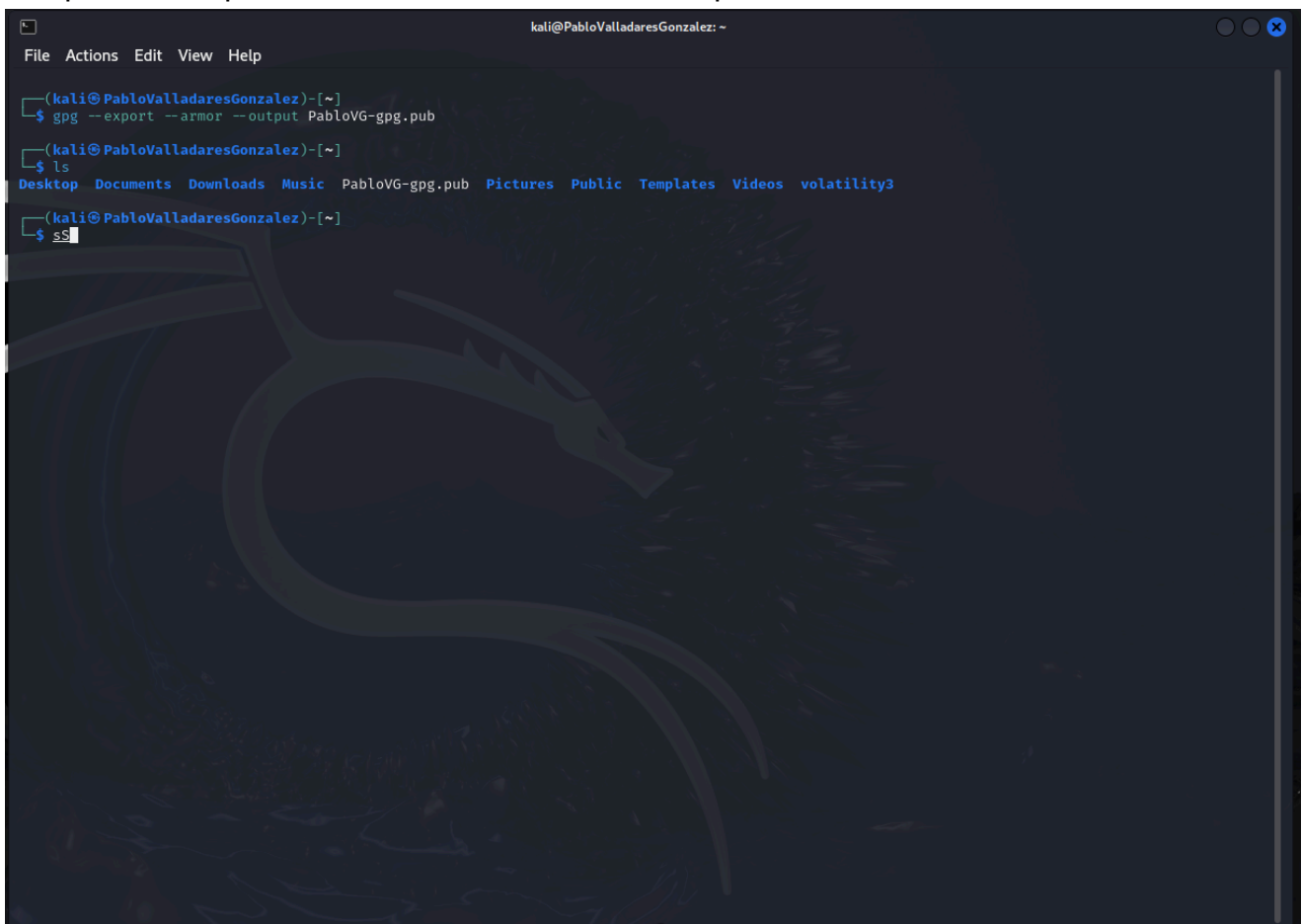
Para exportar nuestras claves tendremos que usar `gpg --export --armor -output fichero`

--export para exportarla

--armor para reforzar el código ASCII (created ASCII armored output)

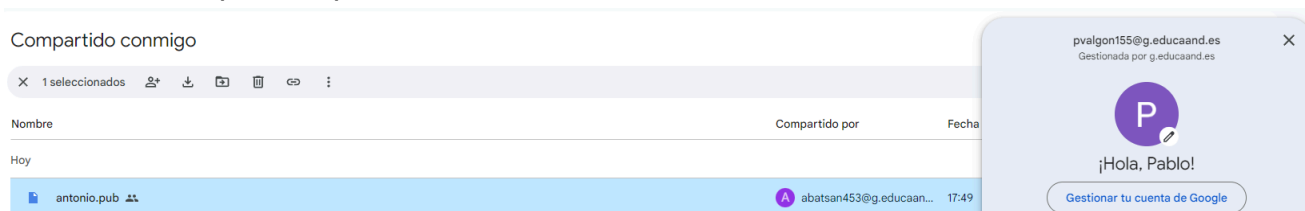
--output fichero para escoger el nombre del archivo que nos devuelve

Una vez usamos dicho comando, para comprobar que está creado, usamos el comando `ls` y comprobamos que esté en el directorio el archivo que acabamos de crear.



### 3. Importar las claves de gpg de otro compañero.

Para importar la clave de un compañero primero necesitaremos que este nos la pase, en mi caso nos la ha pasado por driver.



Una vez en el directorio con el archivo hacemos el siguiente comando `gpg --import fichero`

con este comando importaremos las claves de dicho fichero, tambien podemos hacerlo poniendo la ID, que por normal general sera lo que nos aparezca al hacer TAB

```
kali@PabloValladaresGonzalez: ~/Desktop
File Actions Edit View Help

(kali@PabloValladaresGonzalez)-[~/Desktop]
$ ls
antonio.pub  volatility

(kali@PabloValladaresGonzalez)-[~/Desktop]
$ gpg --import antonio.pub
gpg: key 99B4392CA747782F: public key "pablo <tete6307@gmail.com>" imported
gpg: key 124F5456DEAB3CC0: public key "antonio <tete6307@gmail.com>" imported
gpg: Total number processed: 2
gpg:          imported: 2

(kali@PabloValladaresGonzalez)-[~/Desktop]
$
```

### 1. Listar todas las claves privadas y listar todas las claves publicas

Para mostrar las claves publicas haremos el siguiente comando `gpg --list-public-keys`

Este comando mostrara todas las claves publicas, nos podemos asegurar de ello, ya que aunque parezca que es la privada, a la izquierda del todo pone pub de public, en vez de sec





de secret.

```
kali@PabloValladaresGonzalez: ~/Desktop
File Actions Edit View Help

(kali@PabloValladaresGonzalez)~/Desktop
$ gpg --list-public-keys
/home/kali/.gnupg/pubring.kbx

pub  rsa3072 2024-10-10 [SC] [expires: 2027-10-10]
     5C3D3808D2681D88F06F4631A8231218868A8A08
uid  [ultimate] PabloVG <pvalgon155@g.educaand.es>
sub  rsa3072 2024-10-10 [E] [expires: 2027-10-10]

pub  rsa3072 2024-10-10 [SC] [expires: 2027-10-10]
     9C58D0A3A21AF609CE24741699B4392CA747782F
uid  [ unknown] pablo <tete6307@gmail.com>
sub  rsa3072 2024-10-10 [E] [expires: 2027-10-10]

pub  rsa3072 2024-10-10 [SC] [expires: 2027-10-10]
     E0441ACAB5ECF185B8C6A7EA124F5456DEAB3CC0
uid  [ unknown] antonio <tete6307@gmail.com>
sub  rsa3072 2024-10-10 [E] [expires: 2027-10-10]

(kali@PabloValladaresGonzalez)~/Desktop
$ gpg --list-secret-keys
/home/kali/.gnupg/pubring.kbx

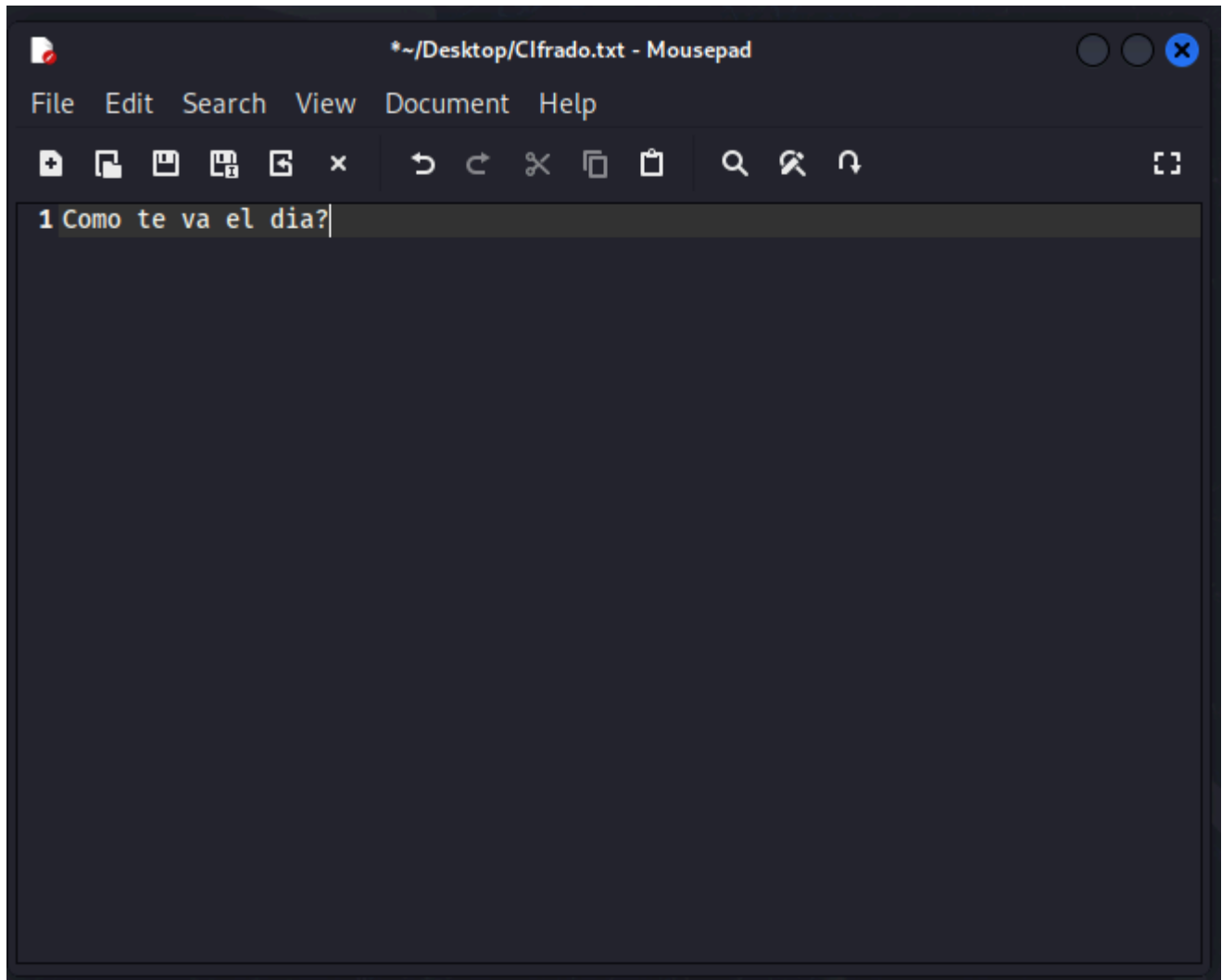
sec  rsa3072 2024-10-10 [SC] [expires: 2027-10-10]
     5C3D3808D2681D88F06F4631A8231218868A8A08
uid  [ultimate] PabloVG <pvalgon155@g.educaand.es>
ssb  rsa3072 2024-10-10 [E] [expires: 2027-10-10]

(kali@PabloValladaresGonzalez)~/Desktop
$
```

**5. Crea un archivo .txt y escribe un texto fácil en él. Cifra dicho archivo con la clave pública del receptor (tu compañero). Envíale ese archivo cifrado.**



Creamos el archivo con un texto sencillo, en este caso con el texto de "Como te va el dia?"



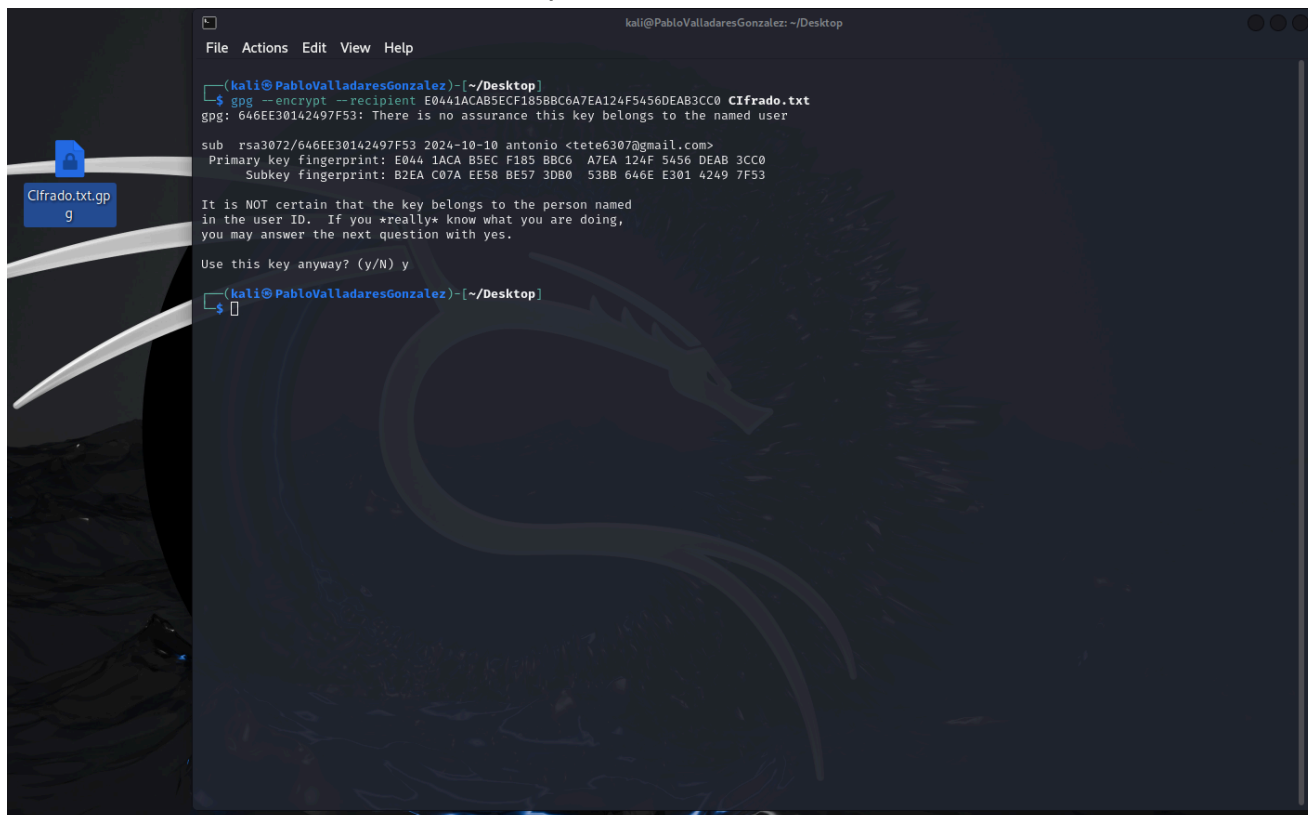
Para encryptarlo usaremos el comando `gpg --encrypt --recipient ID fichero`

--encrypt para encriptarlo

--recipient ID para escoger con que clave vamos a encriptarlo



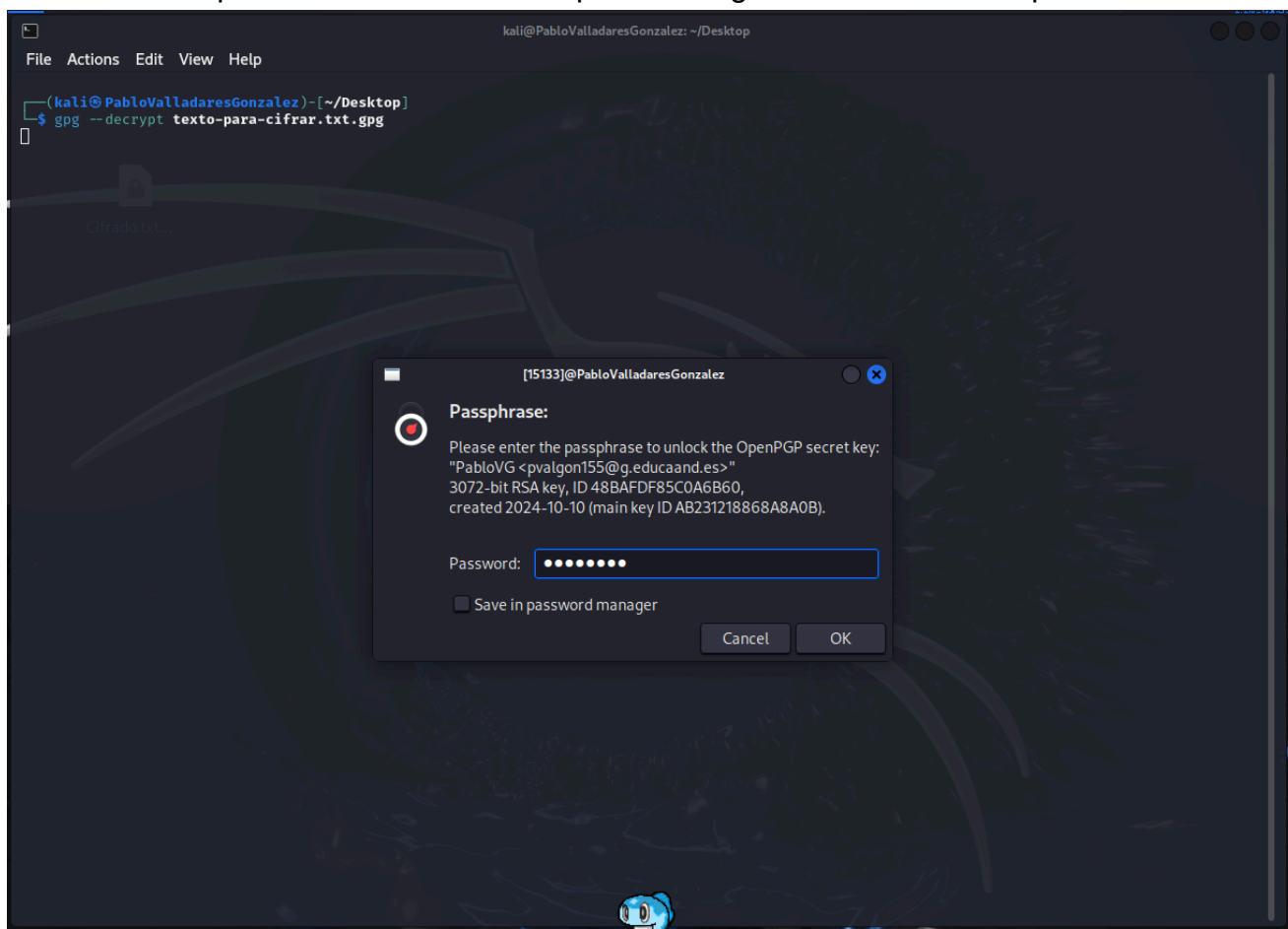
fichero, el nombre del archivo a encriptar



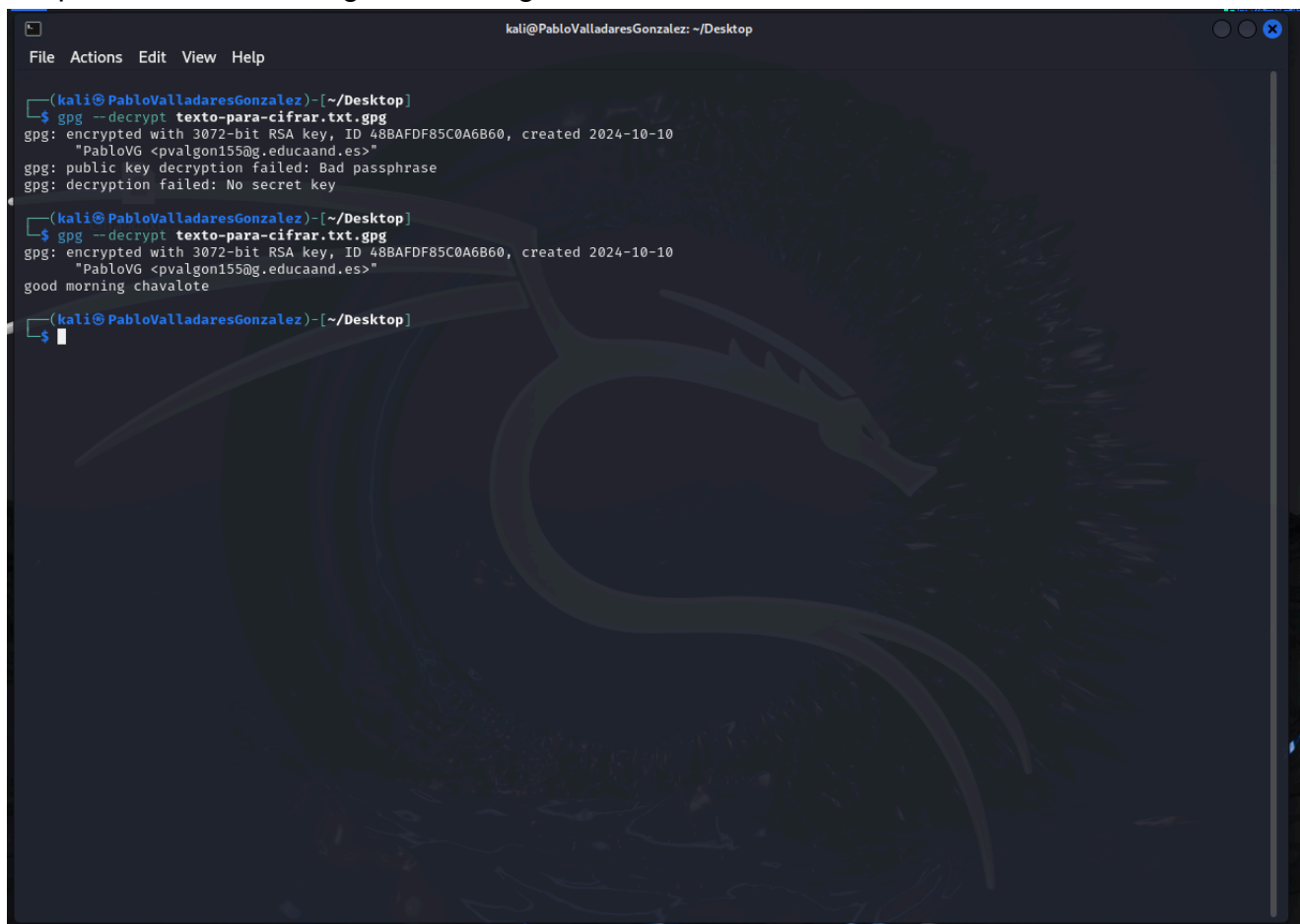
## 1. Descifra el archivo recibido con nuestra clave privada.

Para descifrar un archivo haremos el comando `gpg --decrypt fichero`

En el caso de que nuestra clave de encriptacion tenga contraseña nos la pedira.



Como podemos ver, una vez hemos hecho el comando, nos mostrara el mensaje justo despues, en este caso "good morning chavalote"

A terminal window titled 'kali@PabloValladaresGonzalez: ~/Desktop' with a menu bar (File, Actions, Edit, View, Help). The terminal shows a GPG decryption process. The user runs 'gpg --decrypt texto-para-cifrar.txt.gpg'. The output shows the file was encrypted with a 3072-bit RSA key and that decryption failed due to a bad passphrase. The user then runs 'gpg --decrypt texto-para-cifrar.txt.gpg' again, and the output shows the file was encrypted with a 3072-bit RSA key and that decryption failed due to a bad passphrase. Finally, the user runs 'gpg --decrypt texto-para-cifrar.txt.gpg' a third time, and the output shows the file was encrypted with a 3072-bit RSA key and that decryption failed due to a bad passphrase. The terminal background features a large, faint, stylized dragon logo.

```
(kali@PabloValladaresGonzalez)-[~/Desktop]
$ gpg --decrypt texto-para-cifrar.txt.gpg
gpg: encrypted with 3072-bit RSA key, ID 48BAFDF85C0A6B60, created 2024-10-10
"PabloVG <pvalgon155@g.educaand.es>"
gpg: public key decryption failed: Bad passphrase
gpg: decryption failed: No secret key

(kali@PabloValladaresGonzalez)-[~/Desktop]
$ gpg --decrypt texto-para-cifrar.txt.gpg
gpg: encrypted with 3072-bit RSA key, ID 48BAFDF85C0A6B60, created 2024-10-10
"PabloVG <pvalgon155@g.educaand.es>"
good morning chavalote

(kali@PabloValladaresGonzalez)-[~/Desktop]
$
```



## Bonus

Como podemos ver, si abrimos el archivo de la llave publica. nos aparecera el texto asi. de esta forma podemos comprobar que la llave es la publica, ya que lo pone y esta completamente bien.

```
(kali@PabloValladaresGonzalez)-[~/Desktop]
$ cat PabloVG-gpg.pub
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBGcH9SwBDADEYicrxgGn+vmdrifS2Q+cL9J/Oi5/yN2SzYrsjSkWBKmxeofz
4THL9gCg+PXn2rS2zGA/+nmfLvJTawwy68iyXPAeKm5v5R6CrA6xqBRwJB5/NvUm
iCKpK32xk8v94xbyKj0AKd/naQPSqMDFFRStSi0Isr6vwRf60SAIj5v3JzGd91NU
ElOn4kIVOLwJXEks1UIgvHvUdQHSgU808+iAqIYmmB14T1iPgJddqmmur08MR8o3
iPUWfpcLSXDwx1DLuLgqT6fAaX/5CYuLoEtZv8IN23pNpd0kv+pxg6TBELa+pxY8
aKAb9q1BzXBPNXuhGwC2tiTXBuGNmf40BCYIBs3xxFUZimjeuKpRKo3gbpTABTHK
kc0dCHxeFVOAXoJwrJkkNVaPa8qiU+YBee0ILI75EZtDPHjKKA2f3+URwfMr3MZ3
lmS+/vsUKBCvmp34pf3vaxyB/9XhDAZGHUqu2kxaB27GtUFyp2r+/eSGtgstPY31
CAJaHAJvCIeEaw0AEQEAABQiUGFibG9WRyA8cHZhbGdvbjE1NUBnLmVkdWNhYW5k
LmVzPokB1AQTAAQAPhYhBFw90AjsSax248G9GMasjEhiGiooLBQJnB/UsAhsDBQkF
o5qABQsJCACBhUKCQgLagQWAgMBAh4BAheAAAOJEKsjEhiGiooLZcwL/2eWlFzk
0Qd1c9I0MNP3oUwoCTLzUgndEMaYfyBhzsrcY/yHJslDh3Ix/g4r4IOSrEO9WGr
sNqB/kphUd2xt04PCNaRPl+KRARj5n/ZCT3hF/oWJXYKe1EcFxc2AWJzuP02Fuq6
t1K8ZbZHxBN9/N/jlOYANmyEafNfgo5htHYH5t7mQ489Th0/zDY0PxWV2ZEyN7q/
jXb8qxDyAqZgAK/RJAeNvRhYhAOp8cJpiivBW7hODIALrBk0ssQG8VTwgHbfa3p
5RVDCh2eMk07woYssXQeBtCQH36goIoLoCqUpezZAozsGe1jv3xblv+f/eUGcSW9
W4mTUPXckWrcNQlhm8oeU+zKo05l5ID0hYSQHDke5FWTeDI6F23yvNsBfWyd4vS2
+TDetBKXa7FYjkwI7ANno09/41CqayJfMu+Zplk48gHl0lPALIEYFSIp0mhVJui+
wkdIH7Y59PuepZ1rcym2nv5wgBSm6raF5k2jCm/gZxbLmVypJQc6NIHQ6bkBjQRn
B/UsAQwAuDQCYa3jz/83cabTBM1G6yPPxl4eMY7k9vvhdQah9037bmNP7XlmLdV
oyNqmYcCTQmR7M21SYZWqOPGSl02rjmk2zk57dbUeEliu1qyNc70qLeRjIX4Xmq
jFsdTFXzRuIFvFiVc9nehvNj+bvc2o84yB/R03HRzH/U0uP8EnDGjIlinR/Vd8v
gmfZH/1qMLZdrfjesUdRA+9SFIpdW6uSsOG9+GgPpiE+nvb0sR07wm1FJuxnHoQi
lmsZZBq8gBototon2EE2wIFx80Cy6r4QTHDHJrrFsOgjF9dIbs9gP2G4yaQ6Mn4K
x0H1/aA/bnjAjCU+RQRX8AxKIEbF/kAGhNsfgbqLB5mf5JkpCeU+0c1wyRPzXbV5
PiVsR+p88o0UfCEG8ys9gjj5qpgmIAMV6kc62cmV4709i4Zc1Yp0G9NNPCMsRdr7
u7quI10XBACIMIEkXa07PfUIQp9gFdICM3fwYP58s7bdo2k+SUQjiU/ki3BvmoKp
N30/hAQVABEBAAGJAbwEGAEEKACYWIQRcPTgI0msduPBvRjGrIxIYhoqKCwUCZwf1
LAIbDAUJBA0agAAKCRcRixIYhoqKC3rhC/0eHtnk6Mh+pv3NTjZuK9p9D/JTLoLJ
aiqd4dFift7KLp79m8BHvTPWbJ0RDGP8d6ki7KmvIQDwb0wnCi4e1McTuWaUeKOi
EPRXi2sFBCu2ni2rfzYo/o0UWqvm4XbCLt/jdBzrJDerw6KuuGK3CCK38phufy
UB+EBOKkP67+y9M47DI8mKtNPa2C1RbSAuVluc82oKlTygqMidi3qMo2HR4Wgn20
nIrTrr0VUwbGGs+XuJOA31LvQJBzaCaGmacI3/CZvJGj+ZAlefLUZQVueMZERVV6
eQqF8fwgURJLWSjt382m+MvZStDI+H1aNPvUXa2WAvKutptIleGzt4QQg+f+s5iw
tvXYf9pmquH7D0sywMp9c6Lo7s/S73wpExbAgYY+rhKc2opmDetvNypr2+umq6ea
/adg3FVUsMRu06C250AbcQVMqKTPw3TPts5XZA/UzzPYBlXtGYoMSqjtnuJVW6as
AKqLn+bU+9CwY7TMT028g82nn990zs5PM6U=
=jnxV
-----END PGP PUBLIC KEY BLOCK-----

(kali@PabloValladaresGonzalez)-[~/Desktop]
$ █
```



# Conclusión

Creo que hay muchas formas de poder ser atacado y es necesario ir con precaución cuando tratamos información sensible o importante que necesita de confidencialidad, como hemos visto hay ataques de interceptación (Sniffing) y modificación (Man in the middle) de los cuales podemos ser víctimas cuando mandamos alguna información por internet, creo que a la hora de enviar un documento muy importante, como podría ser datos de la cuenta bancaria o personales. Si los encriptamos nos aseguramos de tener una mayor fiabilidad de que no nos pase nada, creo que es útil el saber este tipo de cosas, aunque por normal general no vayamos a hacerlo siempre. Para cuando queremos ese extra o somos paranoicos es algo muy útil de saber.

No creo que vaya a usarlo demasiado en mi vida personal, pero si que creo que debería ser una practica habitual cuando pasamos información sensibles a terceros aunque pueda llegar a ser mas incomodo, como una frase famoso que dice "A mayor seguridad, mayor incomodidad".



# Bibliografía

gcg --help (con la ayuda del comando | grep palabra, cuando sabia que podía estar relacionado con algo)

<https://medium.com/@biicaleb316/how-to-perform-encryption-and-decryption-with-kali-linux-using-gpg-gnu-privacy-guard-utility-fc5915644bff>

[Red Hat](#)

[Stack Exchange / superuser](#)

[David Poza](#)

