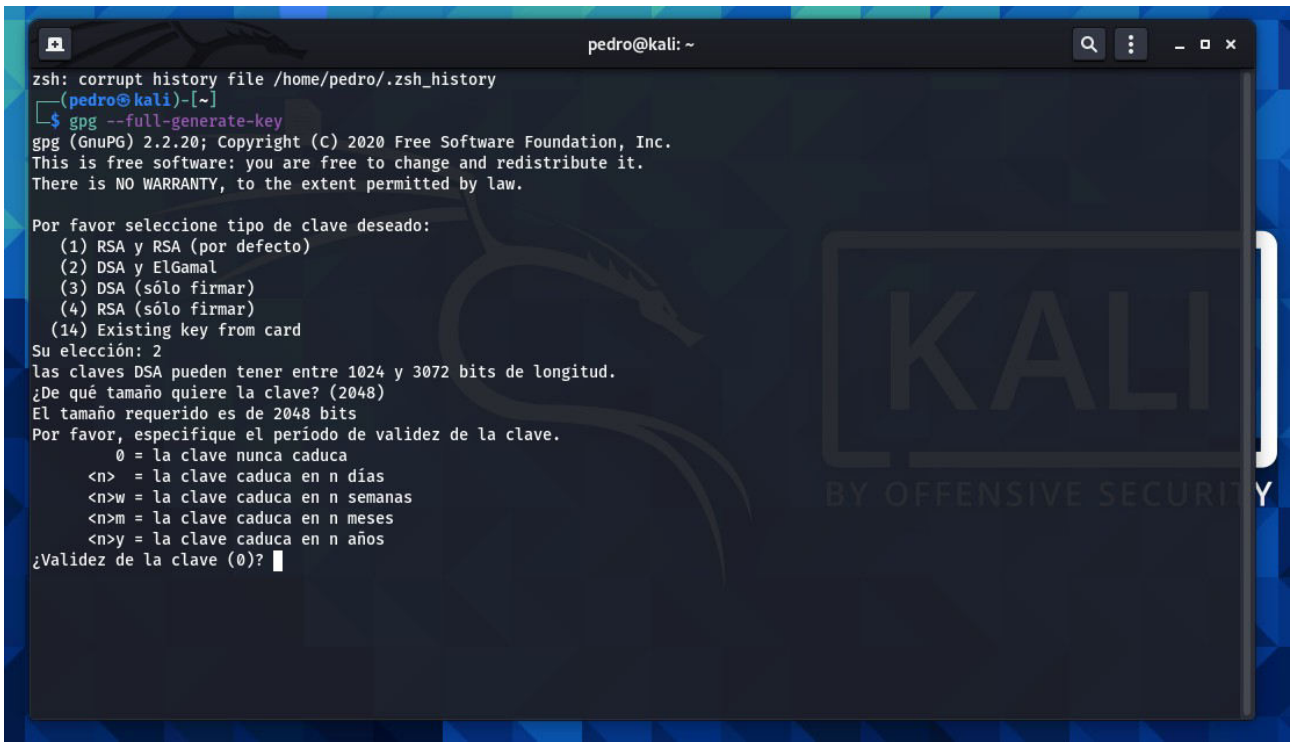
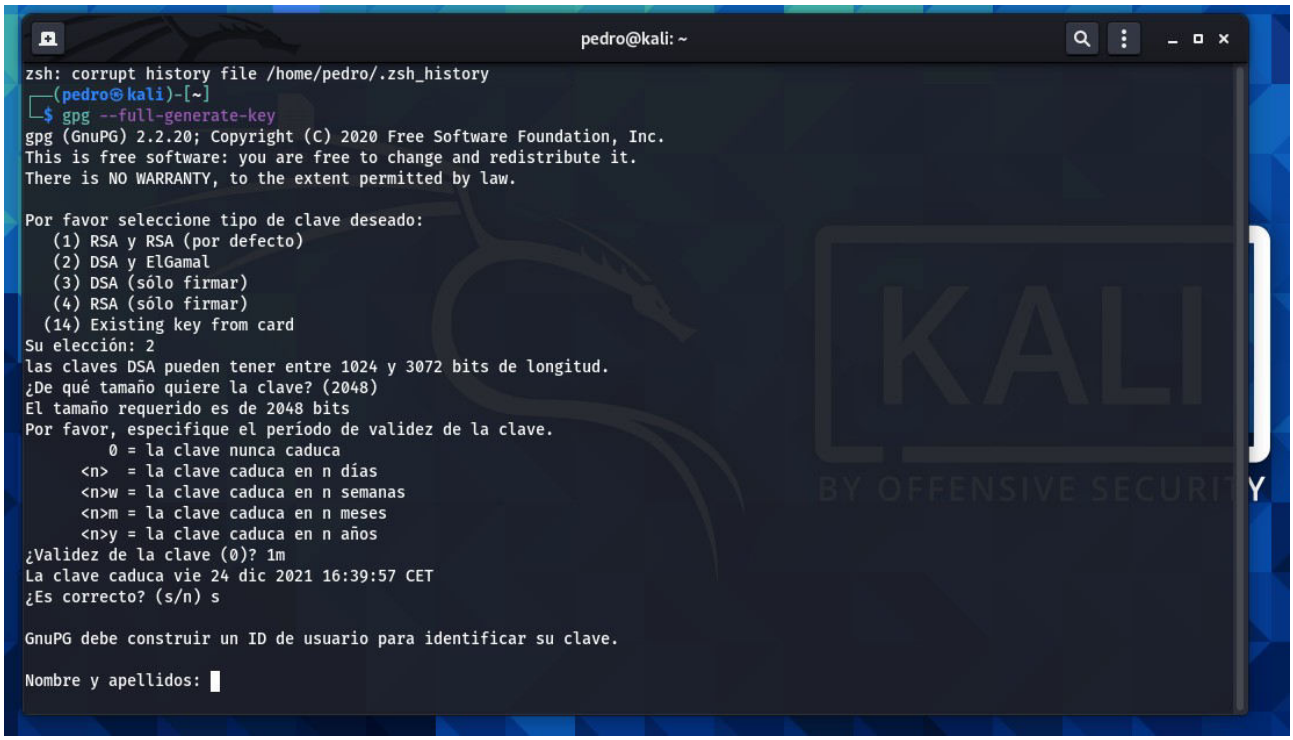
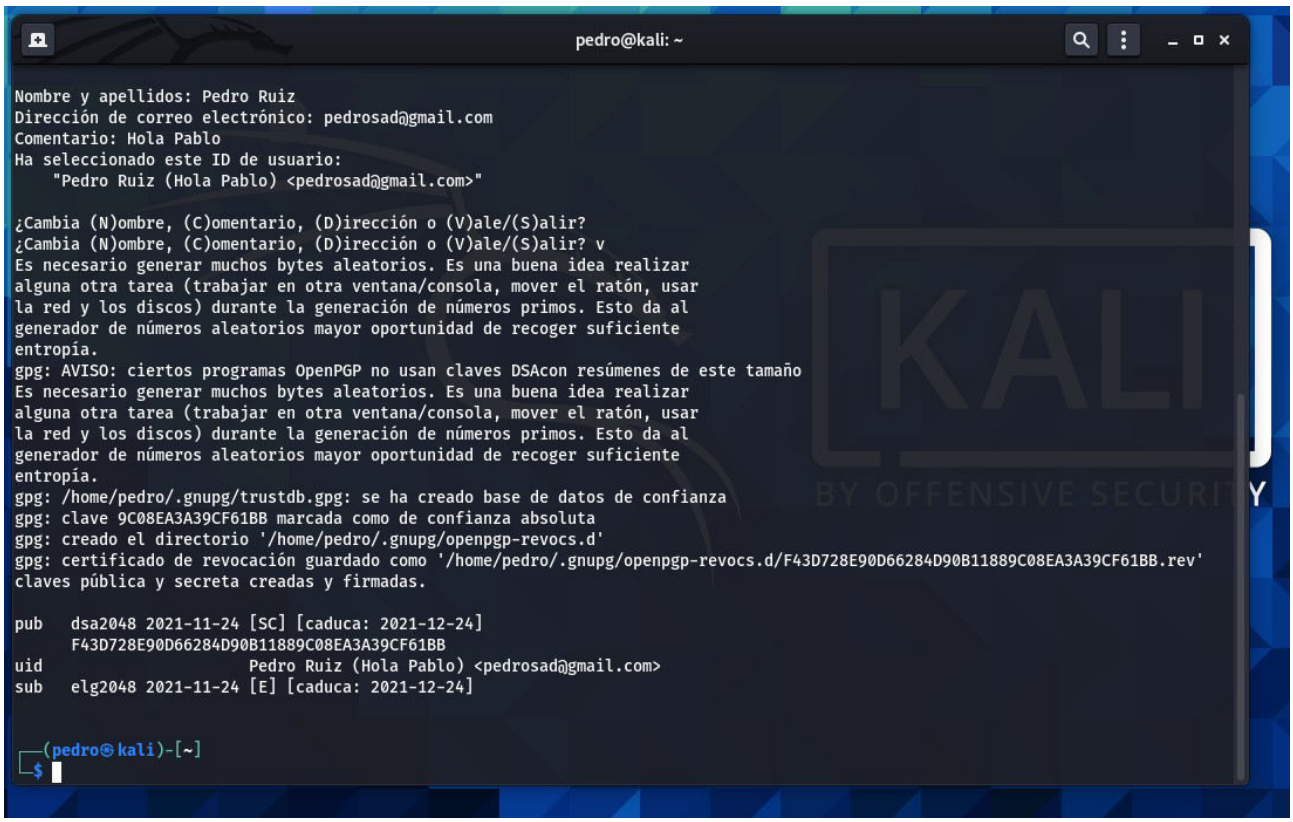
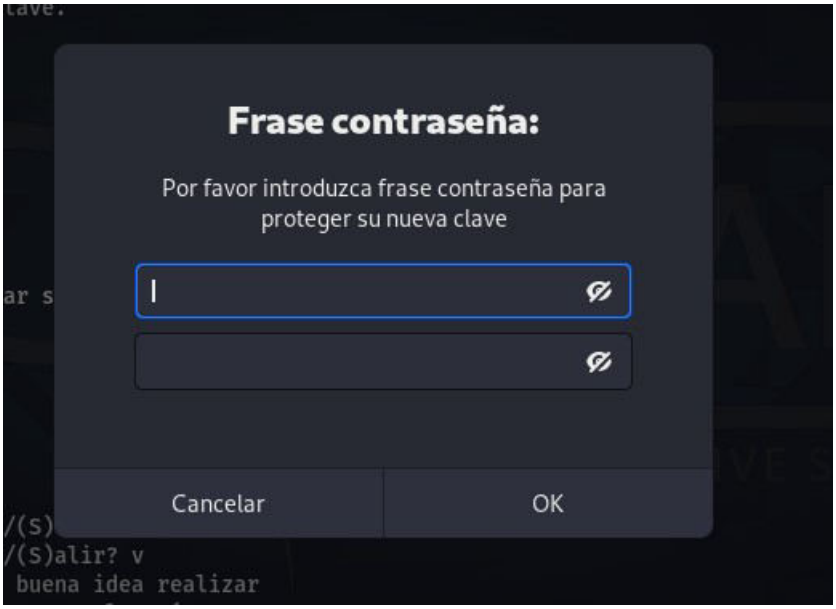
ANEXO CIFRADO ASIMÉTRICO

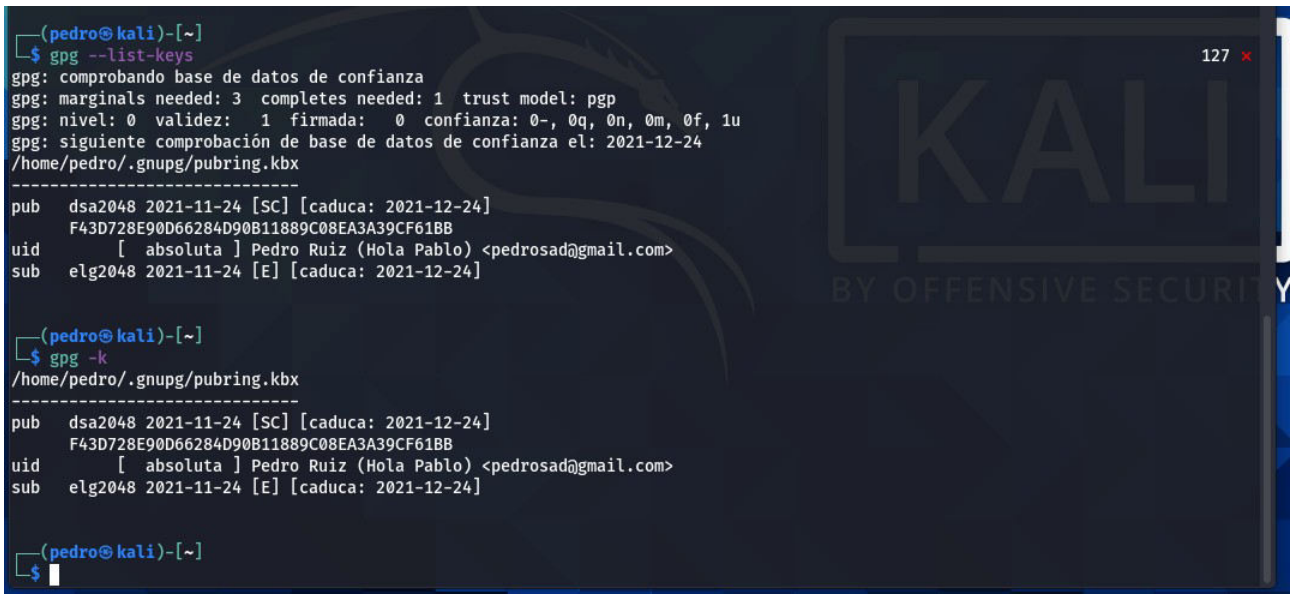
PEDRO RUIZ NUÑEZ


pedro@kali: ~
zsh: corrupt history file /home/pedro/.zsh_history
(pedro㉿kali)-[~]
$ gpg --full-generate-key
gpg (GnuPG) 2.2.20; Copyright (C) 2020 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.
Por favor seleccione tipo de clave deseado:
(1) RSA y RSA (por defecto)
(2) DSA y ElGamal
(3) DSA (sólo firmar)
(4) RSA (sólo firmar)
(14) Existing key from card
Su elección: 2
las claves DSA pueden tener entre 1024 y 3072 bits de longitud.
¿De qué tamaño quiere la clave? (2048)
El tamaño requerido es de 2048 bits
Por favor, especifique el período de validez de la clave.
0 = la clave nunca caduca
<n> = la clave caduca en n días
<n>w = la clave caduca en n semanas
<n>m = la clave caduca en n meses
<n>y = la clave caduca en n años
¿Validez de la clave (0)?

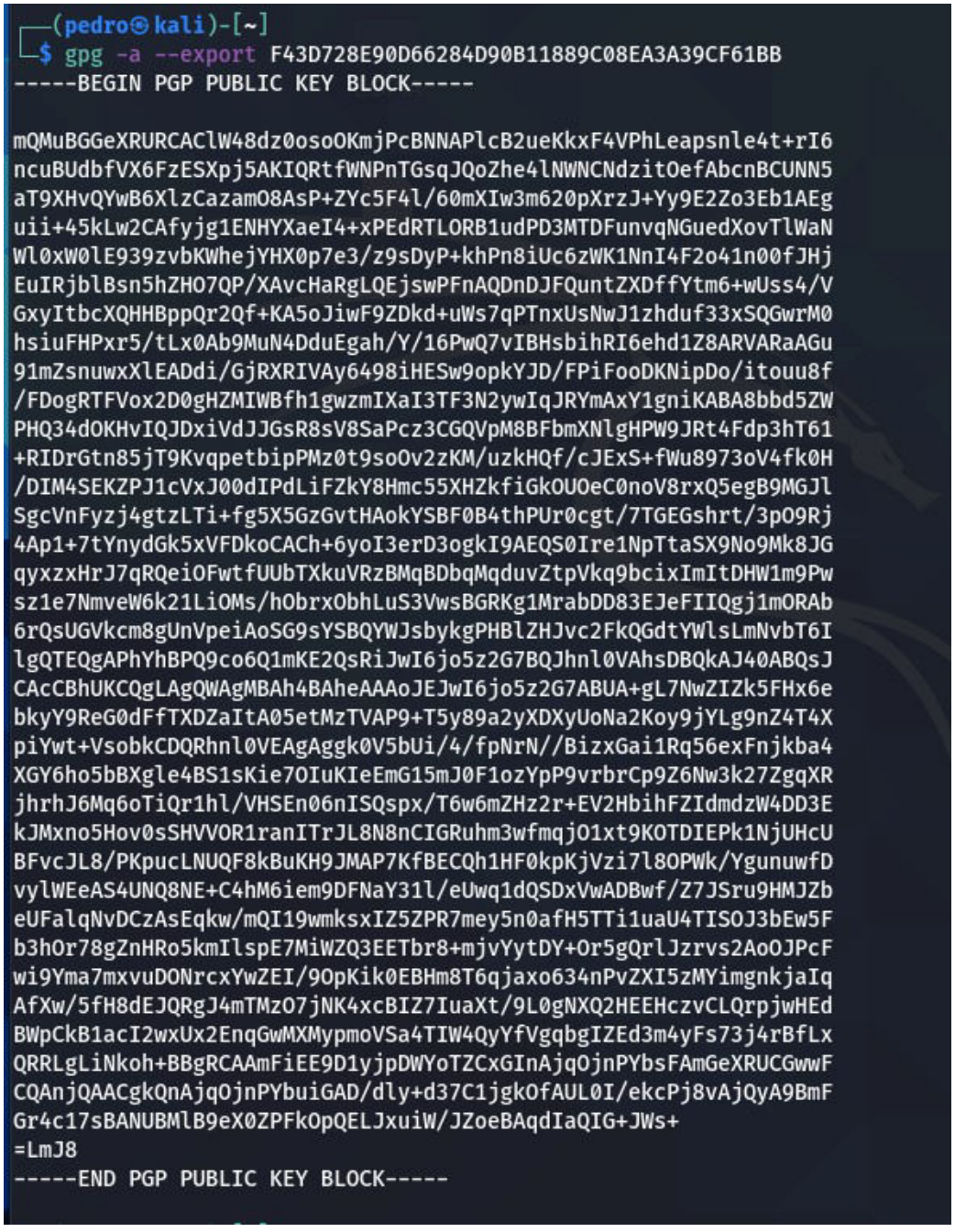

pedro@kali: ~
zsh: corrupt history file /home/pedro/.zsh_history
(pedro㉿kali)-[~]
$ gpg --full-generate-key
gpg (GnuPG) 2.2.20; Copyright (C) 2020 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Por favor seleccione tipo de clave deseado:
(1) RSA y RSA (por defecto)
(2) DSA y ElGamal
(3) DSA (sólo firmar)
(4) RSA (sólo firmar)
(14) Existing key from card
Su elección: 2
las claves DSA pueden tener entre 1024 y 3072 bits de longitud.
¿De qué tamaño quiere la clave? (2048)
El tamaño requerido es de 2048 bits
Por favor, especifique el período de validez de la clave.
0 = la clave nunca caduca
<n> = la clave caduca en n días
<n>w = la clave caduca en n semanas
<n>m = la clave caduca en n meses
<n>y = la clave caduca en n años
¿Validez de la clave (0)? 1m
La clave caduca vie 24 dic 2021 16:39:57 CET
¿Es correcto? (s/n) s
GnuPG debe construir un ID de usuario para identificar su clave.
Nombre y apellidos:


pedro@kali: ~
Nombre y apellidos: Pedro Ruiz
Dirección de correo electrónico: pedrosad@gmail.com
Comentario: Hola Pablo
Ha seleccionado este ID de usuario:
"Pedro Ruiz (Hola Pablo) <pedrosad@gmail.com>"
¿Cambia (N)ombre, (C)omentario, (D)irección o (V)ale/(S)alir?
¿Cambia (N)ombre, (C)omentario, (D)irección o (V)ale/(S)alir? v
Es necesario generar muchos bytes aleatorios. Es una buena idea realizar
alguna otra tarea (trabajar en otra ventana/consola, mover el ratón, usar
la red y los discos) durante la generación de números primos. Esto da al
generador de números aleatorios mayor oportunidad de recoger suficiente
entropía.
gpg: AVISO: ciertos programas OpenPGP no usan claves DSAcon resúmenes de este tamaño
Es necesario generar muchos bytes aleatorios. Es una buena idea realizar
alguna otra tarea (trabajar en otra ventana/consola, mover el ratón, usar
la red y los discos) durante la generación de números primos. Esto da al
generador de números aleatorios mayor oportunidad de recoger suficiente
entropía.
gpg: /home/pedro/.gnupg/trustdb.gpg: se ha creado base de datos de confianza
gpg: clave 9C08EA3A39CF61BB marcada como de confianza absoluta
gpg: creado el directorio '/home/pedro/.gnupg/openpgp-revocs.d'
gpg: certificado de revocación guardado como '/home/pedro/.gnupg/openpgp-revocs.d/F43D728E90D66284D90B11889C08EA3A39CF61BB.rev'
claves pública y secreta creadas y firmadas.
pub dsa2048 2021-11-24 [SC] [caduca: 2021-12-24]
F43D728E90D66284D90B11889C08EA3A39CF61BB
uid Pedro Ruiz (Hola Pablo) <pedrosad@gmail.com>
sub elg2048 2021-11-24 [E] [caduca: 2021-12-24]
(pedro㉿kali)-[~]
$


Frase contraseña:
Por favor introduzca frase contraseña para proteger su nueva clave
Cancelar
OK


(pedro㉿kali)-[~]
$ gpg --list-keys
127
gpg: comprobando base de datos de confianza
gpg: marginals needed: 3 completes needed: 1 trust model: pgp
gpg: nivel: 0 validez: 1 firmada: 0 confianza: 0-, 0q, 0n, 0m, 0f, 1u
gpg: siguiente comprobación de base de datos de confianza el: 2021-12-24
/home/pedro/.gnupg/pubring.kbx
pub dsa2048 2021-11-24 [SC] [caduca: 2021-12-24]
F43D728E90D66284D90B11889C08EA3A39CF61BB
uid [absoluta] Pedro Ruiz (Hola Pablo) <pedrosad@gmail.com>
sub elg2048 2021-11-24 [E] [caduca: 2021-12-24]
(pedro㉿kali)-[~]
$ gpg -k
/home/pedro/.gnupg/pubring.kbx
pub dsa2048 2021-11-24 [SC] [caduca: 2021-12-24]
F43D728E90D66284D90B11889C08EA3A39CF61BB
uid [absoluta] Pedro Ruiz (Hola Pablo) <pedrosad@gmail.com>
sub elg2048 2021-11-24 [E] [caduca: 2021-12-24]
(pedro㉿kali)-[~]
$


(pedro㉿kali)-[~]
$ gpg --output archivo --export F43D728E90D66284D90B11889C08EA3A39CF61BB
(pedro㉿kali)-[~]
$ gpg --send-keys --keyserver pgp.mit.edu
(pedro㉿kali)-[~]
$ gpg --send-keys --keyserver pgp.mit.edu F43D728E90D66284D90B11889C08EA3A39CF61BB
gpg: enviando clave 9C08EA3A39CF61BB a hkp://pgp.mit.edu

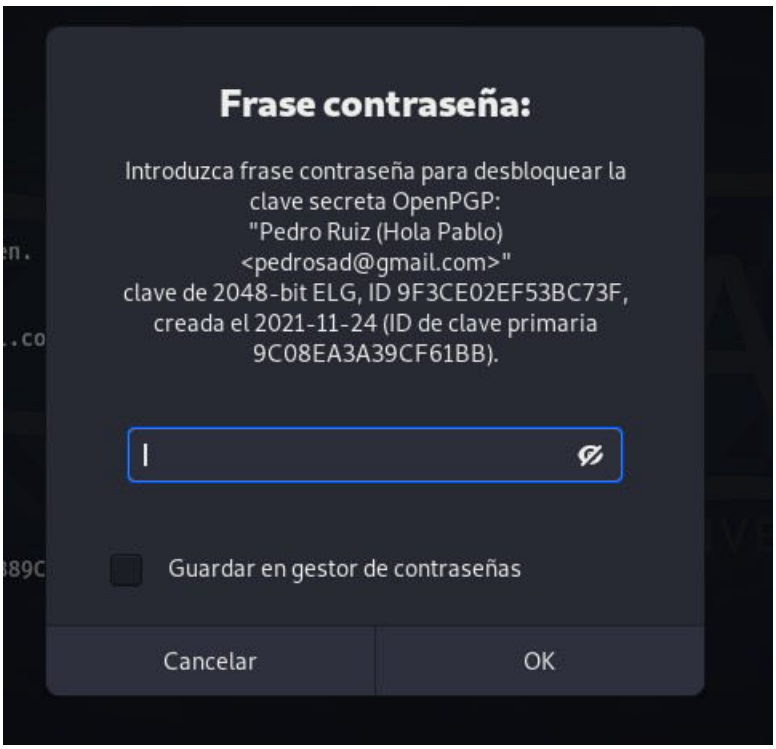

(pedro㉿kali)-[~]
$ gpg -a --export F43D728E90D66284D90B11889C08EA3A39CF61BB
-----BEGIN PGP PUBLIC KEY BLOCK-----
mQMuBGGeXRURCAClW48dz0osoOKmjPcBNNAPlcB2ueKkxF4VPhLeapsnle4t+rI6
ncuBUdbfVX6FzESXpj5AKIQRtfWNPnTGsqJQoZhe4lNWNCNdzitOefAbcnBCUNN5
aT9XHvQYwB6XlzCazamO8AsP+ZYc5F4l/60mXIw3m620pXrzJ+Yy9E2Zo3Eb1AEg
uii+45kLw2CAfyjg1ENHYXaeI4+xPEdRTLORB1udPD3MTDFunvqNGuedXovTlWaN
Wl0xW0lE939zvbKWhejYHX0p7e3/z9sDyP+khPn8iUc6zWK1NnI4F2o41n00fJHj
EuIRjblBsn5hZHO7QP/XAvcHaRgLQEjswPFnAQDnDJFQuntZXDffYtm6+wUss4/V
GxyItbcXQHHBppQr2Qf+KA5oJiwF9ZDkd+uWs7qPTnxUsNwJ1zhduf33xSQGwrM0
hsiuFHPxr5/tLx0Ab9MuN4DduEgah/Y/16PwQ7vIBHsbihRI6ehd1Z8ARVARaAGu
91mZsnuwxXlEADdi/GjRXRIVAy6498iHESw9opkYJD/FPiFooDKNipDo/itouu8f
/FDogRTFVox2D0gHZMIWBfh1gwzmIXaI3TF3N2ywIqJRYmAxY1gniKABA8bbd5ZW
PHQ34dOKHvIQJDxiVdJJGsR8sV8SaPcz3CGQVpM8BFbmXNlgHPW9JRt4Fdp3hT61
+RIDrGtn85jT9KvqpetbipPMz0t9soOv2zKM/uzkHQf/cJExS+fWu8973oV4fk0H
/DIM4SEKZPJ1cVxJ00dIPdLiFZkY8Hmc55XHZkfiGkOUOeC0noV8rxQ5egB9MGJl
SgcVnFyzj4gtzLTi+fg5X5GzGvtHAokYSBF0B4thPUr0cgt/7TGEGshrt/3pO9Rj
4Ap1+7tYnydGk5xVFDkoCACh+6yoI3erD3ogkI9AEQS0Ire1NpTtaSX9No9Mk8JG
qyxzxHrJ7qRQeiOFwtfUUbTXkuVRzBMqBDbqMqduvZtpVkq9bcixImItDHW1m9Pw
sz1e7NmveW6k21LiOMs/hObrxObhLuS3VwsBGRKg1MrabDD83EJeFIIQgj1mORAb
6rQsUGVkcm8gUnVpeiAoSG9sYSBQYWJsbykgPHBlZHJvc2FkQGdtYWlsLmNvbT6I
lgQTEQgAPhYhBPQ9co6Q1mKE2QsRiJwI6jo5z2G7BQJhnl0VAhsDBQkAJ40ABQsJ
CAcCBhUKCQgLAgQWAgMBAh4BAheAAAoJEJwI6jo5z2G7ABUA+gL7NwZIZk5FHx6e
bkyY9ReG0dFfTXDZaItA05etMzTVAP9+T5y89a2yXDXyUoNa2Koy9jYLg9nZ4T4X
piYwt+VsobkCDQRhnl0VEAgAggk0V5bUi/4/fpNrN//BizxGai1Rq56exFnjkba4
XGY6ho5bBXgle4BS1sKie7OIuKIeEmG15mJ0F1ozYpP9vrbrCp9Z6Nw3k27ZgqXR
jhrhJ6Mq6oTiQr1hl/VHSEn06nISQspx/T6w6mZHz2r+EV2HbihFZIdmdzW4DD3E
kJMxno5Hov0sSHVVOR1ranITrJL8N8nCIGRuhm3wfmqjO1xt9KOTDIEPk1NjUHcU
BFvcJL8/PKpucLNUQF8kBuKH9JMAP7KfBECQh1HF0kpKjVzi7l8OPWk/YgunuwfD
vylWEeAS4UNQ8NE+C4hM6iem9DFNaY31l/eUwq1dQSDxVwADBwf/Z7JSru9HMJZb
eUFalqNvDCzAsEqkw/mQI19wmksxIZ5ZPR7mey5n0afH5TTi1uaU4TISOJ3bEw5F
b3hOr78gZnHRo5kmIlspE7MiWZQ3EETbr8+mjvYytDY+Or5gQrlJzrvs2AoOJPcF
wi9Yma7mxvuDONrcxYwZEI/9OpKik0EBHm8T6qjaxo634nPvZXI5zMYimgnkjaIq
AfXw/5fH8dEJQRgJ4mTMzO7jNK4xcBIZ7IuaXt/9L0gNXQ2HEEHczvCLQrpjwHEd
BWpCkB1acI2wxUx2EnqGwMXMypmoVSa4TIW4QyYfVgqbgIZEd3m4yFs73j4rBfLx
QRRLgLiNkoh+BBgRCAAmFiEE9D1yjpDWYoTZCxGInAjqOjnPYbsFAmGeXRUCGwwF
CQAnjQAACgkQnAjqOjnPYbuiGAD/dly+d37C1jgkOfAUL0I/ekcPj8vAjQyA9BmF
Gr4c17sBANUBMlB9eX0ZPFkOpQELJxuiW/JZoeBAqdIaQIG+JWs+
=LmJ8
-----END PGP PUBLIC KEY BLOCK-----

```
┌──(pedro㉿kali)-[~]
└─$ gpg --import archivo
gpg: clave 9C08EA3A39CF61BB: "Pedro Ruiz (Hola Pablo) <pedrosad@gmail.com>" sin cambios
gpg: Cantidad total procesada: 1
gpg:               sin cambios: 1
```

```
┌──(pedro㉿kali)-[~]
└─$ gpg --keyserver pgp.mit.edu --recv-keys F43D728E90D66284D90B11889C08EA3A39CF61BB
gpg: clave 9C08EA3A39CF61BB: "Pedro Ruiz (Hola Pablo) <pedrosad@gmail.com>" sin cambios
gpg: Cantidad total procesada: 1
gpg:               sin cambios: 1
```

```
┌──(pedro㉿kali)-[~]
└─$ gpg --encrypt --recipient F43D728E90D66284D90B11889C08EA3A39CF61BB archivo
```

```
┌──(pedro㉿kali)-[~]
└─$ gpg -d prueba.gpg
gpg: cifrado con clave de 2048 bits ELG, ID 9F3CE02EF53BC73F, creada el 2021-11-24
      "Pedro Ruiz (Hola Pablo) <pedrosad@gmail.com>"
```




```
┌──(pedro㉿kali)-[~]
└─$ gpg --keyserver pgp.mit.edu --recv-keys ABAA33960D6B0EF5F3535E10090F828D8819DF81
gpg: clave 090F828D8819DF81: "Pablo De juan <pablodejuan8@gmail.com>" sin cambios
gpg: Cantidad total procesada: 1
gpg:              sin cambios: 1
```