

Redes de Computadoras 2021

TP3 Teórico: PGP

Alumnos:

Nehemias Mercau Nievas (nehemias.mercau@mi.unc.edu.ar)

Tomás Martín (tomas.martin@mi.unc.edu.ar)

27 de Mayo, 2021

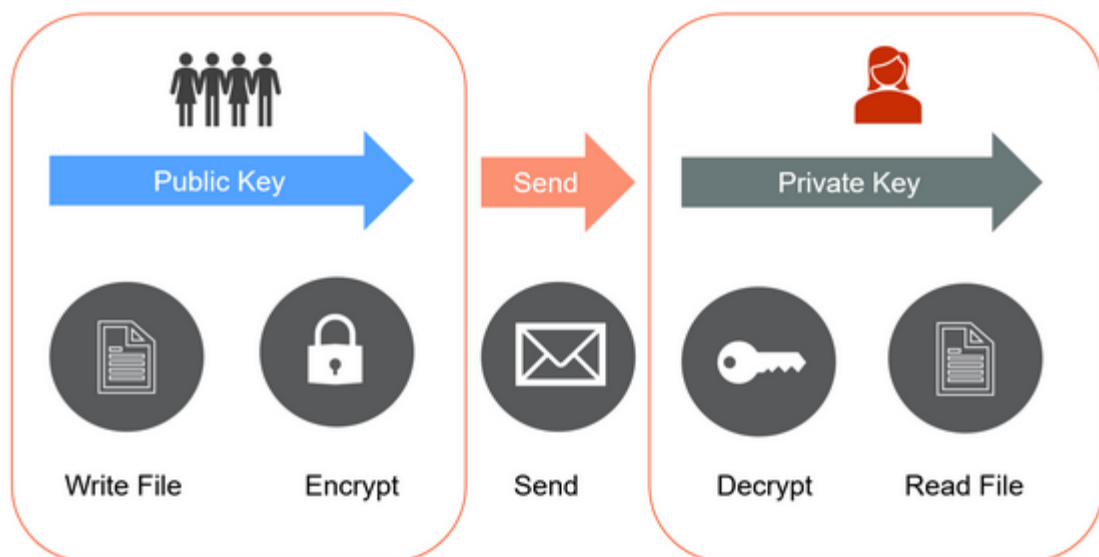
Consigna

- Generar claves privada y pública y mandar a un compañero el mensaje encriptado con la clave pública.

Desarrollo

Para generar las claves y encriptar los mensajes utilizaremos la interfaz gráfica de usuario de GnuPG (GNU Privacy Guard), *GNU Privacy Assistant* (GPA). GnuPG es la implementación del estándar OpenPGP definido en RFC4880. OpenPGP es un estándar de código abierto de PGP para uso público.

PGP (Pretty Good Privacy) utiliza diversas tecnologías de encriptación, como funciones hash, compresión de datos y claves PGP públicas/privadas para proteger la distribución de información crítica. Puede usarse para encriptar correos electrónicos, archivos, directorios y particiones de disco, por lo que es una solución adecuada para las necesidades modernas de Ciberseguridad.



Existen 2 pares de clave, una clave pública y una clave privada. Cuando una persona se quiere comunicar con otra de forma segura, el emisor del mensaje tiene que cifrar el mensaje que quiere enviar con la clave pública del receptor, posteriormente el receptor la desencriptaría con su clave privada. De la misma manera, si el receptor quiere responder tendría que cifrar el mensaje con la clave pública del emisor y tras enviarle el mensaje el emisor lo descifra con su clave privada.

Ambos participantes de la comunicación deben intercambiar, previo a la comunicación, su clave pública. Pero a su clave privada sólo debe conocerla uno mismo, para poder descifrar los mensajes recibidos.

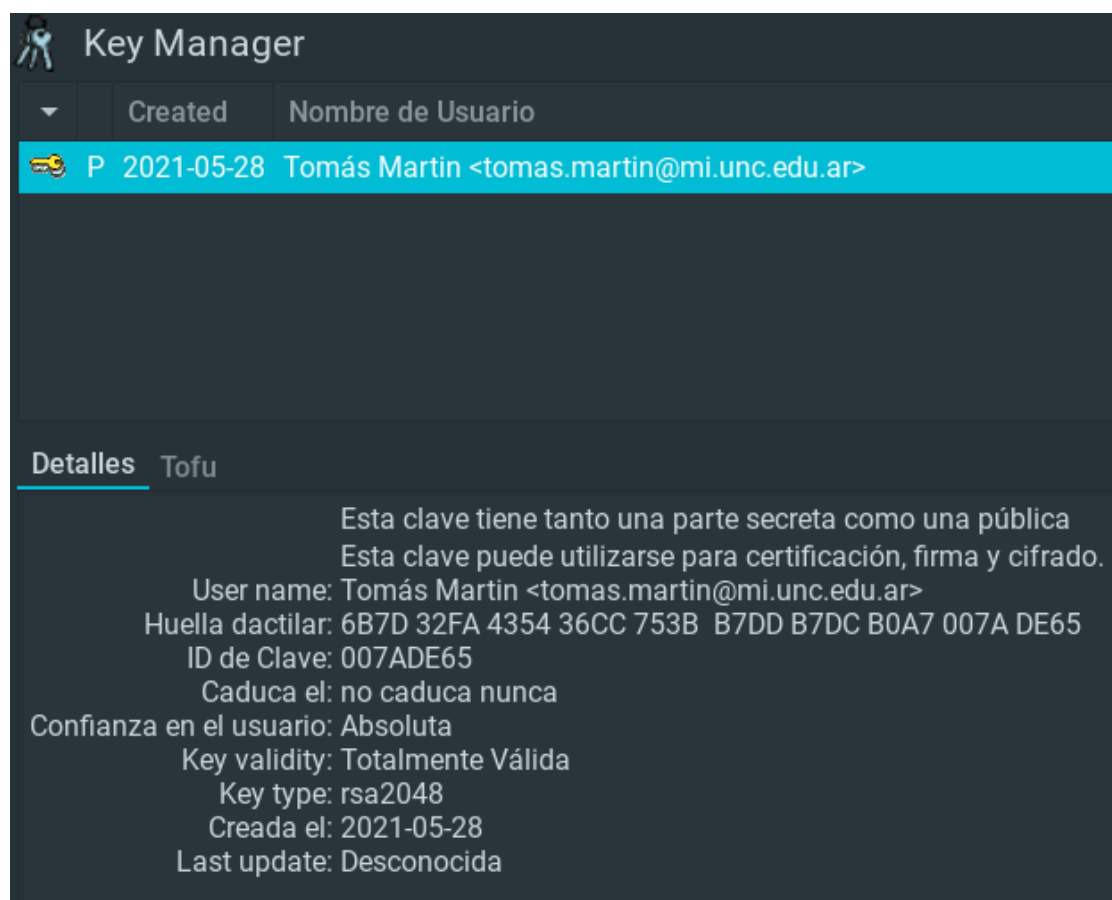
PGP facilita la autenticación de documentos, ya que si una persona le pasa su clave pública a otro para que encripte un mensaje (o documento), y luego cuando lo recibe lo puede desencriptar con su clave privada significa que efectivamente fue la persona a la que le envió la clave pública quien le envió el mensaje.

Instalamos GPA en linux mediante el comando **sudo apt install gnupg gpa**.

Dentro de GPA cada uno creó su clave privada y su clave pública. Luego, nos compartimos nuestra clave pública.

Pasos para enviar un mensaje encriptado (Point 1):

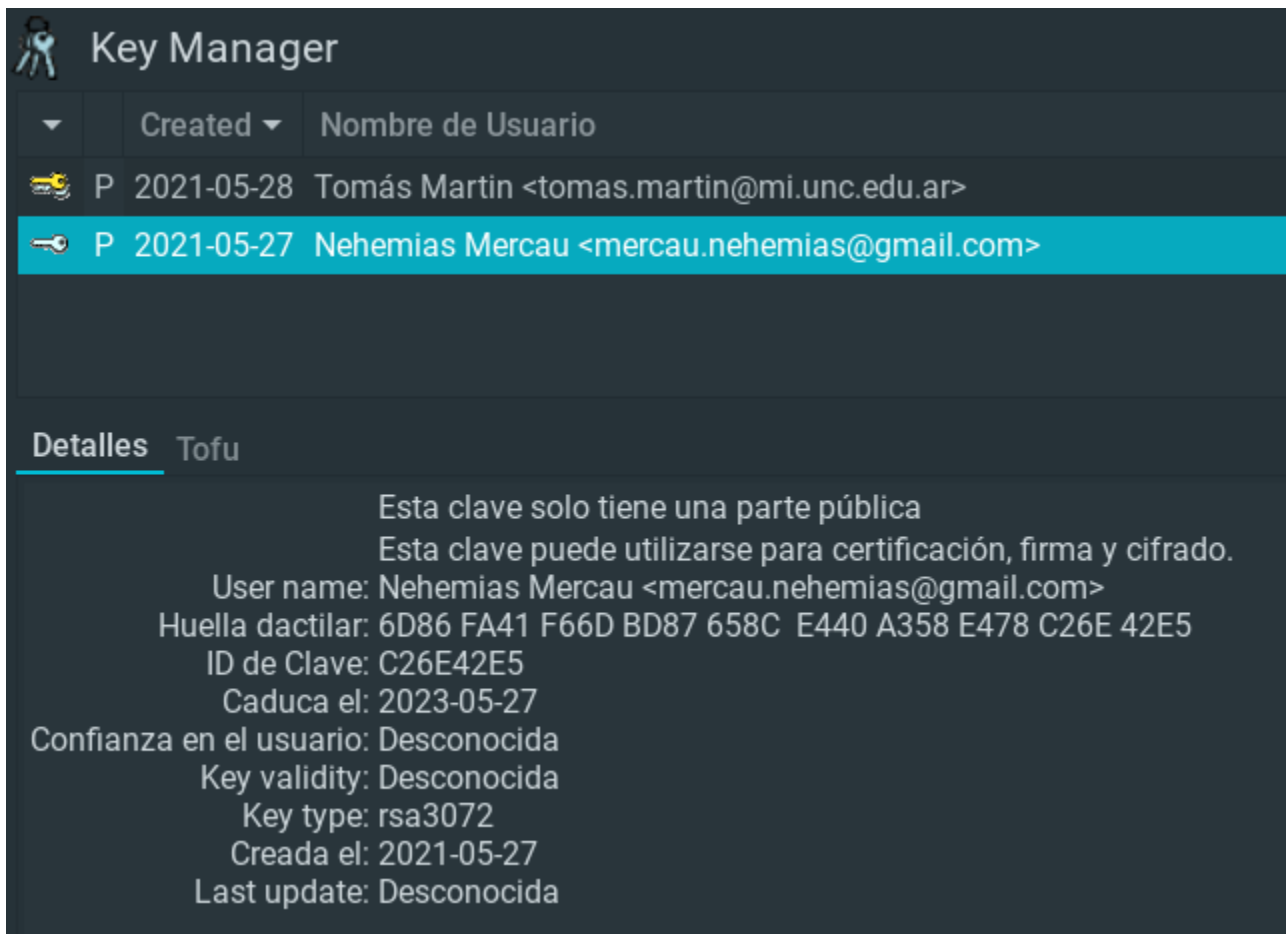
1. Creamos claves: Keys -> New key...



2. Exportamos cada uno su clave pública para pasarle al otro: Click derecho sobre la clave -> Export Keys...

```
tomas ~ cat cp_tm
-----BEGIN PGP PUBLIC KEY BLOCK-----
Created: Nombre de Usuario
mQENBGCwX7YBCADJDtVZLH3Lum5aTi0/qbGe0BtwgNE07OWQeXAlBbhxDPH2IRuQ
zZqcTCTE1M0pAfmCNfiqzG5sNvR1CqorYPEzlIF5Sm6FOilpRjqbc7Jce9WH/Uf8
zmY8ruPXhLj5pTkPhAgxDN/yH7sD+f+MuHtsvnNDxGPrUzQHAUaBTjssRxjBVCCZ
9AKAVdr+6TTZDG8Rpz4taX03pc+eqAdwVmPT5hcNeEe5IYYRaUCUoQoywiSFWErA
9725r3umavCrKi1EWCCwrDfBGvVFkPg+YiZBEAyYyDIZ5E495DbVKGdzy/Xhf8Eg
N9zrzqi6DvHk3LA9ZcfH12gGYibcs2i/5lf9ABEBAAAG0KlRvbc0hcyBNYXJ0aW4g
PHRvbWZzLm1hcnRpbkBTaS51bmMuZWRR1LmFyPokBTgQTAQoA0BYhBgT9MvpDvDbM
dTU33bfcsKcAet5lBQJgsF+2AhsDBQsJCAcCBhUKCQgLAGQWAgMBAh4BAheAAAJ
ELfcsKcAet5l98EH/244tM0uR66zldh+0LsJShnqHUupVlabTntPFpaNMfubvZp
VA1uGhyehDUYEN0e/PjHhOJPPhlcBDJpUrZBeAcH15iHucHPpeLpDNRyXhUvjBYk
ojlKlvcG1UEyafYN4qW8i3dNhbkp4aqdVHmVNltyblwX0Pq3J7WZrY+VCBS1t0q
bPHccF8acuHlmcA4IbNuvjrBm60jBsDrqmtKhmXOpqGJo2G0fYmXSQo9l1DqBjq
1UQNzSUvpOwdlbjLBRz6TsvXKh8u98JMKgLZ+NBQku8R4R8FdVuUbjBg5VnE8XcJ
szzvizlpd7mLdm6YEjFCTohUxY2RPPY8T24Nxy5AQ0EYLBftgEIAMVkpSwUcnvX
tSI8AsV4H3i4e1MpULSdNFhV30ltm14Bxxbo+mxHEUBg35e3Ft5GPhLyEVL5La6t
mzbG9eYVigJW0BYY2bn/1SEWsjJ0p5JPRyt4SDXgP/WVONSQeTZ5EKYcJ1sqpiFb
ftQ0zmOgCmiAtyBaFDCbHrBqJqiViYL0+t3En8wVNkNyVMNxoXpBN78m2yw5jbe8
NsRuCePwY4cVOGTlyDD9Z0STs0k5sp1y9B1H4PDHLJdlPqQuyA8BHSQUEvJ7zCud
94lizlhSb5stkhjQNW4CS9vbnOfd4lKuYmcwVr/pLzeJ5JYi/qhYx9k+P7oje8o2
3CcuwAgZhr8AEQEAAAYkBNgQYAQoAIBYhBgT9MvpDvDbMdTu33bfcsKcAet5lBQJg
sF+2AhsMAAoJELfcsKcAet5lmHMH/jAJbYeEXWT+hJ+bYtE5y4z6s3+FGDXR7++e
1g87g86tM8rNpc8/pgPsLADEdh1d4RKiT713zqBK8cfj5VrciPsyf/TS2Dc0HPbe
KyB3JUVLGYy/abcDuFEftcaJRQecKrKWFULQeuJBmxIDBarRxI2EPLcGqDRDcDhG
MNW5hMA2UVNrtwaBu4PFRt6CF6u60iqnTq4uBfzGRxnoUjVekjlx6qAf7W8h2/uT
sw0UjmnHwOqATiELzsK1U/zZslV7pJr6N20Bp6G6oYpQJoFTkn16fkeEDNGf0u2l
zBEMaGTnNrewnZTu9XqISQcj9PPkdu7YVweKuK7JWma1r5IA1l4=
=9K1X
-----END PGP PUBLIC KEY BLOCK-----
```

3. Importamos la clave pública del otro: Keys -> Import Keys...



Key Manager

	Created	Nombre de Usuario
	P 2021-05-28	Tomás Martin <tomas.martin@mi.unc.edu.ar>
	P 2021-05-27	Nehemias Mercau <mercau.nehemias@gmail.com>

Detalles Tofu

Esta clave solo tiene una parte pública
 Esta clave puede utilizarse para certificación, firma y cifrado.

User name: Nehemias Mercau <mercau.nehemias@gmail.com>
 Huella dactilar: 6D86 FA41 F66D BD87 658C E440 A358 E478 C26E 42E5
 ID de Clave: C26E42E5
 Caduca el: 2023-05-27
 Confianza en el usuario: Desconocida
 Key validity: Desconocida
 Key type: rsa3072
 Creada el: 2021-05-27
 Last update: Desconocida

4. Escribimos un mensaje cada uno, lo ciframos con la clave pública del otro y nos lo enviamos cifrado para luego descryptar el mensaje que nos mandó el otro con la clave privada de cada uno.
 - a. Genero mensaje:



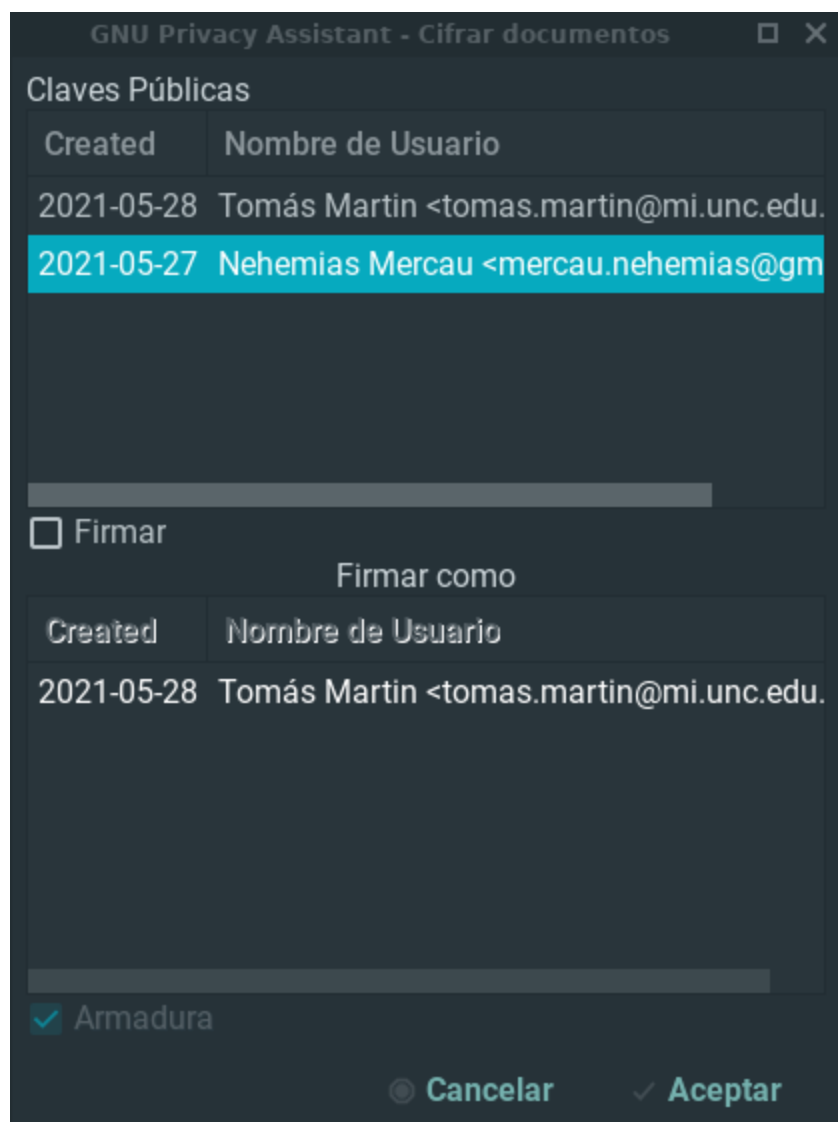
GNU Privacy Assistant - Portapapeles

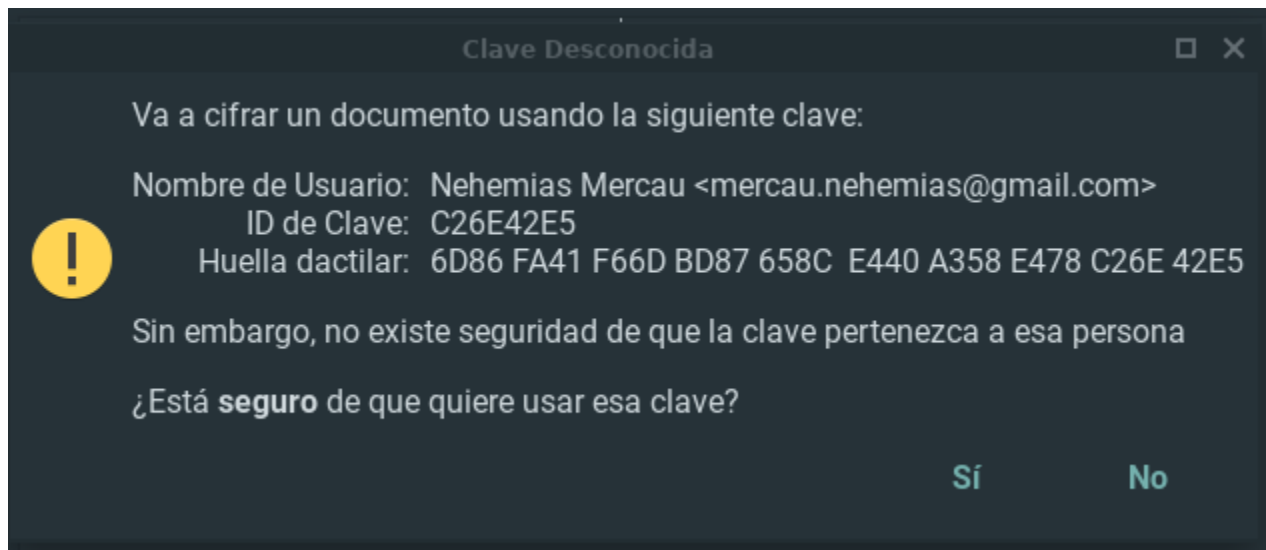
File Edit Windows Help

Portapapeles

Los códigos nucleares son: 3 9 3 2 6 2 2 7|

- b. Encripto con la clave pública:





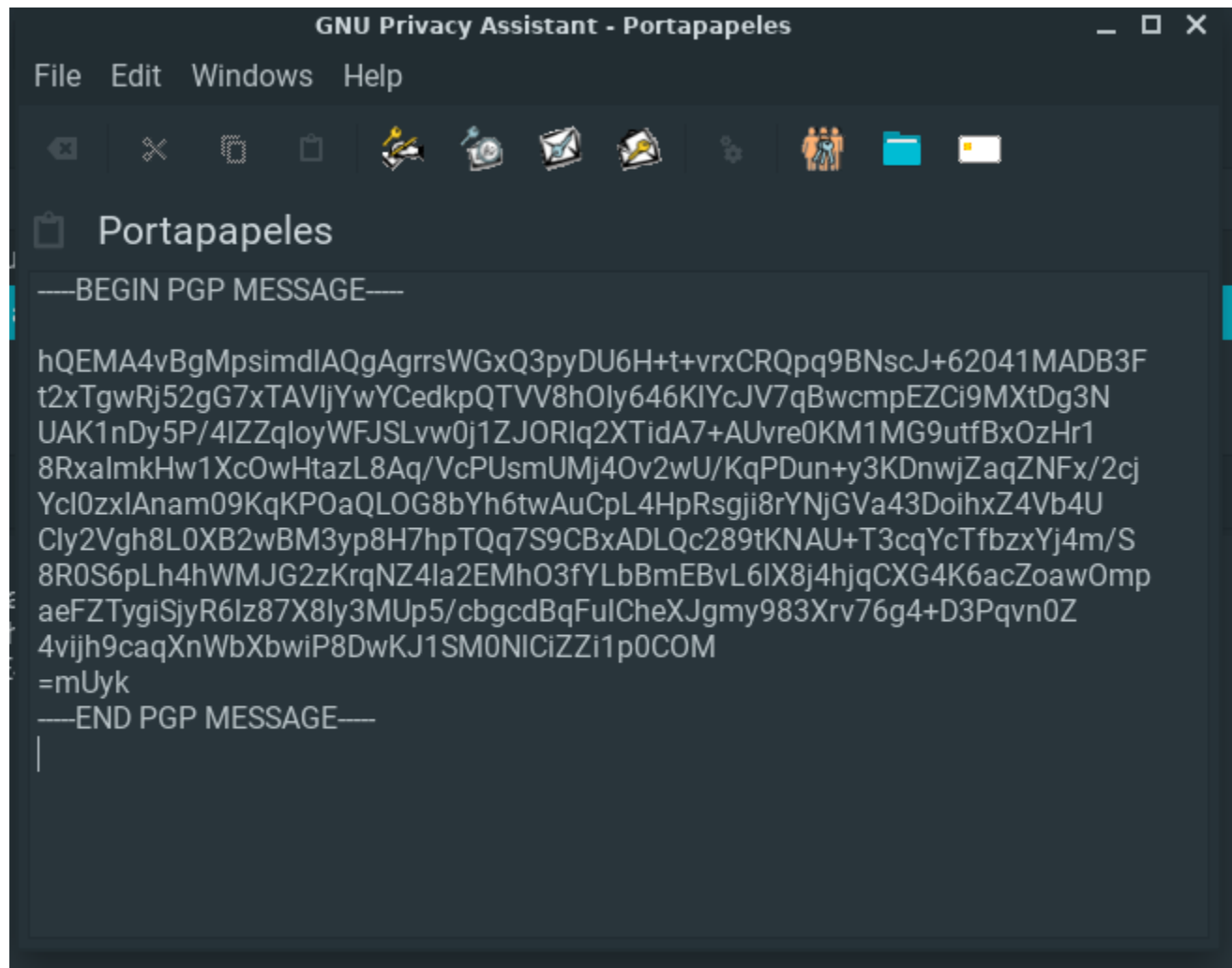
Mensaje encriptado con la clave pública de Nehemias:

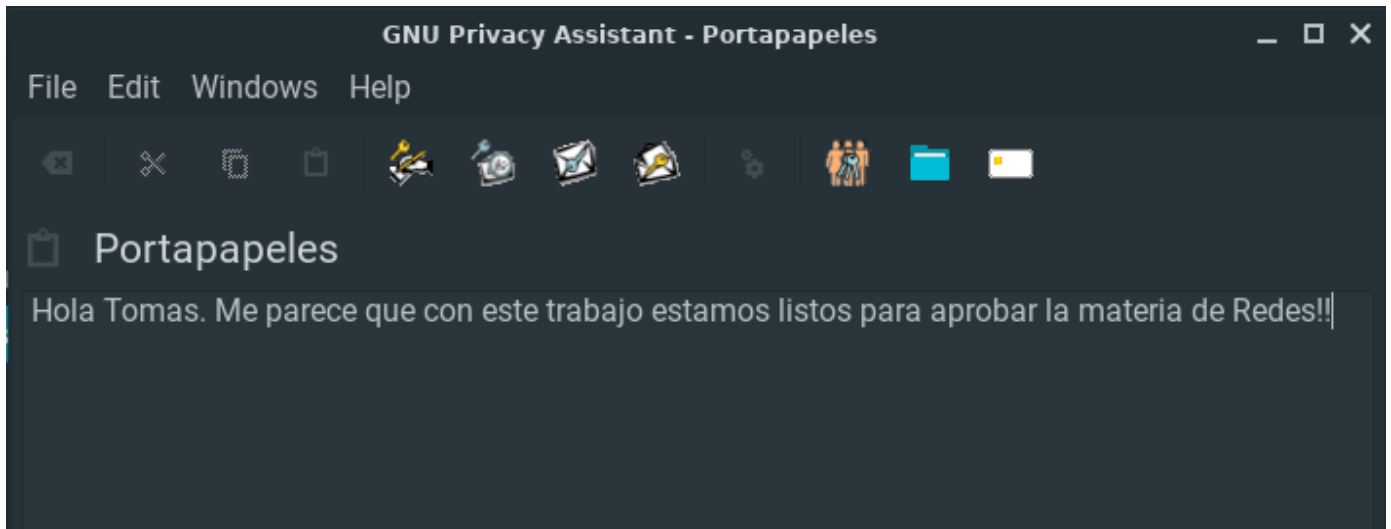
-----BEGIN PGP MESSAGE-----

hQGMA9qJHijxSbmFAQv/XmD47Z1GS2PwXk5lp7JaM1gefIn57R7K/f4uXblmKak5
KbNCh/cyMYrHOXSwPzO3KhXwDIKR3o345Ww1ek6xIF0xJU3Mun+PdG6wZyjH0/o
KbKPdTAQij/B/50SOtHIWDHdWPatS2ITbYQvOlqMh35UAT0hK1SIHYIZ+N+qZEPo
6GojY5rmTywQKLH/aKZbc4oLOmhv4kTC9UXuvyRv6udtjMA8Jgvhe0TJHHPwip5Y
lvGecVJJ6xT5DtE8pVwmaD1GPPJ0In5WrtNnS1X0HeF2HLQ+GfgEjK7Ca0yk4fLy
z5ff8kwRZZJGEs5yEPayRpQzlynkSsfgz0OkNw+1NjRda8NSuACbsKOkUftBFwhT
cJywbM7QkrY5pLv2d9/6vvJV8tAmKI+jyxbLou741VlfBz6OCc73uly6tEg0HPIJ
SdEzy7ujQ96P9kS9Pk3tdhRsb5wlmK/nunlipQ5Fy3UQ9EBH5s26KMNdnhuYBukM
m+3rnhBmRMrlb6TsxKjO0mMBARV7TLCv90qhWU9FxrCvT853kVQRjPxnYYY/nJE
LylTiZE+zW7V505pBagg/Y7mNe2NmHgJp2rE+K24WzGcaUXq6aW8wphefDJSc6Tn
M2sho3D6wF19X+u4935+yy9nqYQ=
=VFVf

-----END PGP MESSAGE-----

- c. Desencriptado con mi clave privada del mensaje que me mandó Nehemias que encriptó con mi clave pública:





Pasos para enviar un mensaje encriptado (Point 2):

1. Generación de key pública y privada:

```
nehemias@nehemias-VirtualBox:~$ gpg --gen-key
gpg (GnuPG) 2.2.19; Copyright (C) 2019 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.

Nota: Usa "gpg --full-generate-key" para el diálogo completo de generación de clave.

GnuPG debe construir un ID de usuario para identificar su clave.

Nombre y apellidos: Nehemias Mercau
Dirección de correo electrónico: mercau.nehemias@gmail.com
Ha seleccionado este ID de usuario:
  "Nehemias Mercau <mercau.nehemias@gmail.com>"

¿Cambia (N)ombre, (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.
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: clave A358E478C26E42E5 marcada como de confianza absoluta
gpg: creado el directorio '/home/nehemias/.gnupg/openpgp-revocs.d'
gpg: certificado de revocación guardado como '/home/nehemias/.gnupg/openpgp-revocs.d/6D86FA41F66DBD87658CE440A358E478C26E42E5.r
ev'
claves pública y secreta creadas y firmadas.

pub   rsa3072 2021-05-28 [SC] [caduca: 2023-05-28]
      6D86FA41F66DBD87658CE440A358E478C26E42E5
uid           Nehemias Mercau <mercau.nehemias@gmail.com>
sub   rsa3072 2021-05-28 [E] [caduca: 2023-05-28]
```

2. Abrimos el key manager, y esta la key que generamos:

GNU Privacy Assistant - Key Manager

File Edit Keys Windows Server Help

Key Manager

	Created	Nombre de Usuario
P	2021-05-27	Nehemias Mercou <mercau.nehemias@gmail.com>
P	2021-05-28	Tomás Martín <tomas.martin@mi.unc.edu.ar>

Detalles

Tofu

Esta clave tiene tanto una parte secreta como una pública

Esta clave puede utilizarse para certificación, firma y cifrado.

User name: Nehemias Mercou <mercau.nehemias@gmail.com>

Huella dactilar: 6D86 FA41 F66D BD87 658C E440 A358 E478 C26E 42E5

ID de Clave: C26E42E5

Caduca el: 2023-05-27

Confianza en el usuario: Absoluta

Key validity: Totalmente Válida

Key type: rsa3072

Creada el: 2021-05-27

Last update: Desconocida

```

nehemias@nehemias-VirtualBox:~/Documentos$ ls
MILLAVEPUBLICA ProjectClcR00cs
nehemias@nehemias-VirtualBox:~/Documentos$ cat MILLAVEPUBLICA
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBGCwOMQBAC2I8J8Jun90SPJ1QggmZ+48JkH2GmAmqjpe2+yIqoobIGpmCmm
3H2SGyarlwvV/56kc9IQakvCF/WKRZWCPTXFDP5CLiwnfhyvEMgDDNEG6dyrj4Vbl
2ouZF54NS+x0cmSH5FaG0Vnk2cgQLHkF8IhdQ0npscse9ohv8qygsu3zWwkoEwFJ
2RAMn8qkFbdf1fZyENEf4z+RBWZewHrPgJoxd4GBX2EBa0WqPuJh0tEXAOEGEOM
p+Wcfz4GhpF1M7057rQq40vETN9H/1dQ7UTK4eFh95S60TpAJqVvovd/vnnMy9
1GY1oT/GpWeiPCaohdXoC4yA/seLRaQUUnuLb1K5GS6kqpJoUM01lenAwID14pMrr
b3p53BLlwFk7Nsx1pThAxTLJlMAsh7PSm9C8VN8DcPyetpesmHNA5bH3R8NH906g
RxxFyHjK+ELur865/hpHFTxawYxxjh6gkdoYH/v1ms9UddA2WdyoyEHmvxgh798M
Lp729GfZua13+18AEQEAABoQrTmVoZW1pYXMGtWVvY2F1IDxtZXJjYXUubmVoZW1p
YXMAZ21haWwY29lP0KB1AQTAQoAPhYh8G2G+kH2bb2HZY2k0KNYSHjcbkLl8Qj9
sDJEAhSDBQkDwmcABQsJCACCBHUKCQgLAQWAgMBAh4BAheAAAOjEKNY5HjcbkLl
a5UL/Au0wu3GHYQVIOopGkxjOZDx3JpBd2tLLxD+oA+YgQkUpdAwBvreyGjctFk2
HwczQ/VASpyYsoycmfJcShQREwVt1uhFavLYUn3c8NWCQ2Qx7o0kHZVPxK195h1c
2a5o+k051EGIP4ugDnKfDbTp0I1yMhXkA5jn4rn29Zz9a1K/JvqO/8eq7Wxq9x5t
OKJ5rNU8SFjpJ0cc9BK1OZch+Gk/m3m6XXH/ZZptta3syjFge19e7gZAGAw53u83
3xdvScnxxze8kyocCZjhLeC255Ezj5LcRjXmK5xW2kFvSo9p1lF6Hb32CgFVl7/w/
JHA15nxt1j8TcVb8hj9NFG3UnwrLEB0H6fjQST61lnteTnn911qUNA9TzT73Qusw
GgbsBK1nm/j+mByBT0MPYL3aa25r4T6Mj8BArUqQkFc+Lqh8hn53JuIF5qAKAUSP
TUYldhR8X3WrN1JbyJUlczqzTXgzYn0U9bnzvBA/wbY//bWUW17hCBKLSah72q4x
f4h4QrkBjQRgsDjEAQwAy4KFxF1B85L/B5GdGSXdsLXr8Y10YVGF0cXR+3sHHW40
FLFRqW51QVpwzykiV91uH58+ZC8j30oqKwsA+HBj/Z89nhGpLGSfBfId9MO+d5+P
fBX062zzSH1VAJ8yqbBq+SjBRLTTu0L29wvEeRR4GqVMKVL4G2HTF3k2+MmdZU9E
ppRn91qB8GoyVz4B71y4Ey6Gy/yc4+FD0518TbPh8gAJhRE0IjPxsVn5Wec8g4G
U0srB08rocP6RQYtVKC/tdeu3pTnF+T0zF5QgyVyufG6E8/yc71J2ThzckN+wlz
lCaGS59zF8157jlex/mFdHJGtIHNfQ4h0EL/uz6KJgGg1kte03d3Th0pGK7jWqCh
ILK/or4J+qkNc0q1/+d/Hpqnw8pubP7zJ2h5mZstcFb730v5TWBE7gmWb0BCKGB
w7uhogdjHldHNXYVoIxxVxvYj4d75IzSGTWtKEHULK6yCTR0ttwAFDC9x4wZh7To
E4acWAF606Lmgm+LKH0PABEBBAC2AbwEABKACyWlQRChvpB9m29h2NMSEcjW0R4
wms5QUICyLA4XATBDdAUJAB7nAAAKRCjW0R4wm5E5a+DC/0DOLY/86x/vd1d0400
P4x/23mmN3Lj5dGN3w16ex0eF95S2L0zWCQTR0oYf9ppxVeVrH19bnnBfH0AGMy
3dq81mez4qhGNV28xpBpd2h9NyBkco0BFCwB70347d07kb0tPj4LBYTgbeJus/+
KDUlUL53FxbVzzssF1t30pGFas99E1Utdcyys2Y40H01oacrJRWXqG0R1PrcygnY
UHQztj0BVBRBFHJC8h+SeG3li1/Hv/ayrwyZnocO/Tsk0059QjeUTdImC62xjEt5
Gb1FQw0zeLK23LLTP0jRuT8xROPNX9YRA0uUaFxb0y1lT/NUJ+5sGyk634WbFGW
8899CquIEEQNJRjoxFTjJkophkGCFgk1F1mLAasR99QxozDXHmJzF5x8SLN6t
53Y8ag19NmQPL+7L6bSofPcm51Xtn6ExJ2hdYVWdms9EmLxfJcAgChvQp1V5lPQW
13UqT0eMX4GunwW9TeD5jn/GBC3n0Kq/LQ0Es1KDmaXtGkE=
xFax
-----END PGP PUBLIC KEY BLOCK-----
nehemias@nehemias-VirtualBox:~/Documentos$

```

3. Agrego la clave pública que me comparte Tomas:

GNU Privacy Assistant - Key Manager

File Edit Keys Windows Server Help

Key Manager

	Created	Nombre de Usuario
P	2021-05-27	Nehemias Mercou <mercau.nehemias@gmail.com>
P	2021-05-28	Tomás Martín <tomas.martin@mi.unc.edu.ar>

Detalles

Tofu

Esta clave solo tiene una parte pública

Esta clave puede utilizarse para certificación, firma y cifrado.

User name: Tomás Martín <tomas.martin@mi.unc.edu.ar>

Huella dactilar: 6B7D 32FA 4354 36CC 753B B7DD B7DC B0A7 007A DE65

ID de Clave: 007ADE65

Caduca el: no caduca nunca

Confianza en el usuario: Desconocida

Key validity: Desconocida

Key type: rsa2048

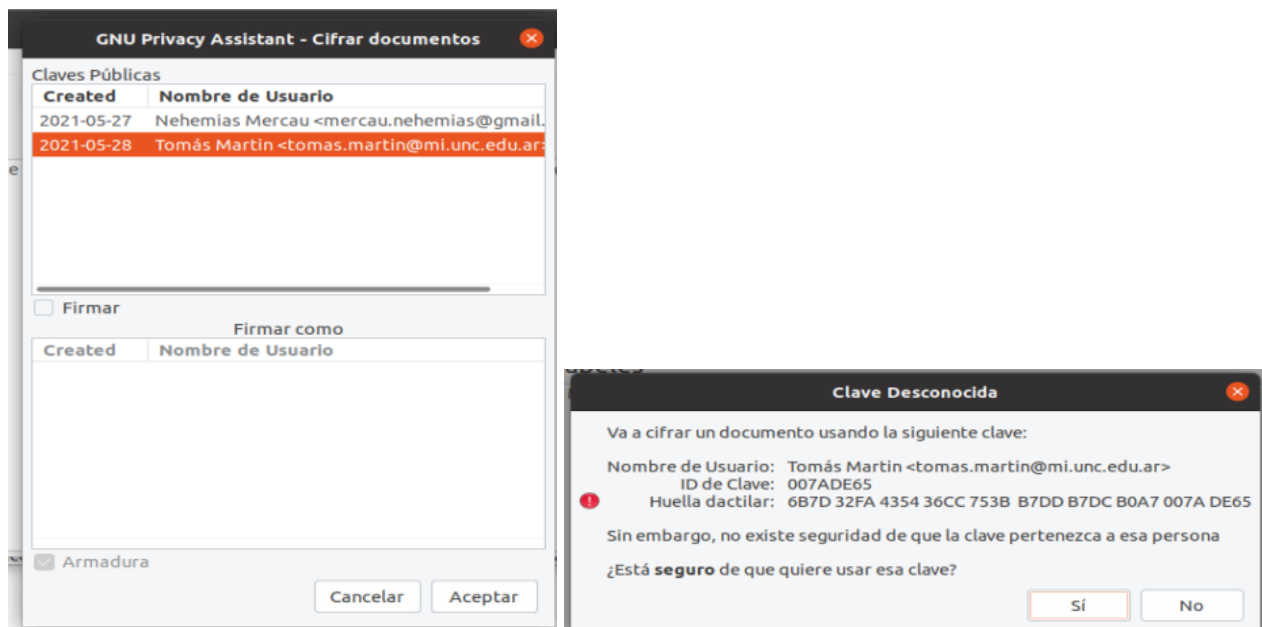
Creada el: 2021-05-28

Last update: Desconocida

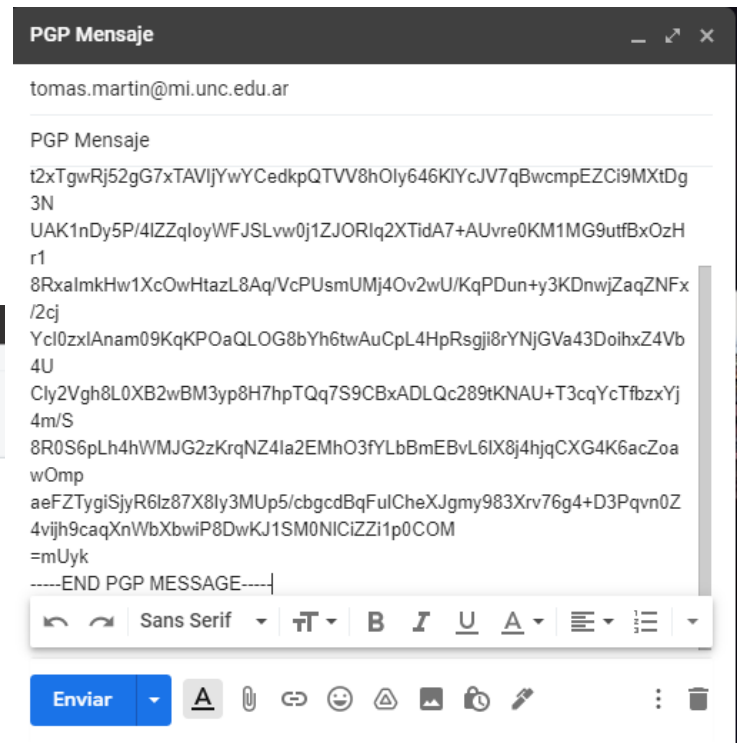
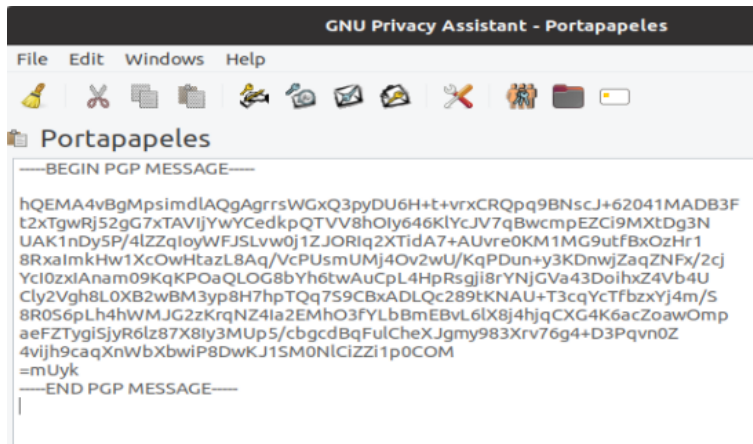
4. Armo el mensaje para enviar:



5. Para encriptar el mensaje, seleccione la clave pública que recién agregue, y confimo:



6. Copio el mensaje encriptado y lo envío por mail.



Mensaje encriptado:

-----BEGIN PGP MESSAGE-----

hQEMA4vBgMpsimdIAQgAgrrsWGxQ3pyDU6H+t+vrxCrQp9BNscJ+62041MADB3F

t2xTgwRj52gG7xTAVIjYwYCedkpQTVV8hOly646KIYcJV7qBwcmpEZCi9MXtDg3N

UAK1nDy5P/4IZZqloyWFJSLvw0j1ZJORIq2XTidA7+AUvre0KM1MG9utfBxOzHr1

8RxalmkHw1XcOwHtazL8Aq/VcPUsmUMj4Ov2wU/KqPDun+y3KDnwjZaqZNFx/2cj

Ycl0zxlAnam09KqKPOaQLOG8bYh6twAuCpL4HpRsgji8rYNjGVa43DoihxZ4Vb4U

Cly2Vgh8L0XB2wBM3yp8H7hpTQq7S9CBxADLQc289tKNAU+T3cqYcTfbzxYj4m/S

8R0S6pLh4hWMJG2zKrQNZ4la2EMhO3fYLBmEBvL6lX8j4hjqCXG4K6acZoawOmp

aeFZTygiSjyR6lz87X8ly3MUp5/cbgcdBqFulCheXJgmy983Xrv76g4+D3Pqvn0Z

4vijn9caqXnWbXbwiP8DwKJ1SM0NICiZZi1p0COM

=mUyk

-----END PGP MESSAGE-----

7. Desencriptar el mensaje que me manda Tomas:

