

SISTEMAS OPERATIVOS

ALEXIS YAHIR ALVAREZ LEON

JOSE ANTONIO RODRIGUEZ ESTUDILLO

TRABAJO EN CLASE DEL DIA

13/11/2025

INGENIERÍA
EN COMPUTACIÓN

Volvimos al tema sobre las encriptaciones pero ahora con una firma de documento y volver a desencriptarlo, y entonces aquí tenemos esta actividad

Paso 1 yo y mi amigo el buen Rodríguez ambos en nuestras laptop empezamos generando la llave publica y privada

ALEXIS

ANTONIO

```
joseantonio@JoseToni: ~ x Ubuntu x + | v
joseantonio@JoseToni: $ sudo gpg --list-secret-keys
joseantonio@JoseToni: $ gpg -full-gen-key
gpg (GnuPG) 2.4.4; Copyright (C) 2024 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.

Please select what kind of key you want:
 (1) RSA and RSA
 (2) DSA and Elgamal
 (3) DSA (sign only)
 (4) RSA (sign only)
 (9) ECC (sign and encrypt) *default*
(10) ECC (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) 3072
Requested keysize is 3072 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) 1w
Key expires at Thu Nov 20 16:01:25 2025 CST
Is this correct? (y/N) y

GnuPG needs to construct a user ID to identify your key.

Real name: Antonio
Email address: jose777toni@gmail.com
Comment: Esta es una llave para la firma de documento
You selected this USER-ID:
    "Antonio (Esta es una llave para la firma de documento) <jose777toni@gmail.com>"

Change (N)ame, (C)omment, (E)mail or (O)key/(Q)uit? [
```

Después lo siguiente exportamos la llave

ALEXIS

```
gpg: option --a ts_dontgood
alexis@LAPTOP-9EVLMCCK: $ gpg --export -a "Yahir Alvarez" > Yahirllave_pub.asc
alexis@LAPTOP-9EVLMCCK: $ [
```

ANTONIO

```
<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) 1w
Key expires at Thu Nov 20 16:01:25 2025 CST
Is this correct? (y/N) y

GnuPG needs to construct a user ID to identify your key.

Real name: Antonio
Email address: jose777toni@gmail.com
Comment: Esta es una llave para la firma de documento
You selected this USER-ID:
    "Antonio (Esta es una llave para la firma de documento) <jose777toni@gmail.com>"

Change (N)ame, (C)omment, (E)mail or (O)key/(Q)uit? 0
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: revocation certificate stored as '/home/joseantonio/.gnupg/openpgp-revocs.d/9ECAFEC2D82BF9E6B161FC6D4679EA43AD525A43.rev'
public and secret key created and signed.

pub    rsa3072 2025-11-13 [SC] [expires: 2025-11-20]
      9ECAFEC2D82BF9E6B161FC6D4679EA43AD525A43
uid            Antonio (Esta es una llave para la firma de documento) <jose777toni@gmail.com>
sub    rsa3072 2025-11-13 [E] [expires: 2025-11-20]

joseantonio@JoseToni: $ gpg --export -a Antonio > Antonio_llave_pub.asc
joseantonio@JoseToni: $ sudo nano Rodriguez_Antonio_Principito.txt
[sudo] password for joseantonio:
```

Ahora creamos el archivo txt y lo ciframos este documento

ALEXIS

```
alexis@LAPTOP-9EVLMCCK: ~ x Ubuntu x + | v
alexis@LAPTOP-9EVLMCCK: $ sudo nano AlvarezAlexis_RomeoyJuliet.txt
alexis@LAPTOP-9EVLMCCK: $ gpg -c AlvarezAlexis_RomeoyJuliet.txt
alexis@LAPTOP-9EVLMCCK: $ ls
AlvarezAlexis_RomeoyJuliet.txt      Yahirllave_pub.asc     documento.txt.asc    llavesHaz.asc:Zone.Identifier    packages.txt
AlvarezAlexis_RomeoyJuliet.txt.gpg   YourPer.txt        documento.txt.gpg  mensaje1.txt      salida.txt
escritorio                         archivo.txt       fonseca.txt       mensaje1.txt.gpg  salida.txt
IDUNICO.txt                         cancion.txt       funciones.sh    mensaje2.txt      saludos1.txt
KeyToni.asc                          cancion_cifrada.gpg holamundo.txt  mensaje2.txt.gpg  saludos1.txt.gpg
KeyToni.asc:Zone.Identifier         cancion_para_toni.gpg keyAlexis.asc  mensaje4.gpg      to-do.txt
MyPort.txt                           cancion.txt       keyAlvarez.asc  mensaje4.txt      venv
MyPort.txt.gpg                      canny.py          keySecretBrayan.asc  mensaje4.txt.gpg  weiteer.txt
MyPort.txt                           canny.py          keySecretSebas.asc  midireccionio  weiteer.txt.gpg
MyPort.txt                           cesar.py          keySecretSebas.asc:Zone.Identifier  monosaurio.txt  weiteer.txt
Sistemas-Operativos-                cesar_full.py    llanto.sh       nombre.txt      youier.txt
UltCon2025B.txt                     crear_usuario.sh  llaves.asc      output.txt      youier.txt.asc
YahirAlvarez_pub.asc               documento.txt    llavesHaz.asc
alexis@LAPTOP-9EVLMCCK: $ ls -l
total 300
-rw-r--r-- 1 root  root  492 Nov 13 16:11 AlvarezAlexis_RomeoyJuliet.txt
-rw-r--r-- 1 alexis alexis 390 Nov 13 16:14 AlvarezAlexis_RomeoyJuliet.txt.gpg
drwxr-xr-x  3 alexis alexis 4096 Oct 28 18:54 Escritorio
-rw-r--r-- 1 alexis alexis 1371 Oct 16 16:41 IDUNICO.txt
-rw-r--r-- 1 alexis alexis 2509 Nov 7 21:08 KeyToni.asc
-rw-r--r-- 1 alexis alexis 61 Nov 7 21:08 KeyToni.asc:Zone.Identifier
-rw-r--r-- 1 alexis alexis 26 Nov 6 20:19 MyPort.txt
-rw-r--r-- 1 alexis alexis 106 Nov 6 20:19 MyPort.txt.gpg
-rw-r--r-- 1 root  root  26 Nov 6 16:18 MyPort.txt
-rw-r--r-- 1 root  root  105 Nov 6 16:15 MyPort.txt.gpg
drwxr-xr-x 10 alexis alexis 4096 Nov 6 20:55 Sistemas-Operativos-
-rw-r--r-- 1 antonio yaned 768 Sep 26 16:08 UltCon2025B.txt
-rw-r--r-- 1 alexis alexis 0 Nov 13 16:05 YahirAlvarez_pub.asc
-rw-r--r-- 1 alexis alexis 2521 Nov 13 16:06 Yahirllave_pub.asc
-rw-r--r-- 1 alexis alexis 24 Nov 6 16:13 YourPer.txt
-rw-r--r-- 1 alexis alexis 47 Sep 1 17:15 archivo.txt
-rw-r--r-- 1 alexis alexis 43 Nov 7 21:14 cancion.txt
-rw-r--r-- 1 alexis alexis 544 Nov 7 21:09 cancion_cifrada.gpg
-rw-r--r-- 1 alexis alexis 523 Nov 7 21:15 cancion_para_toni.gpg
-rw-r--r-- 1 alexis alexis 71 Nov 7 20:11 canatoon.txt
drwxr-xr-x 13 alexis alexis 4096 Nov 6 20:55 canny
-rw-r--r-- 1 alexis alexis 1 Aug 28 15:33 canny.py
04:15 p.m.
13/11/2025
```

ANTONIO

```
joseantonio@JoseToni: ~ x Ubuntu x + | v
<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) 1w
Key expires at Thu Nov 20 16:01:25 2025 CST
Is this correct? (y/N) y
GnuPG needs to construct a user ID to identify your key.

Real name: Antonio
Email address: jose777toni@gmail.com
Comment: Esta es una llave para la firma de documentos
You selected this USER-ID:
  "Antonio (Esta es una llave para la firma de documentos) <jose777toni@gmail.com>"

Change (Name, (Comment, (E)mail or (O)kay/(Q)uit? o
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: revocation certificate stored as '/home/joseantonio/.gnupg/openpgp-revocs.d/9ECAFEC2D82BF9E6B161FC6D4679EA43AD525A43.rev'
public and secret key created and signed.

pub rsa3072 2025-11-13 [SC] [expires: 2025-11-20]
  9ECAFEC2D82BF9E6B161FC6D4679EA43AD525A43
uid           Antonio (Esta es una llave para la firma de documentos) <jose777toni@gmail.com>
sub rsa3072 2025-11-13 [E] [expires: 2025-11-20]

joseantonio@JoseToni: $ gpg --export -a Antonio > Antoniolave_pub.asc
joseantonio@JoseToni: $ sudo nano Rodriguez_Antonio_Principito.txt
[sudo] password for joseantonio:
joseantonio@JoseToni: $
```

El siguiente paso fue lo interesante el firmar el documento con el comando de u el usuario y poner el nombre del documento txt

ALEXIS

```
alexis@LAPTOP-9EVLMCK: $ gpg -u "Yahir Alvarez" --sign AlvarezAlexis_RomeoyJuliet.txt
File 'AlvarezAlexis_RomeoyJuliet.txt.gpg' exists. Overwrite? (y/N) y
alexis@LAPTOP-9EVLMCK: $ gpg --verify AlvarezAlexis_RomeoyJuliet.txt.gpg
gpg: Signature made Thu Nov 13 16:27:35 2025 CST
gpg:           using RSA key 677D74A229EF2679074776D939976CD11E1FB7B
gpg:           issuer "yahir@gmail.com"
gpg: checking the trustdb
gpg: marginals needed: 3 completes needed: 1  trust model: pgp
gpg: depth: 0 valid: 4 signed: 0  trust: 0-, 0q, 0n, 0m, 0f, 4u
gpg: next trustdb check at 2025-11-20
gpg: Good signature from "Yahir Alvarez (esta es una llave para la firma de documento) <yahir@gmail.com>" [ultimate]
alexis@LAPTOP-9EVLMCK: $
```



ANTONIO

```
joseantonio@JoseToni: ~  X  Ubuntu  X  +  v
Enter the user ID. End with an empty line:
gpg: no valid addressees
gpg: Rodriguez_Antonio_Principito.txt.gpg: sign+encrypt failed: No user ID
joseantonio@JoseToni: $ gpg -list-secret-keys
/home/joseantonio/.gnupg/pubring.kbx
-----
sec  rsa3072 2025-11-07 [SC] [expires: 2025-11-14]
    4882A75198EA955530F75067D8886A0A087CD06
uid  [ultimate] Toni (Esta es una llave del trabajo en clase) <jose777toni@gmail.com>
ssb  rsa3072 2025-11-07 [E] [expires: 2025-11-14]

sec  rsa3072 2025-11-13 [SC] [expires: 2025-11-20]
    9ECAFEC2D82BF9E6B161FC6D4679EA43AD525A43
uid  [ultimate] Antonio (Esta es una llave para la firma de documento) <jose777toni@gmail.com>
ssb  rsa3072 2025-11-13 [E] [expires: 2025-11-20]

joseantonio@JoseToni: $ gpg -u "Antonio" -se Rodriguez_Antonio_Principito.txt.gpg
You did not specify a user ID. (you may use "-r")

Current recipients:

Enter the user ID. End with an empty line: 9ECAFEC2D82BF9E6B161FC6D4679EA43AD525A43

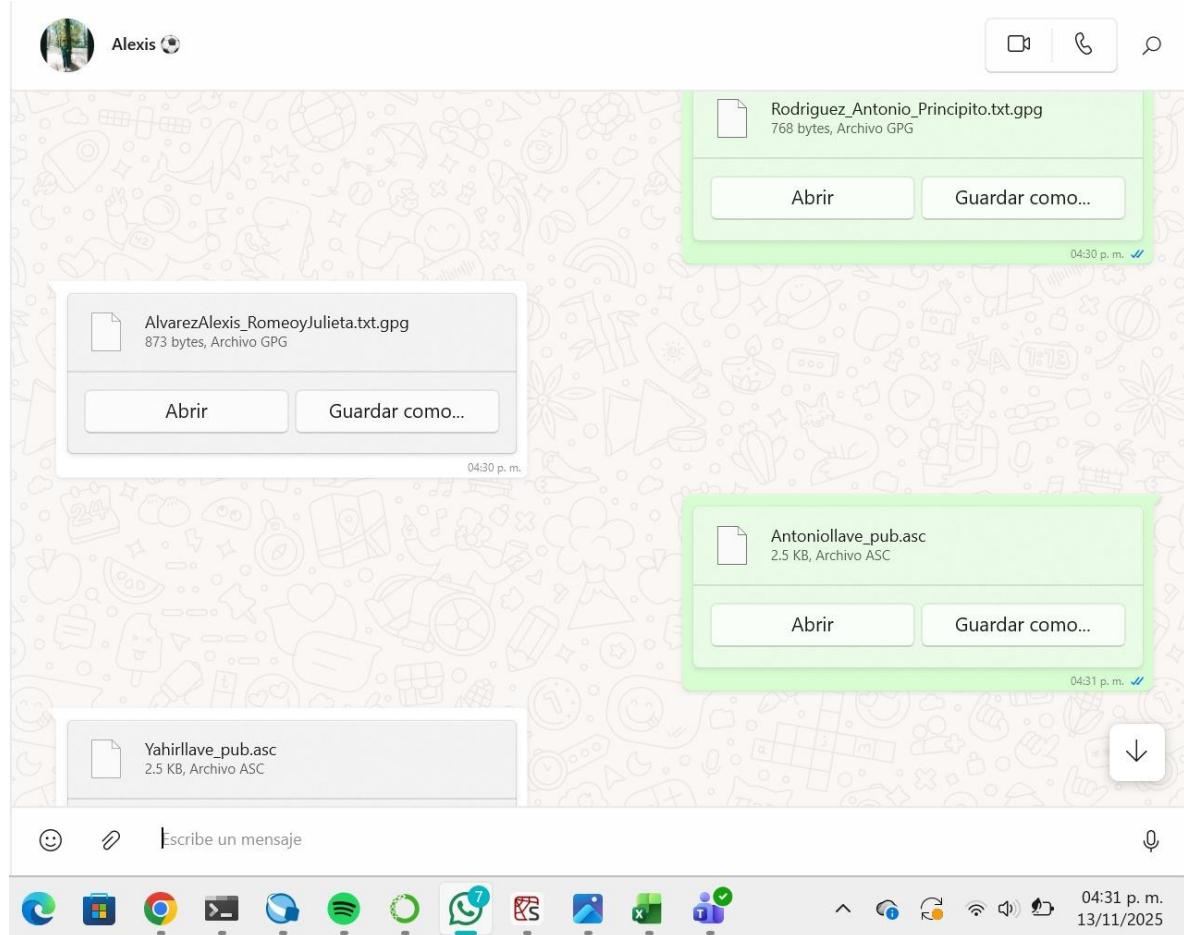
Current recipients:
rsa3072/9833026166C5355F 2025-11-13 "Antonio (Esta es una llave para la firma de documento) <jose777toni@gmail.com>"

Enter the user ID. End with an empty line:
gpg: signing failed: Operation cancelled
gpg: Rodriguez_Antonio_Principito.txt.gpg: sign+encrypt failed: Operation cancelled
joseantonio@JoseToni: $ gpg -u "Antonio" --sign Rodriguez_Antonio_Principito.txt
File 'Rodriguez_Antonio_Principito.txt.gpg' exists. Overwrite? (y/N) y
joseantonio@JoseToni: $ gpg --verify Rodriguez_Antonio_Principito.txt.gpg
gpg: Signature made Thu Nov 13 16:26:29 2025 CST
gpg:           using RSA key 9ECAFEC2D82BF9E6B161FC6D4679EA43AD525A43
gpg:           issuer "jose777toni@gmail.com"
gpg: Good signature from "Antonio (Esta es una llave para la firma de documento) <jose777toni@gmail.com>" [ultimate]
joseantonio@JoseToni: $
```



INGENIERÍA
EN COMPUTACIÓN

Después no compartimos las llaves para poder hacer las descriptaciones

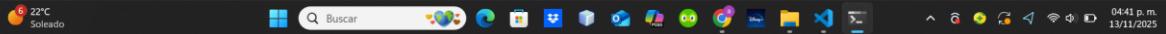


Ya teniendo eso los siguientes pasos de la persona 2 que hicimos ambos fue recibir el documento y verificar si si estaban firmados y se utilizo el comando gpg import para importar la llave y para la firma fue gpg verify con el nombre del archivo txt

ALEXIS

```
alexis@LAPTOP-9EVLNCCK: ~
```

alexis@LAPTOP-9EVLNCCK: \$ gpg -import Antoniollave_pub.asc
gpg: key 4679EA43AD525A43; public key "Antonio (Esta es una llave para la firma de documento) <jose77toni@gmail.com>" imported
gpg: Total number processed: 1
gpg: imported: 1
alexis@LAPTOP-9EVLNCCK: \$ gpg --verify Rodriguez_Antonio_Principito.txt.gpg
gpg: Signature made Thu Nov 13 16:26:29 2025 CST
gpg: using RSA key 9ECAFEC2D82BF9E6B161FC6D4679EA43AD525A43
gpg: issuer "jose77toni@gmail.com"
gpg: Good signature from "Antonio (Esta es una llave para la firma de documento) <jose77toni@gmail.com>" [unknown]
gpg: WARNING: The key's User ID is not certified with a trusted signature!
gpg: There is no indication that the signature belongs to the owner.
Primary key fingerprint: 9ECA FEC2 D82B F9E6 B161 FC6D 4679 EA43 AD52 5A43
alexis@LAPTOP-9EVLNCCK: \$ gpg -d Rodriguez_Antonio_Principito.txt.gpg
Command 'gpg' not found, but there are 21 similar ones.
alexis@LAPTOP-9EVLNCCK: \$ gpg -d Rodriguez_Antonio_Principito.txt.gpg
-Adiós -dijo el zorro-. He aquí mi secreto. Es muy simple: no se ve bien sino con el corazón. Lo esencial es invisible a los ojos.
-Lo esencial es invisible a los ojos -repitió el principito, a fin de acordarse.
-El tiempo que perdiste por tu rosa hace que tu rosa sea tan importante.
-El tiempo que perdí por mi rosa... -repitió el principito, a fin de acordarse.
gpg: Signature made Thu Nov 13 16:26:29 2025 CST
gpg: using RSA key 9ECAFEC2D82BF9E6B161FC6D4679EA43AD525A43
gpg: issuer "jose77toni@gmail.com"
gpg: Good signature from "Antonio (Esta es una llave para la firma de documento) <jose77toni@gmail.com>" [unknown]
gpg: WARNING: The key's User ID is not certified with a trusted signature!
gpg: There is no indication that the signature belongs to the owner.
Primary key fingerprint: 9ECA FEC2 D82B F9E6 B161 FC6D 4679 EA43 AD52 5A43
alexis@LAPTOP-9EVLNCCK: \$



ANTONIO

```
joseantonioire@JoseToni: ~
```

joseantonioire@JoseToni: ~

```
uid      [ultimate] Antonio (Esta es una llave para la firma de documento) <jose77toni@gmail.com>
sub   rsa3072 2025-11-13 [E] [expires: 2025-11-20]

pub   rsa3072 2025-11-13 [SC] [expires: 2025-11-20]
      677D74A229EF2679D747760F939976CD11E1FB7B

uid      [ unknown] Yahir Alvarez (esta es una llave para la firma de documento) <yahir@gmail.com>
sub   rsa3072 2025-11-13 [E] [expires: 2025-11-20]

joseantonioire@JoseToni: $ gpg --verify AlvarezAlexis_RomeoyJuliet.txt.gpg
gpg: Signature made Thu Nov 13 16:27:35 2025 CST
gpg: using RSA key 677D74A229EF2679D747760F939976CD11E1FB7B
gpg: issuer "yahir@gmail.com"
gpg: Good signature from "Yahir Alvarez (esta es una llave para la firma de documento) <yahir@gmail.com>" [unknown]
gpg: WARNING: The key's User ID is not certified with a trusted signature!
gpg: There is no indication that the signature belongs to the owner.
Primary key fingerprint: 677D 74A2 29EF 2679 D747 760F 9399 76CD 11E1 FB7B
joseantonioire@JoseToni: $ gpg -d AlvarezAlexis_RomeoyJuliet.txt.gpg
SANSON Gregorio, te lo juro, no llevaremos carbono.
GREGORIO No, porque entonces seríamos carboneros.
SANSON Quiero decir, si estamos enojados, desenfundaremos
GREGORIO Ay, mientras vivas, saca tu cuello de
collar
SANSON Ataco rápidamente, movido por la emoción.
GREGORIO Pero tú no te mueves rápidamente para atacar.
SANSON Un perro de la casa de Montesco me mueve.
GREGORIO Moverse es agitarse, y ser valiente es
mantenerse firme. Por lo tanto, si te mueves, huyes
lejos.

gpg: Signature made Thu Nov 13 16:27:35 2025 CST
gpg: using RSA key 677D74A229EF2679D747760F939976CD11E1FB7B
gpg: issuer "yahir@gmail.com"
gpg: Good signature from "Yahir Alvarez (esta es una llave para la firma de documento) <yahir@gmail.com>" [unknown]
gpg: WARNING: The key's User ID is not certified with a trusted signature!
gpg: There is no indication that the signature belongs to the owner.
Primary key fingerprint: 677D 74A2 29EF 2679 D747 760F 9399 76CD 11E1 FB7B
joseantonioire@JoseToni: $
```



Ya al final lo último creamos un nuevo archivo txt para guardar el mensaje desencriptado con lo que venia ahí mismo

ALEXIS

```
alexis@LAPTOP-9EVLMCK: $ gpg -d Rodriguez_Antonio_Principito.txt.gpg > DesAlvarezP2Alexis.txt
gpg: Signature made Thu Nov 13 16:26:29 2025 CST
gpg:           using RSA key 9ECAFEC2D82BF9E6B161FC604679EA43AD525A43
gpg:           issuer "jose777toni@gmail.com"
gpg: Good signature from "Antonio (Esta es una llave para la firma de documento) <jose777toni@gmail.com>" [unknown]
gpg: WARNING: The key's User ID is not certified with a trusted signature!
gpg: There is no indication that the signature belongs to the owner.
Primary key fingerprint: 9ECA FEC2 D82B F9E6 B161 FC6D 4679 EA43 AD52 5A43
alexis@LAPTOP-9EVLMCK: $ cat DesAlvarezP2Alexis.txt
-Adiós -dijo el zorro-. Hé aquí mi secreto. Es muy simple: no se ve bien sino con el corazón. Lo esencial es invisible a los ojos.
-Lo esencial es invisible a los ojos -repitió el principito, a fin de acordarse.
-El tiempo que perdiste por tu rosa hace que tu rosa sea tan importante.
-El tiempo que perdi por mi rosa.. -repitió el principito, a fin de acordarse.
alexis@LAPTOP-9EVLMCK: $
```

04:46 p. m.
13/11/2025

ANTONIO

```
joseantonio@JoseToni: ~  X  Ubuntu  X  +  v
uid      [ultimate] Antonio (Esta es una llave para la firma de documento) <jose777toni@gmail.com>
sub   rsa3072 2025-11-13 [E] [expires: 2025-11-20]
pub   rsa3072 2025-11-13 [SC] [expires: 2025-11-20]
      677D74A229EF2679074776DF939976CD11E1FB78
uid      [ unknown] Yahir Alvarez (esta es una llave para la firma de documento) <yahir@gmail.com>
sub   rsa3072 2025-11-13 [E] [expires: 2025-11-20]
joseantonio@JoseToni: $ gpg --verify AlvarezAlexis_RomeoyJuliet.txt.gpg
gpg: Signature made Thu Nov 13 16:27:35 2025 CST
gpg:           using RSA key 677D74A229EF2679074776DF939976CD11E1FB78
gpg:           issuer "yahir@gmail.com"
gpg: Good signature from "Yahir Alvarez (esta es una llave para la firma de documento) <yahir@gmail.com>" [unknown]
gpg: WARNING: The key's User ID is not certified with a trusted signature!
gpg: There is no indication that the signature belongs to the owner.
Primary key fingerprint: 677D 74A2 29EF 2679 0747 76DF 9399 76CD 11E1 FB78
joseantonio@JoseToni: $ gpg -d AlvarezAlexis_RomeoyJuliet.txt.gpg
SANSON Gregorio, te lo juro, no llevaremos carbón.
GREGORIO No, porque entonces seríamos carboneros.
SANSON Querido decir, si estamos enojados, desenfundaremos
GREGORIO Ay, mientras vivas, saca tu cuello de
collar
SANSON Ataco rápidamente, movido por la emoción.
GREGORIO Pero tú no te mueves rápidamente para atacar.
SANSON Un perro de la casa de Montesco me mueve.
GREGORIO Moverse es agitarse, y ser valiente es
mantenerse firme. Por lo tanto, si te mueves, huyes
lejos.
gpg: Signature made Thu Nov 13 16:27:35 2025 CST
gpg:           using RSA key 677D74A229EF2679074776DF939976CD11E1FB78
gpg:           issuer "yahir@gmail.com"
gpg: Good signature from "Yahir Alvarez (esta es una llave para la firma de documento) <yahir@gmail.com>" [unknown]
gpg: WARNING: The key's User ID is not certified with a trusted signature!
gpg: There is no indication that the signature belongs to the owner.
Primary key fingerprint: 677D 74A2 29EF 2679 0747 76DF 9399 76CD 11E1 FB78
joseantonio@JoseToni: $
```

04:40 p. m.
13/11/2025

Y así fue nuestro trabajo de ahora como poner firma y ver si fue correcta esa firma

