



Ciberseguridad en Entornos de las Tecnologías de la Información

Módulo 5021 – Incidentes de Ciberseguridad

Ejercicio – Cifrado Asimétrico

Pliego de Descargo

- *Los ejercicios y conocimientos contenidos en el Módulo 5021, Incidentes de Ciberseguridad, tienen un propósito exclusivamente formativo, por lo que **nunca se deberán utilizar con fines maliciosos o delictivos.***
- *Ni el Ministerio de Educación y Formación Profesional como organismo oficial, ni el CIDEAD como área integrada en el mismo, serán responsables en ningún caso de los daños directos o indirectos que pudieran derivarse del uso inadecuado de las herramientas de hacking ético utilizadas en dichos ejercicios.*



Cifrado de Datos – La historia de Claudio y Claudina

- Claudio Romeo y Claudina Julieta tienen algo en común: siempre están en las nubes.
- Por eso sus respectivas y rivales familias les han apodado con sobrenombres relacionados con la “cloud”.
- Además, están enamorados.
- Intercambian sus mensajes de amor cifrados de forma simétrica con una clave que acordaron antes de que sus destinos se separasen.
- Así pasan algún tiempo, intercambiando tórridos mensajes de forma secreta, hasta que un día aciago uno de sus familiares más cotillas, Teobaldo, intercepta uno de estos mensajes, averigua la clave y monta un escándalo en el Instagram de Verona.
- Claudio y Claudina no saben qué hacer, y acuden a Fray Lorenzo, que después de reflexionar unos instantes, acaba sentenciando: “la solución a vuestro problema es emplear un cifrado asimétrico; cada uno de vosotros conocerá su clave privada, y además sabrá con certeza que el mensaje recibido proviene de su amado o su amada, pues él o ella lo habrá cifrado con la clave pública recíproca”.

GPG – Configuración y Algoritmos Soportados

```
pi@claudio: ~  
pi@claudio:~$ gpg -h | head -n 15  
gpg (GnuPG) 2.2.12  
libgcrypt 1.8.4  
Copyright (C) 2018 Free Software Foundation, Inc.  
License GPLv3+: GNU GPL version 3 or later <https://gnu.org/licenses/gpl.html>  
This is free software: you are free to change and redistribute it.  
There is NO WARRANTY, to the extent permitted by law.  
  
Home: /home/pi/.gnupg  
Algoritmos disponibles:  
Clave pública: RSA, ELG, DSA, ECDH, ECDSA, EDDSA  
Cifrado: IDEA, 3DES, CAST5, BLOWFISH, AES, AES192, AES256, TWOFISH,  
CAMELLIA128, CAMELLIA192, CAMELLIA256  
Resumen: SHA1, RIPEMD160, SHA256, SHA384, SHA512, SHA224  
Compresión: Sin comprimir, ZIP, ZLIB, BZIP2  
  
pi@claudio:~$ █  
  
pi@claudina: ~  
pi@claudina:~$ gpg -h | head -n 15  
gpg (GnuPG) 2.2.12  
libgcrypt 1.8.4  
Copyright (C) 2018 Free Software Foundation, Inc.  
License GPLv3+: GNU GPL version 3 or later <https://gnu.org/licenses/gpl.html>  
This is free software: you are free to change and redistribute it.  
There is NO WARRANTY, to the extent permitted by law.  
  
Home: /home/pi/.gnupg  
Supported algorithms:  
Pubkey: RSA, ELG, DSA, ECDH, ECDSA, EDDSA  
Cipher: IDEA, 3DES, CAST5, BLOWFISH, AES, AES192, AES256, TWOFISH,  
CAMELLIA128, CAMELLIA192, CAMELLIA256  
Hash: SHA1, RIPEMD160, SHA256, SHA384, SHA512, SHA224  
Compression: Uncompressed, ZIP, ZLIB, BZIP2  
  
pi@claudina:~$ █
```

Crear Fichero Texto y Cifrar

```
pi@claudio:~/CIFRADO_lab $ nano carta_amor.txt
pi@claudio:~/CIFRADO_lab $ cat carta_amor.txt

Indignada está la brisa
dice que ya no la quiero,
pues no escucho ya el susurro
- que sonábame antes puro -
de su voz entre los cedros.

Francisco Artés

pi@claudio:~/CIFRADO_lab $ file carta_amor.txt
carta_amor.txt: UTF-8 Unicode text
pi@claudio:~/CIFRADO_lab $ gpg -c carta_amor.txt
pi@claudio:~/CIFRADO_lab $ ls -l
total 8
-rw-r--r-- 1 pi pi 158 mar 20 15:50 carta_amor.txt
-rw-r--r-- 1 pi pi 207 mar 20 15:55 carta_amor.txt.gpg
pi@claudio:~/CIFRADO_lab $ file carta_amor.txt.gpg
carta_amor.txt.gpg: GPG symmetrically encrypted data (AES256 cipher)
```

[illegible]

Contraseña: arpeggio

```

pi@claudio: ~/CIFRADO_lab
pi@claudio:~/CIFRADO_lab $ ls -l
total 8
-rw-r--r-- 1 pi pi 158 mar 20 15:50 carta_amor.txt
-rw-r--r-- 1 pi pi 207 mar 20 15:55 carta_amor.txt.gpg
pi@claudio:~/CIFRADO_lab $ hexdump -C carta_amor.txt
00000000  0a 49 6e 64 69 67 6e 61  64 61 20 65 73 74 c3 a1  |.Indignada est..|
00000010  20 6c 61 20 62 72 69 73  61 0a 64 69 63 65 20 71  | la brisa.dice q|
00000020  75 65 20 79 61 20 6e 6f  20 6c 61 20 71 75 69 65  |ue ya no la quie|
00000030  72 6f 2c 0a 70 75 65 73  20 6e 6f 20 65 73 63 75  |ro, pues no escu|
00000040  63 68 6f 20 79 61 20 65  6c 20 73 75 73 75 72 72  |cho ya el susurr|
00000050  6f 0a 2d 20 71 75 65 20  73 6f 6e c3 a1 62 61 6d  |o.- que son..bam|
00000060  65 20 61 6e 74 65 73 20  70 75 72 6f 20 2d 0a 64  |e antes puro -.d|
00000070  65 20 73 75 20 76 6f 7a  20 65 6e 74 72 65 20 6c  |e su voz entre l|
00000080  6f 73 20 63 65 64 72 6f  73 2e 0a 0a 46 72 61 6e  |os cedros...Fran|
00000090  63 69 73 63 6f 20 41 72  74 c3 a9 73 0a 0a         |cisco Art..s...|
0000009e
pi@claudio:~/CIFRADO_lab $ hexdump -C carta_amor.txt.gpg
00000000  8c 0d 04 09 03 02 9a 93  98 79 dd 65 58 e1 d9 d2  |.....y.eX...|
00000010  be 01 d8 c4 98 9c 6f 61  7b 66 56 16 03 56 a7 73  |.....a.fv..V.s|
00000020  63 09 ec 62 bd 29 ec e6  75 bf 15 b3 62 6d e5 a4  |[c..b.)..u..b..|
00000030  f4 88 71 ea 41 14 09 a5  d3 94 50 06 1b 2e 43 bc  |[..q.A.....P...C.|
00000040  ee b2 f6 97 c9 1f 20 c3  7f 35 b4 07 ca b9 30 d2  |[.....5.....0.|
00000050  de 6d 07 f2 b7 b3 52 5b  61 1b 5e 26 43 60 39 be  |[.m.....R[a.^&C^9.|
00000060  31 e5 56 f9 88 ac 73 ee  27 13 1b b9 fe 5d 9c b6  |[l.V....s'......]|
00000070  e4 d6 35 45 8d 66 d1 e2  62 f5 9a 80 cb 3b ef 70  |[..5E.f..b....;p|
00000080  70 27 6b 41 e0 72 da f0  d6 75 92 e8 4a 8d 79 7e  |[p'kA.r.....J.y~|
00000090  77 16 23 66 0a aa e4 46  04 93 9a 36 d9 24 b3 21  |[w.#f...F....$.~!|
000000a0  30 4f b1 5d 72 b1 bb 1a  4c 1d a8 98 8a 5e 04 6e  |[00.]r...L.....n|
000000b0  83 cb be 1f ca 5f 47 dc  43 58 5e fe ff 33 ca 57  |[...._G.CX^.3.W|
000000c0  71 2f 76 a8 29 a9 9f 60  85 cb 58 5f 1a 38 49     |[q/v.)...X_8I|
000000cf
pi@claudio:~/CIFRADO_lab $

```

Enviar fichero a Claudina, que descubre que está cifrado

```
pi@claudio: ~/CIFRADO_lab
pi@claudio:~/CIFRADO_lab $ ls -l
total 8
-rw-r--r-- 1 pi pi 158 mar 20 15:50 carta_amor.txt
-rw-r--r-- 1 pi pi 207 mar 20 15:55 carta_amor.txt.gpg
pi@claudio:~/CIFRADO_lab $ sftp claudina
The authenticity of host 'claudina (192.168.1.20)' can't be established.
ECDSA key fingerprint is SHA256:hedPCS+z7jXy6XzP5FsmDQumqERC7XOervnXBvYl+v0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'claudina,192.168.1.20' (ECDSA) to the list of known hosts.
pi@claudina's password:
Connected to claudina.
sftp> pwd
Remote working directory: /home/pi
sftp> cd CIFRADO_lab
sftp> ls -l
sftp> put carta_amor.txt.gpg
Uploading carta_amor.txt.gpg to /home/pi/CIFRADO_lab/carta_amor.txt.gpg
carta_amor.txt.gpg 100% 207 137.7KB/s 00:00
sftp> ls -l
-rw-r--r-- 1 pi pi 207 Mar 20 16:08 carta_amor.txt.gpg
sftp> exit
pi@claudio:~/CIFRADO_lab $
```

```
pi@claudina: ~/CIFRADO_lab
pi@claudina:~/CIFRADO_lab $ ls -l
total 4
-rw-r--r-- 1 pi pi 207 Mar 20 16:08 carta_amor.txt.gpg
pi@claudina:~/CIFRADO_lab $ hexdump -C carta_amor.txt.gpg
00000000 8c 0d 04 09 03 02 9a 93 98 79 dd 65 58 e1 d9 d2 |.....y.eX...|
00000010 be 01 d8 c4 98 9c fd 61 fb 66 56 16 03 56 a7 73 |.....a.fV..V.s|
00000020 63 09 ec 62 bd 29 ec ec 75 bf 15 b3 62 d6 e5 a4 |c..b.)..u...b...|
00000030 f4 88 71 ea 41 14 09 a5 d3 94 50 06 1b 2e 43 bc |..q.A....P...C.|
00000040 ee b2 f6 97 c9 1f 20 c3 7f 35 b4 07 ca b9 30 d2 |.....5.....0.|
00000050 de 6d 07 f2 b7 b3 52 5b 61 1b 5e 26 43 60 39 be |.m....R[a.^&C`9.|
00000060 31 e5 56 f9 88 ac 73 ee 27 13 1b b9 fe 5d 9c b6 |l.V...s.'....]..|
00000070 e4 d6 35 45 8d 66 d1 e2 62 f5 9a 80 cb 3b ef 70 |..5E.f..b....;p|
00000080 70 27 6b 41 e0 72 da f0 d6 75 92 e8 4a 8d 79 7e |p'kA.r...u...J.y~|
00000090 77 16 23 66 0a aa e4 46 04 93 9a 36 d9 24 b3 21 |w.#f...F...6.$.!|
000000a0 30 4f b1 5d 72 b1 bb 1a 4c 1d a8 98 8a 5e 04 6e |[00.]r...L....^..n|
000000b0 83 cb be 1f ca 5f 47 dc 43 58 5e fe ff 33 ca 57 |.....G.CX^...3.W|
000000c0 71 2f 76 a8 29 a9 9f 60 85 cb 58 5f 1a 38 49 |q/v.)...`..X_.8I|
000000cf
pi@claudina:~/CIFRADO_lab $ file carta_amor.txt.gpg
carta_amor.txt.gpg: GPG symmetrically encrypted data (AES256 cipher)
pi@claudina:~/CIFRADO_lab $
```

```

pi@claudina: ~/CIFRADO_lab
pi@claudina:~/CIFRADO_lab $ ls -l
total 4
-rw-r--r-- 1 pi pi 207 Mar 20 16:08 carta_amor.txt.gpg
pi@claudina:~/CIFRADO_lab $ gpg carta_amor.txt.gpg
gpg: WARNING: no command supplied. Trying to guess what you mean ...
gpg: AES256 encrypted data
gpg: problem with the agent: Timeout
gpg: encrypted with 1 passphrase
gpg: decryption failed: No secret key
pi@claudina:~/CIFRADO_lab $ gpg carta_amor.txt.gpg
gpg: WARNING: no command supplied. Trying to guess what you mean ...
gpg: AES256 encrypted data
gpg: encrypted with 1 passphrase
pi@claudina:~/CIFRADO_lab $ ls -l
total 8
-rw-r--r-- 1 pi pi 158 Mar 20 16:14 carta_amor.txt
-rw-r--r-- 1 pi pi 207 Mar 20 16:08 carta_amor.txt.gpg
pi@claudina:~/CIFRADO_lab $ hexdump -C carta_amor.txt
00000000 0a 49 6e 64 69 67 6e 61 64 61 20 65 73 74 c3 a1 |.Indignada est..|
00000010 20 6c 61 20 62 72 69 73 61 0a 64 69 63 65 20 71 | | la brisa.dice q|
00000020 75 65 20 79 61 20 6e 6f 20 6c 61 20 71 75 69 65 |ue ya no la quie|
00000030 72 6f 2c 0a 70 75 65 73 20 6e 6f 20 65 73 63 75 |ro,. pues no escu|
00000040 63 68 6f 20 79 61 20 65 6c 20 73 75 73 75 72 72 |cho ya el susurr|
00000050 6f 0a 2d 20 71 75 65 20 73 6f 6e c3 a1 62 61 6d |o.- que son..bam|
00000060 65 20 61 6e 74 65 63 20 70 75 72 6f 20 2d 0a 64 |e antes puro -.d|
00000070 65 20 73 75 20 76 6f 7a 20 65 6e 74 72 65 20 6c |e su voz entre l|
00000080 6f 73 20 63 65 64 72 6f 73 2e 0a 0a 46 72 61 6e |os cedros...Fran|
00000090 63 69 73 63 6f 20 41 72 74 c3 a9 73 0a 0a |cisco Art...s..|
0000009e
pi@claudina:~/CIFRADO_lab $

```

```
lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
x Enter passphrase                                           x
x                                                         x
x                                                         x
x Passphrase: ████████████████████████████████████████ x
x                                                         x
x      <OK>                                             <Cancel>    x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

```
pi@claudina: ~/CIFRADO_lab
pi@claudina:~/CIFRADO_lab $ ls -l
total 8
-rw-r--r-- 1 pi pi 158 Mar 20 16:14 carta_amor.txt
-rw-r--r-- 1 pi pi 207 Mar 20 16:08 carta_amor.txt.gpg
pi@claudina:~/CIFRADO_lab $ cat carta_amor.txt

Indignada está la brisa
dice que ya no la quiero,
pues no escucho ya el susurro
- que sonábame antes puro -
de su voz entre los cedros.

Francisco Artés

pi@claudina:~/CIFRADO_lab $
```

Contraseña: arpeggio



teobaldo_brutto



Indignada está la brisa
dice que ya no la quiero,
pues no escucho ya el susurro
- que sonábame antes puro -
de su voz entre los cedros

Les gusta a **paulo_scemo** y **14.345 personas más**

teobaldo_brutto ya están estos dos pardillos enviándose cartitas tontas otra vez, nunca aprenderán, esto va a acabar como una tragedia griega...



Agrega un comentario...

Publicar

- Todo iba fenomenal, pero el malvado Teobaldo la lía parda en el Instagram de Verona...

Cifrado Asimétrico – Generación de Parejas de Claves

Como comentábamos al principio, estando la comunicación secreta entre los amantes a pleno rendimiento, Teobaldo intercepta un mensaje, consigue la clave a través de sus malas artes, y publica la historia en Instagram.

Ellos dos siguen el consejo de Fray Lorenzo: deciden emplear un cifrado asimétrico; cada uno de ellos conocerá su clave privada, y además sabrá con certeza que el mensaje recibido proviene del otro, pues él o ella lo habrá cifrado con la clave pública recíproca.

Pareja de claves de Claudio Romeo Montesco:

- Privada: la password elegida. No desvelar a nadie.
- Pública: la clave generada para enviar a Claudina.

Pareja de claves de Claudina Julieta Capuleto:

- Privada: la password elegida. No desvelar a nadie.
- Pública: la clave generada para enviar a Claudio.

Generación de Pareja de Claves de Claudio Romeo Montesco

```
gpg: /home/pi/.gnupg/trustdb.gpg: se ha creado base de datos de confianza
gpg: clave 45069128A6AD318E marcada como de confianza absoluta
gpg: creado el directorio '/home/pi/.gnupg/openpgp-revocs.d'
gpg: certificado de revocación guardado como '/home/pi/.gnupg/openpgp-revocs.d/C2EB5EA4891914DE7C9B8DF545069128A6AD318E.rev'
claves pública y secreta creadas y firmadas.

pub  rsa4096 2021-03-20 [SC] [caduca: 2021-03-27]
     C2EB5EA4891914DE7C9B8DF545069128A6AD318E
uid                          Claudio Romeo (Hola Claudina) <francisco.artes@icloud.com>
sub  rsa4096 2021-03-20 [E] [caduca: 2021-03-27]

pi@claudio:~/CIFRADO_lab/Asimetrico $
```

```

pi@claudina: ~/CIFRADO_lab/Asimetrico
pi@claudina:~/CIFRADO_lab/Asimetrico $ gpg --full-generate-key
gpg (GnuPG) 2.2.12; Copyright (C) 2018 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.

Please select what kind of key you want:
  (1) RSA and RSA (default)
  (2) DSA and Elgamal
  (3) DSA (sign only)
  (4) RSA (sign only)
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (3072) 4096
Requested keysize is 4096 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) 7
Key expires at Sat Mar 27 16:49:20 2021 CET
Is this correct? (y/N) y

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

Real name: Claudina Julieta
Email address: francisco.artes@outlook.com
Comment: Hola Claudio
You selected this USER-ID:
    "Claudina Julieta (Hola Claudio) <francisco.artes@outlook.com>"

Change (N)ame, (C)omment, (E)mail or (O)key/(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.

```

Generación de Pareja de Claves de Claudina Julieta Capuleto

```

lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
x Enter passphrase x
x x x
x x x
x Passphrase: x
x x x
x <OK> <Cancel> x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj

```

Contraseña: acorde_sinfonico

Generación de Pareja de Claves de Claudina Julieta Capuleto

```
gpg: /home/pi/.gnupg/trustdb.gpg: trustdb created
gpg: key 7D20A5DB8363C0AE marked as ultimately trusted
gpg: directory '/home/pi/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/pi/.gnupg/openpgp-revocs.d/9628FCEDA789691C9BFF282D7D20A5DB8363C0AE.rev'
public and secret key created and signed.

pub   rsa4096 2021-03-20 [SC] [expires: 2021-03-27]
       9628FCEDA789691C9BFF282D7D20A5DB8363C0AE
uid           Claudina Julieta (Hola Claudio) <francisco.artes@outlook.com>
sub   rsa4096 2021-03-20 [E] [expires: 2021-03-27]

pi@claudina:~/CIFRADO_lab/Asimetrico $
```

Claudio exporta su clave pública

```
pi@claudio:~/CIFRADO_lab/Asimetrico $ pi@claudio:~/CIFRADO_lab/Asimetrico $ gpg -a --export francisco.artes@icloud.com > claudio.gpg.asc
pi@claudio:~/CIFRADO_lab/Asimetrico $ ls -l
total 8
-rw-r--r-- 1 pi pi 3183 mar 20 16:59 claudio.gpg.asc
-rw-r--r-- 1 pi pi 366 mar 20 16:29 ultima_carta.txt
pi@claudio:~/CIFRADO_lab/Asimetrico $ cat claudio.gpg.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBGBWf3oBEADvIxallpWcKnu7hx5wLSyM/N3fGxfxEwoVTfqFopgT/YtKNq1+
g6RFLJpTIFYjYiMynSAUBLLSE6n4D1V5mSMR/Dp9yyLaBNhhUJGnB9Ov4o39Yp4ka
r16+1HRRZOZwKCZuvIEMMFU+HSKfuB4ASApEUIwKmHw8YZOLyW29mmbaHRa17c0F
5IA5vvoYlGcLnHrHAGA4kxw3bGkaS+WxmeBrepVFctxXlbrVH9reSbCJMgiJdM
PirlawO6eBQFW7qlbk13MjTMOT4dfrXTovya32DXxIUml2NS32SP6xNXkFGJIZW7
1JbMIA8wdrw142ydwYXgUOVXZJTYZ28fxnh5IjZPK2hLmCk2k3dImCr7H2+tj45I
6gQqDvY8LAL96oFFOqI8IZflhDFMHTeazQZOiu1X+zFFJkCg26sQndwqVXJ8uYRz
X9mFRons6CMUnlaiuFjaJbLnOAHj47WSXG1Gb92w/xLYWS/jHFSIzflYwF4pw8vN
OAaqjPv+5tC7u+Ke4BHHpSxpCUNjfQJmJjRIqN3mxAL3Q6Jddg5KqqEQsVsFFFH
PvUsciI+1zaN+ygqfXuwicFlby3S1uxvDCYaeXzFnuYgP1LdhojZ2RvXwHPWda0L
fSUpD6VDtZ/8unK/x9qJbR3113qj9GoyLzDEa7pClq9DEv2Ebous0UuFQARAQAB
tDpDbGF1ZGlwIFJvbnVvVichIb2xhIENsYXVkaW5hKSA8ZnJhbmNpc2NvLmYyZGVz
QGljbG91ZC5jb20+iQJUBBMBCGAFiEEwutePik2FN58m431RQaRKKatMY4fAmBW
F3oCGwMFCQAJoAFCwkIBwIGFQoJCAsCBBCAwEChgECF4AACGkQRQARKKatMY4/
RBAApiYKtpInmdy9jY3ntWrrjOTYICituWcbO8dyuP76/wc+c5WhieYwIATP9zoyB
9wExXo8wDKIBWzsc+CHKDpWypDYCvCJueZXBg9WK3wmI3yA62LoxHWRh1Q2EBVB
clMZR6agQOUKp6ZAZPIliwuREFSCI2jeuWaYEtGIqcbRF5h+xHsIkpypWh0ZiTS5C
0A67tIOxm+CFkcnBnksQCeJgGanwli9ERHaKafOIC28CcfmhSAGBsFFYf5GQfgc
P7ufLaxcoCG85/XORrrk0dVCUauC+Ig7YkjKb7krwajpmI+AbAlrYan1+2yoH0m
RdsnvJlVmfzUO7P1SBbIpIIX2fLMOVspH21XFC+jdoT3XSV+qLe+XEiIn35lEWR
bAb6brKIUt2ByfJWYDvu8C8Np0c66d/NV7+G6iAxfnEzhd9rhxPv/1Ya2mm9e1DL
53yq+5UwtPMr2hUtibwW3BKFPXPP2tYJbhACrLfnOQZ2e2XP2U1v0AmMiJGKs/r
JrMo8uq69eT6srtLzneyB/IMqu0I7lEMvhACyFJcdElMtKzPgdfoq/2cuL4rBv1
x/kNO2GbUoFuxDseyUilLvsYFmdeO1+ligqKK9H558C/HJF269juyOZ/E9ckF3G8
btrvc1U8HntBvoZ8amVS1scsCV8guT199NhKfH8AmwFsau5Ag0EYFYegQBAEMEY
/1gh6a/Wh/Pjnc/fTygoellq+05ilt3psq0JJlMMfA+VcnNcG1PoyZVSsvYSiH
K9cDn41kV+KpQDvBGvqQ+7IvuuUQyYrAC1XiGny5J0mVot1KuS6eQis8FoH0i1
6Ql4d1Rrmgch5u3KwAcAUAc979jHp20oY/bDaR4zVzs5/x8UdnvF0ClkJmIa7s/
MVv18/os4ejPlvWxzy0ZmaFkh+dICFCj6Rwsu338ysM6fWcL2XFds9EGTbA+DYC7
0JY3Q/RU8yEvoO/tF2Ddh4iJQdPRYWP0qg/da6NZTgHkZVaKlfenpsYahsr0JN7
q7Q6A5W37ztCSZNG+g2tKold9huZUOhF/HNiAtnvwBSCBgKmiDgs7toXlNgSik0
snkg0m/PuB2eXDTYAXM09kqr+F6sRVxG211Mm5WqDg+tbO6NeuKwoanrLYcSk0Qy
/jpmrob/Ib2Iqb4H2QZqQ0lx6GyF7d9KybPENd2TfdwjaZkhd9y2HAXm3b2dpDsE
cVMEmcFA62Hhz+nJH52jHKCFmzx2Nv6Qn75bbOoXNr05Kj4PKAFI29rM7fZPZTDY
xpHDX36VidOTCJHOQH7CDiG9Z8owSCL84822V18ksXD5YftL65YzFwDs1S6cPgE
B+a5oxCA8EeAnqMWDsW8uSsLt1/y6mHsjchr9389ABEBAAGJAjwEGAECACWlQITC
```

Claudina exporta su clave pública

```
pi@claudina:~/CIFRADO_lab/Asimetrico $ gpg --export francisco.artes@outlook.com > claudina.gpg.asc
pi@claudina:~/CIFRADO_lab/Asimetrico $ ls -l
total 8
-rw-r--r-- 1 pi pi 3187 Mar 20 17:02 claudina.gpg.asc
-rw-r--r-- 1 pi pi 167 Mar 20 16:33 ultima_respuesta.txt
pi@claudina:~/CIFRADO_lab/Asimetrico $ cat claudina.gpg.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBGBWGB4BEACqU+aaCVk6MkRuoKZkRzassZEITMURkuPlnoZmVwbujgNDK/0m
mVTUzbRmFIAHyc4j0AWD2yB9CKATArW5R66v7i+UH6Uc3mKyZtYp2szm8SkwpNL/
9mJlWex0ODGtYhFA2/CWijt/jG/9V4n0+B4sYL0K2KGyXK08fUuU/56YmJlH6owQ
BuhGkXQ8B1qbCD3eS/AbtdUBxYBCjLxwDKNoTpr6BN+ydE1HX/kqhYMRU2EZt09
SLOWL4lpWzZZaXK1q5IMPwUZpxL0gVBHYBpg75Bd28ZFVKWxX/pDSsNCnJp0FqUB
sq9R92shnWCx7uyAicNJEjVSPv4tUZH306ggBX8Q98hwy1Ma7tn/W+QbQ7L4Av7K
DmlyBr1R22MKqe/3qf8cdf8ELA5BdE959+XT5IFr6yjCrcuDfSDP+3cnQEYNasdq
1DS76VTAS5Fo8OJQ4KSglVB6xzLyy97RhSknBBt21KGrvN+kVBQu0OXnpUnFjrXP
zlttEYUfFuGA9d9o1iGpIZAud8vH1+oVaAv1VxJdFHxnNphum0Lm967ridfWha
gR0b299uUY5uJrySlU2oJqkwgRiboN1QJukWJSwtl1CYPrV8MJ2em1quz1M1LaW
L9V7N+Qg8mfNho1lLtjxs0ZzBwdpurohIyrXGyzwvBVwDE7mzN0zZODSvARAQAB
tD1DbGF1ZGluYSBKbWxpZXRhIChlb2xhIENsYXVkaW8pIDxmcuFuY21zY28uYXJ0
ZXNAb3V0bG9vay5jb20+IQUBBMBcGgA+FiEELij87aeJaRyb/ygtfSC124NjwK4F
AmBWGb4CGwMFCQAJoAFCwkIBwIGFQoJCAAsCBBYCAwECHgECF4AAAGkQFSC124Nj
wK7Csg/9FmS62Z68kNBDcXc4JWYLSGp56P1BCGV6ahEWdZ8nh43F+4rdurvtvpCx
6qAxSg9rQsQxrInB8bbc8dN4SCguak9cudUsx0TY194yS2t+pHRJs9xuMXkeW/Nj
95dASTG28PLIEOWqjXW1Tl19+JxrS6sj2wrvIppvNqniICzBAfHHYbE7kUA+dG/m
17fMocgEEkwTv9LOAI504whPH3bksEYxcgmHyPvDFmX218D14ca08ncDP5/Tjs1/
Vs6EFVfv8hYK5yOaozppfY5r80aR8nxjMBN492dZvIkhEmLuEdxQwwgyByWDDPqn
/hzTqdRv2gcySOWNvtu5bd9dw/s+Ofr80Lwgu0YFSw99XJBKjx9Fr4s8bg1Y3JW
/9maY44a19ZglEwBBwPQeOqEdk9QmDvoSs66g7yDKIYD31sIyWrh611DP9CeWyLU
D5iV61fRd5UxMgd5nKuSpMj1MnHrXs5BSADuCWjBUYxSuzx7kCb+2XuSePbCOVS9R
dD2Or+THS6SGoy10idqTREGxjsYwA1NoD4iWV/e9W1S8OP420uDXiSWixf1FCQ/O
a19ofRr5DPUpu+7nGf71Cp6ftMGyVkeFG74uzpd0X0MsmqJTSBpkqVwMBNMOXyK7
Kt8mOstEIE4d47vt0APxRm03fAxx8dvDFdVfBp25xtEtEq5rza5Ag0EYFFZvgEQ
AL+hEvg9GT8AAu0FhDddnjGhpvNgKg5kQ8Cy/qfp9Fhr9EmyLKe96AwUNLHWEW
Cu0GBvJqlsDV0Qj68LrTgg1v196I1FsswVQ5F42QpT5ZyVK55YbEUyoJB1UvFu8S
GixypcIsvPYZ27yCtlt0VQxnQ1UnZKhgYcse4DHFur6rcs7jtLk460rdRq5M8AE6
WZ1KCvnmG8jldEE8V1yRkVouINhyvGjtwxYLNYYR5eD0YH5VsauX5B8XHd3GD8mJ
IaJCVEGpv18RXY+0ndn90AdMZ1rwNPFt22mu5MErNcDoSWyD1VONSJ6kcNBa/Sb9
ywwI7qBFVLVpQq3GS6YdBNVeJ/AZzeNjFJZ1glrYC4iSPFu0BsAuA5rqT4Py+uu
fXgsFblgnlDdpbdgByZlpmmoJ5pC/R5WWHCRrmxiKXQ0iHM2XwYsZb5+2fh8rVZ2
8J8NwI/NqwpTKlm7i4TgYFXhgmUc4o0usiatpvlpI8AwJitxeRhW01N0agDfglmc
gbyXo5JAbA8Mgf0t65Y8TMC1zfBdlbqQ/ONAWOj99EWJOJw38qU8NKQkfkqy/m
lDkDw1UvZ0SdMzX1icEAY0NeEh6F35m2UaaSM0JHyR/vAsOyVvy9aLgDOcxM26C
FH/1lmIwZuGSwoiBQZGmbvNPDfAssGnevduqYyTLCgtHABEBAAGJAjwEGAECACYW
```

Claudio y Claudina intercambian sus claves públicas

```
pi@claudio: ~/CIFRADO_lab/Asimetrico
pi@claudio:~/CIFRADO_lab/Asimetrico $ ls -l
total 8
-rw-r--r-- 1 pi pi 3183 mar 20 16:59 claudio.gpg.asc
-rw-r--r-- 1 pi pi 366 mar 20 16:29 ultima_carta.txt
pi@claudio:~/CIFRADO_lab/Asimetrico $ sftp claudina
pi@claudina's password:
Connected to claudina.
sftp> pwd
Remote working directory: /home/pi
sftp> cd CIFRADO_lab
sftp> cd Asimetrico
sftp> pwd
Remote working directory: /home/pi/CIFRADO_lab/Asimetrico
sftp> put claudio.gpg.asc
Uploading claudio.gpg.asc to /home/pi/CIFRADO_lab/Asimetrico/claudio.gpg.asc
claudio.gpg.asc 100% 3183 1.5MB/s 00:00
sftp> ls -l
-rw-r--r-- 1 pi pi 3187 Mar 20 17:02 claudina.gpg.asc
-rw-r--r-- 1 pi pi 3183 Mar 20 17:11 claudio.gpg.asc
-rw-r--r-- 1 pi pi 167 Mar 20 16:33 ultima_respuesta.txt
sftp> quit
pi@claudio:~/CIFRADO_lab/Asimetrico $

pi@claudina: ~/CIFRADO_lab/Asimetrico
pi@claudina:~/CIFRADO_lab/Asimetrico $ ls -l
total 8
-rw-r--r-- 1 pi pi 3187 Mar 20 17:02 claudina.gpg.asc
-rw-r--r-- 1 pi pi 167 Mar 20 16:33 ultima_respuesta.txt
pi@claudina:~/CIFRADO_lab/Asimetrico $ sftp claudio
The authenticity of host 'claudio (192.168.1.30)' can't be established.
ECDSA key fingerprint is SHA256:WxJs+bdxTgB860Ai0LLXuvjKM7l2ku0L2zLU3Qa4W4U.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/pi/.ssh/known_hosts).
pi@claudio's password:
Connected to claudio.
sftp> pwd
Remote working directory: /home/pi
sftp> cd CIFRADO_lab/Asimetrico
sftp> pwd
Remote working directory: /home/pi/CIFRADO_lab/Asimetrico
sftp> put claudina.gpg.asc
Uploading claudina.gpg.asc to /home/pi/CIFRADO_lab/Asimetrico/claudina.gpg.asc
claudina.gpg.asc 100% 3187 1.5MB/s 00:00
sftp> ls -l
-rw-r--r-- 1 pi pi 3187 Mar 20 17:12 claudina.gpg.asc
-rw-r--r-- 1 pi pi 3183 Mar 20 16:59 claudio.gpg.asc
-rw-r--r-- 1 pi pi 366 Mar 20 16:29 ultima_carta.txt
sftp> quit
pi@claudina:~/CIFRADO_lab/Asimetrico $
```


Claudio y Claudina importan sus recíprocas claves públicas

```
pi@claudio: ~/CIFRADO_lab/Asimetrico
pi@claudio:~/CIFRADO_lab/Asimetrico $ ls -l
total 12
-rw-r--r-- 1 pi pi 3187 mar 20 17:12 claudina.gpg.asc
-rw-r--r-- 1 pi pi 3183 mar 20 16:59 claudio.gpg.asc
-rw-r--r-- 1 pi pi 366 mar 20 16:29 ultima_carta.txt
pi@claudio:~/CIFRADO_lab/Asimetrico $ gpg --import claudina.gpg.asc
gpg: clave 7D20A5DB8363C0AE: clave pública "Claudina Julieta (Hola Claudio) <francisco.artes@outlook.com>" importada
gpg: Cantidad total procesada: 1
gpg:      importadas: 1
pi@claudio:~/CIFRADO_lab/Asimetrico $

pi@claudina: ~/CIFRADO_lab/Asimetrico
pi@claudina:~/CIFRADO_lab/Asimetrico $ ls -l
total 12
-rw-r--r-- 1 pi pi 3187 Mar 20 17:02 claudina.gpg.asc
-rw-r--r-- 1 pi pi 3183 Mar 20 17:11 claudio.gpg.asc
-rw-r--r-- 1 pi pi 167 Mar 20 16:33 ultima_respuesta.txt
pi@claudina:~/CIFRADO_lab/Asimetrico $ gpg --import claudio.gpg.asc
gpg: key 45069128A6AD318E: public key "Claudio Romeo (Hola Claudina) <francisco.artes@icloud.com>" imported
gpg: Total number processed: 1
gpg:      imported: 1
pi@claudina:~/CIFRADO_lab/Asimetrico $
```

Claudio y Claudina cifran sus mensajes con las claves recíprocas

```
pi@claudio: ~/CIFRADO_lab/Asimetrico
pi@claudio:~/CIFRADO_lab/Asimetrico $ ls -l
total 12
-rw-r--r-- 1 pi pi 3187 mar 20 17:12 claudina.gpg.asc
-rw-r--r-- 1 pi pi 3183 mar 20 16:59 claudio.gpg.asc
-rw-r--r-- 1 pi pi 366 mar 20 16:29 ultima_carta.txt
pi@claudio:~/CIFRADO_lab/Asimetrico $ gpg -a -r francisco.artes@outlook.com --en
crypt ultima_carta.txt
gpg: D50E7A7BE52FBE4C: No hay seguridad de que esta clave pertenezca realmente
al usuario que se nombra

sub rsa4096/D50E7A7BE52FBE4C 2021-03-20 Claudina Julieta (Hola Claudio) <franci
sco.artes@outlook.com>
Huella clave primaria: 9628 FCED A789 691C 9BFF 282D 7D20 A5DB 8363 C0AE
Huella de subclave: 02CB 533B 39E4 65AB B586 4AD8 D50E 7A7B E52F BE4C

No es seguro que la clave pertenezca a la persona que se nombra en el
identificador de usuario. Si *realmente* sabe lo que está haciendo,
puede contestar sí a la siguiente pregunta.

¿Usar esta clave de todas formas? (s/N) s
pi@claudio:~/CIFRADO_lab/Asimetrico $ ls -l
total 16
-rw-r--r-- 1 pi pi 3187 mar 20 17:12 claudina.gpg.asc
-rw-r--r-- 1 pi pi 3183 mar 20 16:59 claudio.gpg.asc
-rw-r--r-- 1 pi pi 366 mar 20 16:29 ultima_carta.txt
-rw-r--r-- 1 pi pi 1199 mar 20 17:29 ultima_carta.txt.asc
pi@claudio:~/CIFRADO_lab/Asimetrico $

pi@claudina: ~/CIFRADO_lab/Asimetrico
pi@claudina:~/CIFRADO_lab/Asimetrico $ ls -l
total 12
-rw-r--r-- 1 pi pi 3187 Mar 20 17:02 claudina.gpg.asc
-rw-r--r-- 1 pi pi 3183 Mar 20 17:11 claudio.gpg.asc
-rw-r--r-- 1 pi pi 167 Mar 20 16:33 ultima_respuesta.txt
pi@claudina:~/CIFRADO_lab/Asimetrico $ gpg -a -r francisco.artes@icloud.com --en
crypt ultima_respuesta.txt
gpg: checking the trustdb
gpg: marginals needed: 3 completes needed: 1 trust model: pgp
gpg: depth: 0 valid: 1 signed: 0 trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2021-03-27
gpg: 35DE0098C5D447FD: There is no assurance this key belongs to the named user

sub rsa4096/35DE0098C5D447FD 2021-03-20 Claudio Romeo (Hola Claudina) <francis
co.artes@icloud.com>
Primary key fingerprint: C2EB 5EA4 8919 14DE 7C9B 8DF5 4506 9128 A6AD 318E
Subkey fingerprint: 4E80 F077 5671 743C 6382 FCD1 35DE 0098 C5D4 47FD

It is NOT certain that the key belongs to the person named
in the user ID. If you *really* know what you are doing,
you may answer the next question with yes.

Use this key anyway? (y/N) y
pi@claudina:~/CIFRADO_lab/Asimetrico $ ls -l
total 16
-rw-r--r-- 1 pi pi 3187 Mar 20 17:02 claudina.gpg.asc
-rw-r--r-- 1 pi pi 3183 Mar 20 17:11 claudio.gpg.asc
-rw-r--r-- 1 pi pi 167 Mar 20 16:33 ultima_respuesta.txt
-rw-r--r-- 1 pi pi 1053 Mar 20 17:29 ultima_respuesta.txt.asc
pi@claudina:~/CIFRADO_lab/Asimetrico $
```

Claudio y Claudina intercambian sus mensajes cifrados

[illegible]

Claudio y Claudina descifran los mensajes con sus claves privadas

```
pi@claudio: ~/CIFRADO_lab/Asimetrico
pi@claudio:~/CIFRADO_lab/Asimetrico $ gpg -a --decrypt ultima_respuesta.txt.asc
> ultima_respuesta.txt
gpg: cifrado con clave de 4096 bits RSA, ID 35DE0098C5D447FD, creada el 2021-03-20
"Claudio Romeo (Hola Claudina) <francisco.artes@icloud.com>"
pi@claudio:~/CIFRADO_lab/Asimetrico $ ls -l
total 24
-rw-r--r-- 1 pi pi 3187 mar 20 17:12 claudina.gpg.asc
-rw-r--r-- 1 pi pi 3183 mar 20 16:59 claudio.gpg.asc
-rw-r--r-- 1 pi pi 366 mar 20 16:29 ultima_carta.txt
-rw-r--r-- 1 pi pi 1199 mar 20 17:29 ultima_carta.txt.asc
-rw-r--r-- 1 pi pi 167 mar 20 17:42 ultima_respuesta.txt
-rw-r--r-- 1 pi pi 1053 mar 20 17:36 ultima_respuesta.txt.asc
pi@claudio:~/CIFRADO_lab/Asimetrico $ cat ultima_respuesta.txt

No recuerdo tu mirar,
de tus labios no me acuerdo,
pero tengo tu sentir
muy profundo, muy muy dentro,
y ahora puedes escuchar
lo que sabes, que Te Quiero.

Claudina

pi@claudio:~/CIFRADO_lab/Asimetrico $
pi@claudio:~/CIFRADO_lab/Asimetrico $
pi@claudio:~/CIFRADO_lab/Asimetrico $
pi@claudio:~/CIFRADO_lab/Asimetrico $
pi@claudio:~/CIFRADO_lab/Asimetrico $
pi@claudio:~/CIFRADO_lab/Asimetrico $
pi@claudio:~/CIFRADO_lab/Asimetrico $
pi@claudio:~/CIFRADO_lab/Asimetrico $

pi@claudina: ~/CIFRADO_lab/Asimetrico
pi@claudina:~/CIFRADO_lab/Asimetrico $ gpg -a --decrypt ultima_carta.txt.asc > u
ltima_carta.txt
gpg: encrypted with 4096-bit RSA key, ID D50E7A7BE52FBE4C, created 2021-03-20
"Claudina Julieta (Hola Claudio) <francisco.artes@outlook.com>"
pi@claudina:~/CIFRADO_lab/Asimetrico $ ls -l
total 24
-rw-r--r-- 1 pi pi 3187 Mar 20 17:02 claudina.gpg.asc
-rw-r--r-- 1 pi pi 3183 Mar 20 17:11 claudio.gpg.asc
-rw-r--r-- 1 pi pi 366 Mar 20 17:44 ultima_carta.txt
-rw-r--r-- 1 pi pi 1199 Mar 20 17:35 ultima_carta.txt.asc
-rw-r--r-- 1 pi pi 167 Mar 20 16:33 ultima_respuesta.txt
-rw-r--r-- 1 pi pi 1053 Mar 20 17:29 ultima_respuesta.txt.asc
pi@claudina:~/CIFRADO_lab/Asimetrico $ cat ultima_carta.txt

Necesito que me ames
¡por tu vida, dame amor!
que me marchó, que me muero
y tan breve es mi existir
y tan corto se hace el tiempo
que prefiero, amor, amarte
a decirte que Te Quiero;
ya no hay tiempo de palabras
de miradas, ni de gestos,
sólo hay tiempo para amarse,
no a la lengua dar recreo
pues es mero intermediario
entre cerebro y cerebro.

Francisco Artés

pi@claudina:~/CIFRADO_lab/Asimetrico $
pi@claudina:~/CIFRADO_lab/Asimetrico $
```

Claudio y Claudina descifran los ficheros con sus claves privadas

[illegible]

Contraseña: arpeggio

[illegible]

Contraseña: acorde sinfonico