

## UF1. [PAC02] SOLUCIÓN

### Actividades

#### Parte teórica

1. Explicar las diferencias entre los algoritmos de cifrado de clave pública y de clave privada. ¿Qué ventajas e inconvenientes tiene cada uno de ellos?

Los sistemas simétricos o de clave privada usan una misma clave para cifrar y descifrar los mensajes, que deben compartir emisor y receptor, y que no debe conocer nada más.

Ventajas:

- El proceso de cifrado suele ser bastante más rápido que los sistemas que utilizan los algoritmos de clave pública.

Inconvenientes:

- Requieren de un sistema de distribución de claves (entre emisor y receptor) muy seguro, ya que en caso de que alguien más conozca la clave, el mensaje queda comprometido.
- Complejidad de gestión de las claves en caso de tener múltiples receptores, ya que para cada uno usaremos una clave diferente.

Por otro lado, los sistemas asimétricos o de clave pública, usan dos claves, una secreta que solo conoce el emisor, y una clave pública que comparte con los receptores.

Usamos la clave pública del emisor para cifrar los mensajes que le enviamos y él los podrá verificar que el mensaje lo hemos mandado nosotros. La criptografía asimétrica basa su seguridad en la complejidad de obtener la clave secreta a partir de la pública, que suele ser un proceso computacionalmente muy costoso.

Ventajas:

- Permiten conseguir autenticación y no repudio para muchos protocolos criptográficos, lo que significa que, si firmamos un correo con nuestra clave privada, esto nos identifica como emisor del mensaje y verifica la autenticidad de éste.
- Suelen emplearse en colaboración con cualquiera de los otros métodos criptográficos. Hay muchos protocolos seguros que usan los algoritmos de clave pública para intercambiar un mensaje cifrado que contenga una nueva clave privada de criptografía simétrica, y a partir de entonces usan esta clave para enviarse grandes cantidades de datos cifradas, ya que la criptografía de clave secreta es bastante más rápida. Y la criptografía de clave pública ya nos resuelve el problema de intercambiar la clave privada que tenían los sistemas anteriores.
- Permiten tener una administración sencilla de claves al no necesitar que haya un intercambio seguro de claves.

### Inconvenientes:

- Son algoritmos más lentos que los de clave secreta, con lo que no suelen utilizarse para cifrar gran cantidad de datos.
- Sus implementaciones son hechas comúnmente con software.
- Para una red de usuarios y/o máquinas se requieren un sistema de certificación de la autenticidad de las claves públicas.
- Dan lugar a mensajes cifrados de mayor tamaño que los originales.

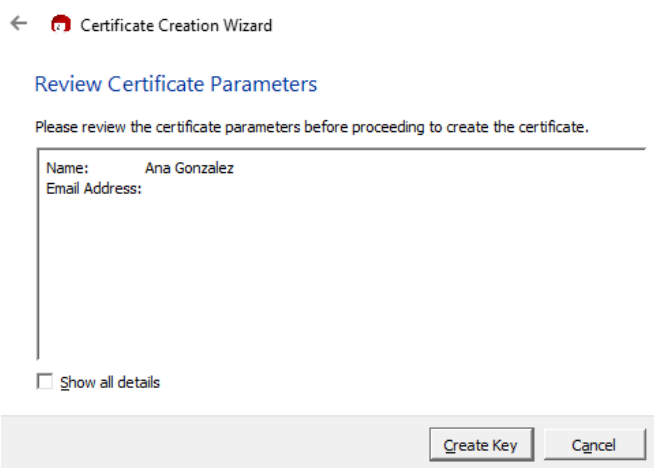
### 2. Explica para qué sirve firmar un correo.

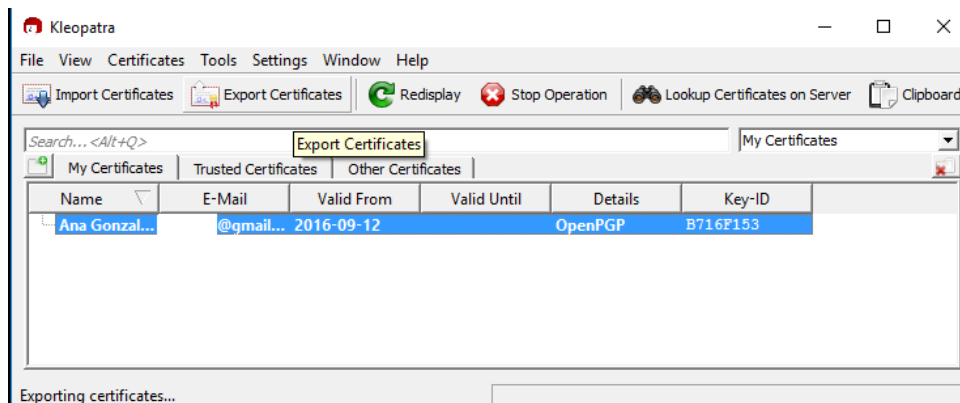
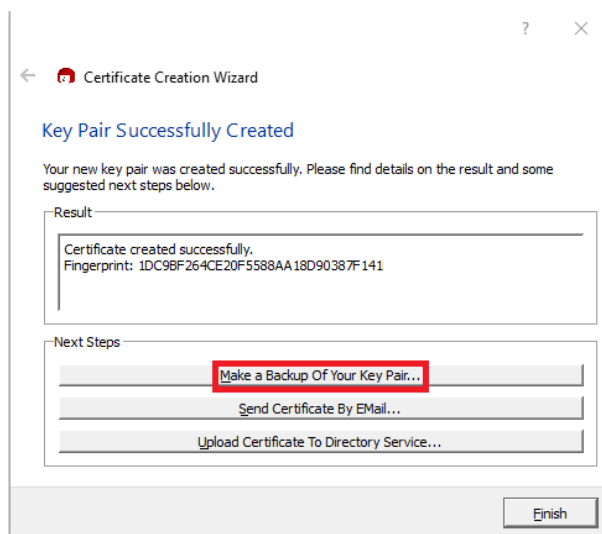
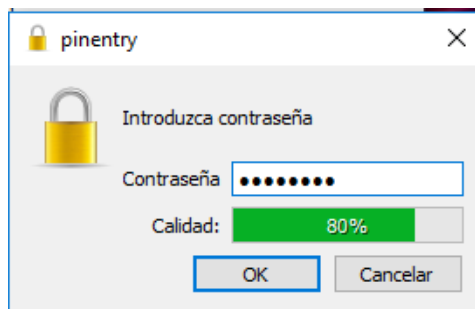
Para firmar un mensaje, ciframos con nuestra clave privada un resumen del mensaje (generado por una función hash) y lo enviamos junto al mensaje original. Entonces, el receptor lo podrá verificar con nuestra clave pública. Para ello, el receptor descifrá con la clave pública del emisor el mensaje resumen cifrado enviado junto al mensaje original, y verificará que coincida con el mensaje resumen generado por nosotros (con la misma función hash, habitualmente MD5 o Hash-1).

La firma de un mensaje sirve principalmente para dos cosas, para verificar que el emisor es quién dice ser, es decir, la firma autentica el mensaje como generado por el emisor. Y segundo, verifica la integridad del mensaje, es decir, verifica que no ha sido modificado por terceros.

### Parte práctica

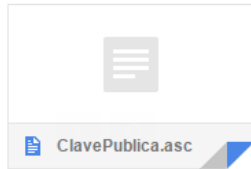
3. Crear un par de claves (pública y privada) con el programa GPG4win que lo podéis descargar de <https://www.gpg4win.org/download.html>, y después:
  - a. Mandar un correo a la siguiente dirección: [agonzalez@ilernaonline.com](mailto:agonzalez@ilernaonline.com) con vuestra clave pública adjuntada, y el asunto: Clave Pública Nombre Apellido1 Apellido2.
  - b. Mandar un mensaje cifrado a [agonzalez@ilernaonline.com](mailto:agonzalez@ilernaonline.com) con el asunto: Mensaje Cifrado Nombre Apellido1 Apellido2.





## CLAVE PUBLICA ANA GONZALEZ BLAZQUEZ ▾

Ana Gonzalez Blazquez <@gmail.com>  
 para agonzalez ▾



← Sign/Encrypt Files

What do you want to do?

Please select here whether you want to sign or encrypt files.

Selected file:

\* C:\Users\Online\Desktop\ENUNCIADOS PACS 1S1617\M09 PROGRAMACIÓN DE SERVICIOS Y PROCESOS\UF1\DAM\_M09\_UF1\_PAC2.docx

☐ Archive files with: TAR (PGP@-compatible)

Archive name (OpenPGP): DOS PACS 1S1617\M09 PROGRAMACIÓN DE SERVICIOS Y PROCESOS\UF1\DAM\_M09\_UF1\_PAC2.docx.tar

Archive name (S/MIME): JS PACS 1S1617\M09 PROGRAMACIÓN DE SERVICIOS Y PROCESOS\UF1\DAM\_M09\_UF1\_PAC2.docx.tar.gz

☐ Sign and Encrypt (OpenPGP only)

☒ Encrypt

☐ Sign

☒ Text output (ASCII armor)

☐ Remove unencrypted original file when done

Next Cancel

← Sign/Encrypt Files

For whom do you want to encrypt?

Please select for whom you want the files to be encrypted. Do not forget to pick one of your own certificates.

Search... All Certificates ▾

Name	E-Mail	Valid From	Valid Until	Details	Key-ID
Ana Gonzalez	@gmail.com	2016-09-12		OpenPGP	B716F153

▼ Add ▲ Remove


Name	E-Mail	Valid From	Valid Until	Details	Key-ID
Ana Gonzalez	@gmail.com	2016-09-12		OpenPGP	B716F153

Encrypt Cancel

```
DAM_M09_UF1_PAC2.docx: Bloc de notas
Archivo Edición Formato Ver Ayuda
|-----BEGIN PGP MESSAGE-----
Version: GnuPG v2

hQEMA+8oo5EbwJ06AQf+L6SttkF79WkAKm9iS276duWs1MAeT9NudQdfEUcJ7q2I
GkXMGs2ou9TKuHhcE8XLPqzP9z0xre+CyuJteYzt8bMcODUNlaKZaIStYHStIPs9
ia6Mb5mM5THhH8NGopc7AiSMIHxYpAK8bZmmwUpqxCSNHL7KFSMT3m60arpzcuJO
kx5z916moCxAdWs2uUyW88dX01t/bSvdnjzUQeid7gXz/G5fB0tkE8EWi5I5wK4R
Egb5ahHgAOEOryRpcqxU33PusF68UXVCT7+E4mQSD4jbtch9NdmVR8jNEv67mrMS
HuEvrMQosTVvbHSOhPEeCRDeHAbd3aTtOsEt7HIDftLtAejwdT9DKdOgkn9JpVLe
PFTBS4eVX8sKSfmdDvMVymPWPRwLCcNOKS49IDa1cn1zrKBul7Y8A4SNSop61Gn
d9CA4Uex0Tcmu1sftGc8+6IJ5Rx9BCxbL58IQy7hfb2GVgnYyippNOL4B68PHojD
zMnGS3KVyS45DEvaR/RVX0vUOu+9Yh2txvytdbHQrta1y51XFrjA7veP8NjWh6hj
JW0sXyW5mAo1FwF+zPZtqzXPhHgP5Uo9KfCtu+ulfrNiitVk0sHEPwHN3XzZmqoA
Ht3R4dqKQ6ceMdfFpaNPjgxCitFLVaW/05ZQQ5ZrgabJDdVKZcASpsARKXfGZ/tv
Lg3LYMN/MyXRpHCi3EYgQmzu8wWuRLUccSLqOS2XDcczXmhnX+sKv2R4dg8bKQ8
8BBAD508yH7hcP+j09DUTCSz01uPPk8j40p607zj3nmu6L1RI3h9TG2kb1jWsYm8
```

## MENSAJE CIFRADO ANA GONZALEZ BLAZQUEZ

Ana Gonzalez Blazquez <@gmail.com>  
 para agonzalez 

-----BEGIN PGP MESSAGE-----  
 Version: GnuPG v2

```
hQEMA+8oo5EbwJ06AQf+L6SttkF79WkAKm9iS276duWs1MAeT9NudQdfEUcJ7q2I
GkXMGs2ou9TKuHhcE8XLPqzP9z0xre+CyuJteYzt8bMcODUNlaKZaIStYHStIPs9
ia6Mb5mM5THhH8NGopc7AiSMIHxYpAK8bZmmwUpqxCSNHL7KFSMT3m60arpzcuJO
kx5z916moCxAdWs2uUyW88dX01t/bSvdnjzUQeid7gXz/G5fB0tkE8EWi5I5wK4R
Egb5ahHgAOEOryRpcqxU33PusF68UXVCT7+E4mQSD4jbtch9NdmVR8jNEv67mrMS
HuEvrMQosTVvbHSOhPEeCRDeHAbd3aTtOsEt7HIDftLtAejwdT9DKdOgkn9JpVLe
PFTBS4eVX8sKSfmdDvMVymPWPRwLCcNOKS49IDa1cn1zrKBul7Y8A4SNSop61Gn
d9CA4Uex0Tcmu1sftGc8+6IJ5Rx9BCxbL58IQy7hfb2GVgnYyippNOL4B68PHojD
zMnGS3KVyS45DEvaR/RVX0vUOu+9Yh2txvytdbHQrta1y51XFrjA7veP8NjWh6hj
JW0sXyW5mAo1FwF+zPZtqzXPhHgP5Uo9KfCtu+ulfrNiitVk0sHEPwHN3XzZmqoA
Ht3R4dqKQ6ceMdfFpaNPjgxCitFLVaW/05ZQQ5ZrgabJDdVKZcASpsARKXfGZ/tv
Lg3LYMN/MyXRpHCi3EYgQmzu8wWuRLUccSLqOS2XDcczXmhnX+sKv2R4dg8bKQ8
8BBAD508yH7hcP+j09DUTCSz01uPPk8j40p607zj3nmu6L1RI3h9TG2kb1jWsYm8
d8LLcwiG12lwLoBkVCmjHpE81LLeKx2vgi+gul6yKy8hICFWi8+C9G+2RpL2NpbO
raY1mDOCvGKLAX4Ajy9BcdJHOicMUI4ahWsZ6hazhWjoNPi9BE7VKG/6ah7jGoc
y5a4XKzwmMzH4ybZTgSMkMfsdWlbnlOSeAzPlc8UeOVm5glZwDpVvdVvpjU1PM4B
cc+wPRBNYqa089PHts3wsfYanGUE8OtfbQSh7iymuER2ucaaiBaLOBjRaT5qMJJn
h8O3i/STfmFyd2UXCqA+UXa8l7f6TwRwXeQbOkQdikz5HLzs3bcBGcV3PFPmHLR
```

