Auditoria de Sistemas de Información

Ing. Erwin Roberto Méndez

emendeza@miumg.edu.gt

Protocolo de Encriptación PGP

PGP o Pretty Good Privacy

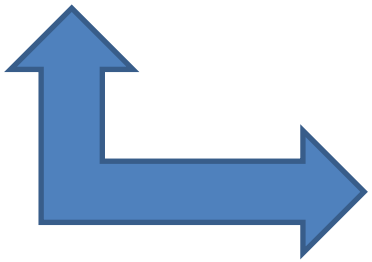
Es posiblemente el *software* de **cifrado de datos más extendido del mundo** para las comunicaciones de datos a través de Internet.

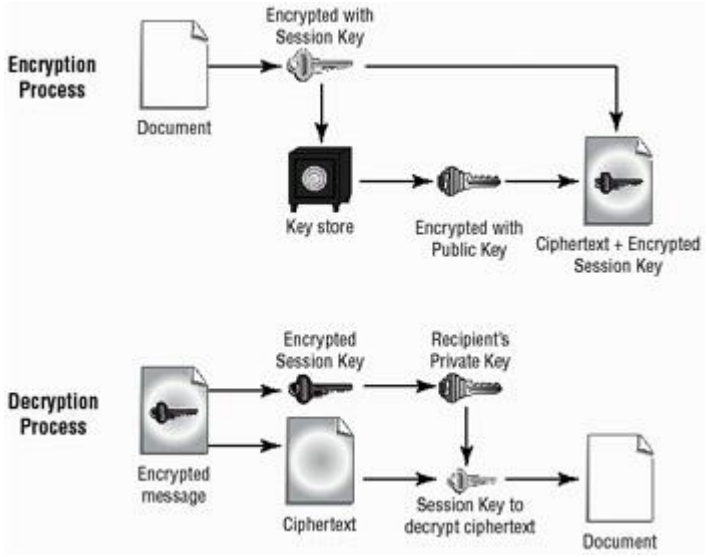
- ✓ Entre sus muchos usos podemos mencionar:
- ✓ Cifrar y descifrar las comunicaciones por email.
- ✓ Garantizar la seguridad de ficheros, directorios
- ✓ Garantizar la seguridad a particiones enteras de disco.

PGP o Pretty Good Privacy

Lamentablemente, a pesar de vivir su segunda juventud por razones de la NSA y de llevar por bandera la *bastante buena privacidad*, su funcionamiento también es *bastante complejo de entender* para el usuario, al que poco le importa la criptografía y al que eso de las claves públicas y privadas le suena algo complicado.

Explicaremos en que consiste





¿Qué es cifrar un mensaje?

Básicamente consiste en coger un texto perfectamente legible y entendible por todo el mundo y convertirlo en algo incomprensible para cualquier persona que intercepta ese mensaje indebidamente.

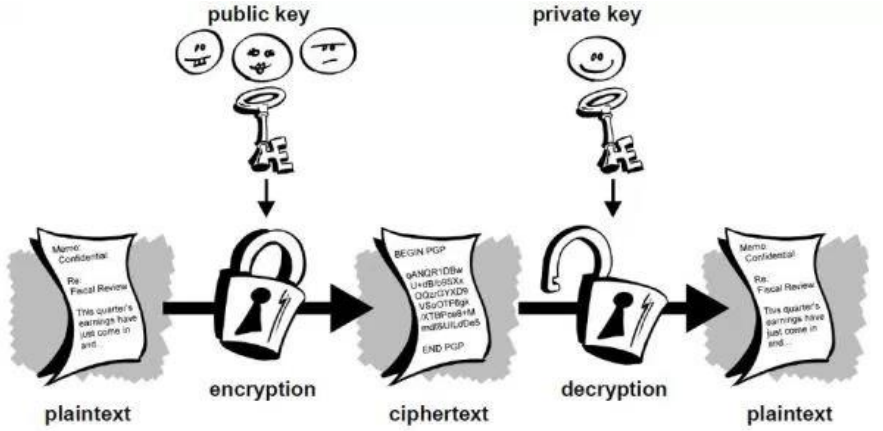
De esta manera, el mensaje cifrado se envía a través de Internet, donde todo el mundo lo puede leer, pero nadie es capaz de descifrarlo, hasta llegar a su destino, donde el receptor es capaz de volver a obtener el mensaje original.

¿Y cómo lo logra el receptor?

Empleando una **clave de descifrado** que sólo él conoce. El problema reside en cómo transmitirle a este receptor la clave a usar.

Aquí es donde entra en juego lo que se conoce como **criptografía asimétrica, de clave pública o de dos claves**, que es el método en el que se basa PGP.

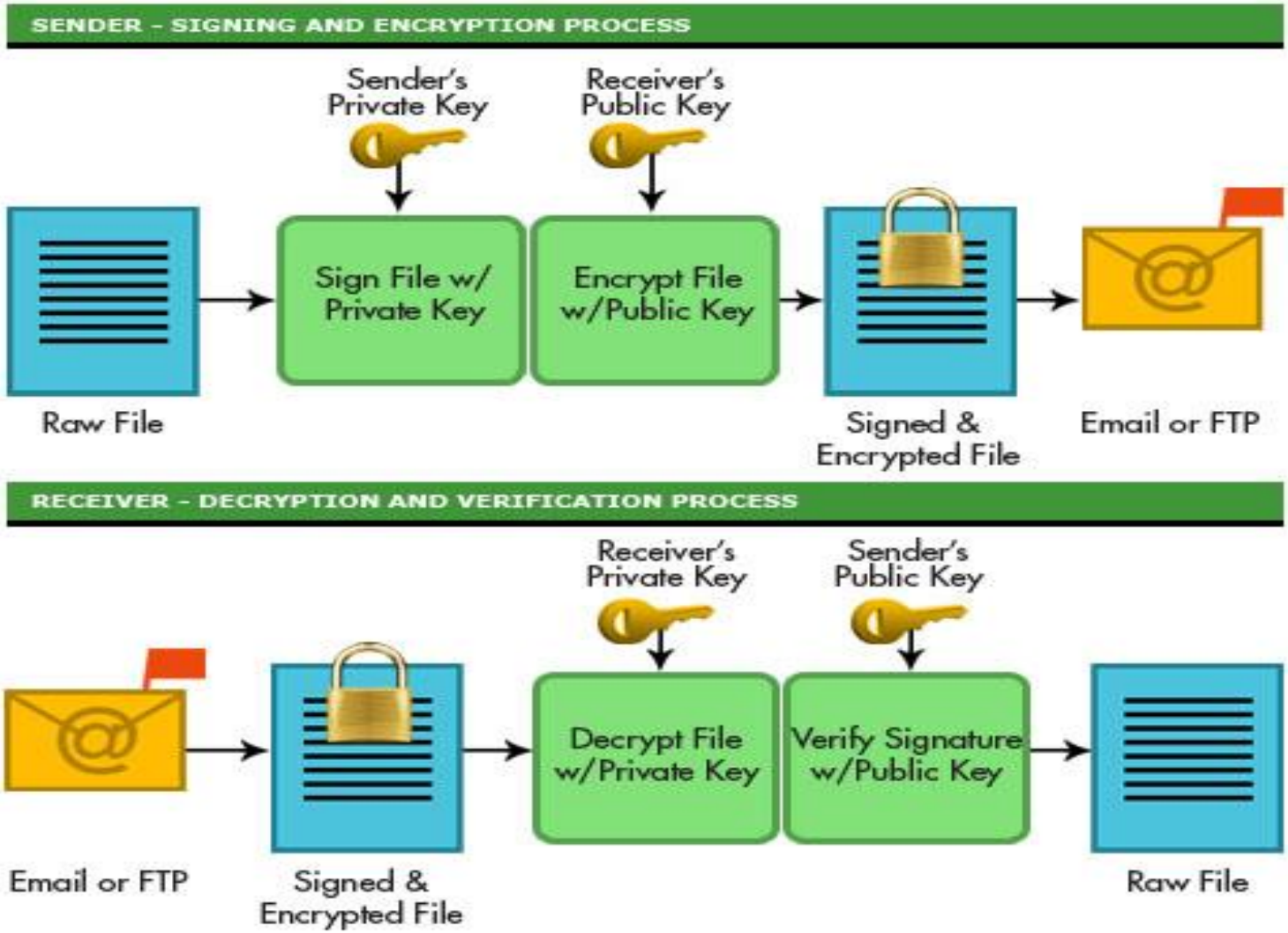
Cada una de las partes de una conversación tiene la posibilidad de crear dos claves, una **privada que sólo es conocida por la persona a la que pertenece** y otra **pública que se proporciona a cualquier persona con la que uno quiera comunicarse de manera segura**. No pasa absolutamente nada si la clave pública está a la vista de todos.



Si quiero escribir un mensaje cifrado a Luis, busco su clave pública que seguramente muestre en la firma de su **correo electrónico, en su web personal o incluso en su perfil de Facebook**, la descargo y cifro mi mensaje usando esa clave con cualquiera de los muchos clientes disponibles.

El mensaje se envía a Luis a través de Internet. Puede que alguien espíe la conversación, pero como resultado sólo obtendrá una ristra de números incomprensibles e imposibles de descifrar.

Cuando el mensaje le llega a Luis, se lo descargará y mediante su clave privada, que sólo él y nadie más que él conoce, podrá descifrar el mensaje que le he enviado. Es importante recalcar la importancia de proteger muy bien nuestra clave privada, ya que es el núcleo en el que se basa la seguridad de este método.


SENDER - SIGNING AND ENCRYPTION PROCESS
Sender's Private Key
Receiver's Public Key
Sign File w/ Private Key
Encrypt File w/Public Key
Raw File
Signed & Encrypted File
Email or FTP
RECEIVER - DECRYPTION AND VERIFICATION PROCESS
Receiver's Private Key
Sender's Public Key
Decrypt File w/Private Key
Verify Signature w/Public Key
Email or FTP
Signed & Encrypted File
Raw File

¿Cómo se hace el cifrado con PGP?

Cuando un usuario emplea PGP para cifrar un texto, éste se comprime para ahorrar espacio, tiempo de transmisión y fortalecer la seguridad, ya que será más difícil de encontrar patrones en el texto para romper el cifrado.

Posteriormente, se crea una clave de sesión secreta que solo se empleará una vez. Esta clave es un número aleatorio generado a partir de los **movimientos del ratón y las teclas que se pulsen durante unos segundos con el propósito específico de generar** esta, también puede combinarlo con la clave anteriormente generada.

Una vez que los datos se encuentran cifrados, la clave de sesión se cifra con la clave pública del receptor, como ya hemos explicado anteriormente, resultando en un mensaje completamente ilegible como el siguiente:

```
<code>
hQEMA8yG//Vk86KdAQf/cISYhN2KuyyOYWiX66JFSesTXFWjB9G5LLqS3bG2JWtl
chZImgm0v41widgDWEXoYkm89CrH1jYoEzH337yLmLmL+q6WMt8EA6Fjzcvqa9GC
ZkxLi5JqMK8s2H4mutn/RzstFDSCMByqwWaxvqHVu0ZuHc+XrW3BEeb1Z9w9zXjs
PvRR4pBHbu1pCS2+lgFMzF9rZ9b830sm9icShn1MhuRWx/pFATwXL2ax2EAkMZ3F
iE3hm1Rq2QgG1lz0ovf/N8PrshHim/p1NdAb2+A6RbNtMqLNeBv7B86991JfgDEN
PsE0HeDHbxZDFOJAjaU9mRS4YSAFarUEJdD/EdTn3ck5johyRjs2ClRoAAgC9cd/
qyQl6hLjR4NpY/IDfCMQVmaCVU5KQFWtxYf+lD44IjW7ZLb+eyRqnpBw=6IFJ
```

¿Cómo puedo crear mis claves y usar PGP?

Hay varias herramientas online con el que puede generar tu clave pública y privada de manera muy sencilla, además de una utilidad para cifrar y descifrar cualquier mensaje. Con estas herramientas, crear una pareja de claves es muy fácil. Uno sólo tiene que **introducir su dirección de correo electrónico al que irán asociadas las claves y una contraseña maestra** para ellas. El programa genera las claves automáticamente, ofreciendo tanto la pública como la privada.

¿Cómo puedo crear mis claves y usar PGP?

De la misma manera, también existen **complementos para navegadores** con los que realizar el proceso:

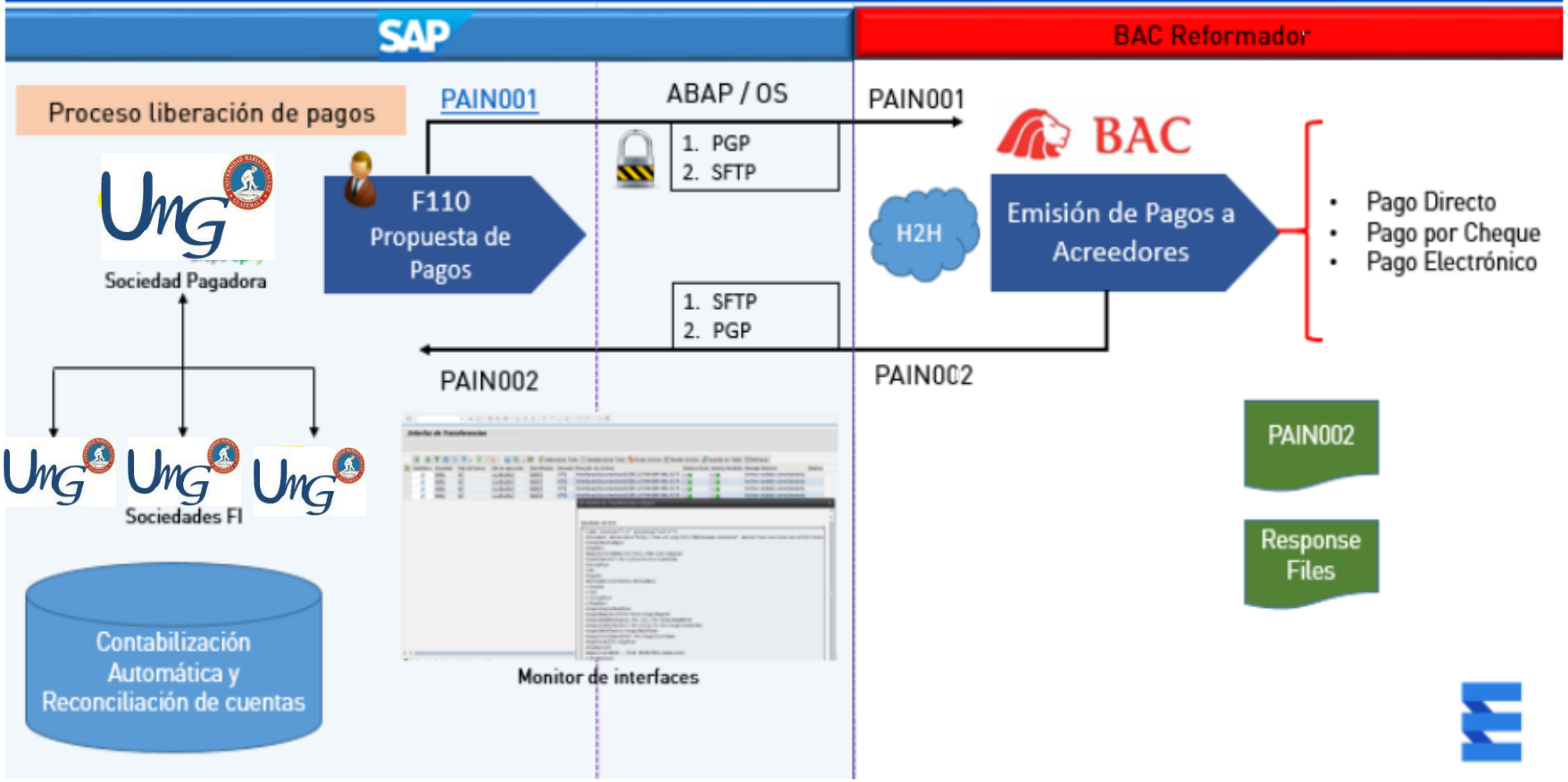
Navegador Chrome **Mailvelope**
En Windows **Gpg4win**
En Mac, **GPG Suite**, por sólo citar algunos ejemplos.

Encriptar correos con Mailvelope

- Crear Claves Publicas y privada https://youtu.be/kw93sS3psvA
- PGP Con Google Chrome + Mailvelope https://youtu.be/z3ySWxCrUPU

Aplicación Practica PGP

Pagos a Acreedores – BAC Reformador



GnuPG https://gnupg.org/index.html http://openpgp.org/