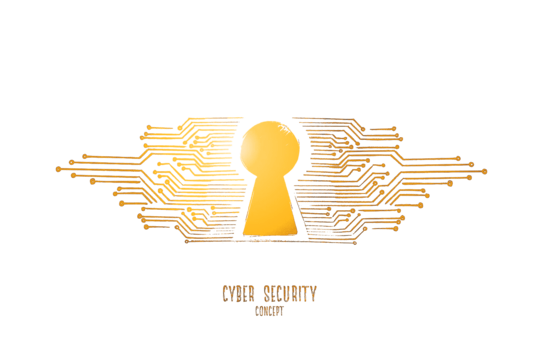
Bastionado de redes 

y sistemas.



# Apartados

1.- Instalar GnuPG

2.- Crear un par de claves pública privada

3.- Exportar clave pública

3.1.- Fichero

3.2.- Servidores (keyserver.ubuntu.com)

4.- Entre dos usuario (cifrar/descifrar)

# Actividad 1

| **1.- Instalar GnuPG** |
| --- |
| Sudo apt-get install gnupg |
| **2.- Crear un par de claves pública privada** |
| # gpg --gen-key  # p para generar clave de forma extendida  gpg --full-gen-key |
|  |
|  |
|  |
|  |
| * /home/ymir/.gnupg/pubring.kbx es la ubicación del archivo de tu llavero GPG donde se almacenan las claves públicas. En este caso, la dirección indica la ubicación en el sistema de usuario "ymir". * pub indica que es una clave pública. * rsa3072 indica que la clave es de tipo RSA con un tamaño de 3072 bits. * 2023-10-26 es la fecha en la que se creó la clave. * [SC] indica que esta clave se utiliza para firmar y cifrar (Signing y Ciphertext). * 24200DDFFCA6381A2A2B76D5A0CE0CA295CD41DD es el ID único de la clave. Este identificador se utiliza para referenciar la clave. * uid [ultimate] bastionado <bastionado@bastionado.ieselrincon.es> muestra la información del usuario asociado con la clave. En este caso, el nombre de usuario es "bastionado" y la dirección de correo electrónico es "bastionado@bastionado.ieselrincon.es". La etiqueta [ultimate] indica que esta clave es la clave de confianza máxima para ese usuario. * sub indica que es una subclave. Las subclaves son extensiones de la clave principal y pueden tener diferentes capacidades. * [E] indica que esta subclave se utiliza para el cifrado (Encryption). |
|  |
| Para listar las claves |
| **Públicas:** |
| gpg -k |
|  |
| **Privadas:** |
| gpg -K |
|  |
| Directorio de claves: |
|  |
| **3.- Exportar clave pública**  **3.1.- Fichero** |
| gpg -k # lista las llaves públicas  # evitando la bandera -o|--output hará que se imprima en el #stdout.  # -a, –armor cambia el formato de salida a Armored ASCII en  # lugar de la salida estándar en binario,  gpg --export -a bastionado > key\_copy.gpg |
|  |
| **\*\*Clave privada**  gpg –export-secret-key -a “ID\_usuario” > key\_copy.key  # nos pedirá la contraseña |
| **Importar la clave pública** |
|  |
| El estado es unknown  Procedemos a firmar con la clave secreta  gpg --edit-key “correo”  fpr  sign    La key cambiará de estado a **full** |
| **4. Entre dos usuarios (cifrar/descifrar)** |
| Al ser cifrado con RSA (asimétricamente) el flujo del envío será tal que: |
| Pc “A” y “B” **sin importar claves públicas**   1. A encripta y envía un mensaje a B.   **A(mensaje) -> pc B**   1. B recibe un mensaje encriptado con una llave pública así que lo encripta también y lo devuelve a A.   **AB(mensaje) -> pc A.**   1. B desencripta el mensaje con su clave secreta y lo envía a B.   **B(mensaje) -> B**   1. B recibe el mensaje encriptado por su clave, así que puede acceder a su información.   **(mensaje)**  El archivo/mensaje siempre ha estado cifrado. |
| Nosotros al ya tener importado la clave pública en nuestra máquina virtual.  **Los mensajes de la máquina con cPub externas puede ser descifrados por ordenadores que tengan la clave privada de dichas claves públicas externas.** |
|  |
|  |
|  |
|  |
| **Lo enviamos a nuestro host y desencriptamos con la clave privada** |
|  |

Recursos :

<https://devhints.io/gnupg>

https://www.gnupg.org/gph/en/manual/x56.html