UD1. Adopción de pautas de seguridad informática. Legislación

Tarea 5 – Cifrado simétrico

OpenPGP es un protocolo no propietario para encriptación basado en el original PGP (Pretty Good Privacy)

La herramienta usada para encriptar es gpg.

Características:

- Para encriptar con clave simétrica se utiliza `gpg --symmetric fichero`
- Pedirá una clave y creará un fichero con extensión .gpg
- Para desencriptar usaremos `gpg --decrypt fichero.gpg`
- Nos pedirá la clave y mostrará el contenido del fichero

Otras opciones de gpg:

- Con `-o` especificamos el fichero de salida
- Con `-a` creamos un fichero ascii en lugar de un fichero binario. Además cambiará la extensión a `.asc` en lugar de `.gpg`
- Con `--cipher-alg` especificamos con qué algoritmo queremos cifrar (por defecto gpg utiliza CAST5). Ejemplo: `gpg --symetric --cipher-alg 3DES fichero` nos cifrará con Triple DES
- También se pueden cifrar ficheros binarios, no sólo de texto

La forma de usar el comando siempre será con las opciones primero y el fichero a encriptar como último parámetro.

Elabora un documento y añade las capturas de pantalla de cada uno de los pasos que se indican a continuación:

1. Crea un fichero de texto con un mensaje.
2. Utiliza la orden correspondiente para encriptarlo con cifrado simétrico, sin utilizar parámetros.
3. Comprueba de qué tipo es el fichero que se ha generado (binario o de texto).
4. Utiliza el comando correspondiente para desencriptar el fichero. ¿El resultaodo se guarda en algún fichero?
5. Vuelve a realizar el paso 2, pero en este caso asegúrate de que el fichero encriptado se guarda en un fichero de texto.
6. Haz una captura del contenido de dicho fichero.
7. Sube a Aules el documento creado, así como los ficheros creados (el original y los encriptados). Indica en el documento la contrseña que has utilizado para que el profesor pueda desencriptarlos.