Cifrado de Archivos y Protección de Archivos

Realizado por: Jesús Losada Arauzo

Introducción

Objetivos:

-Entender qué es el cifrado y la importancia de la protección de los datos

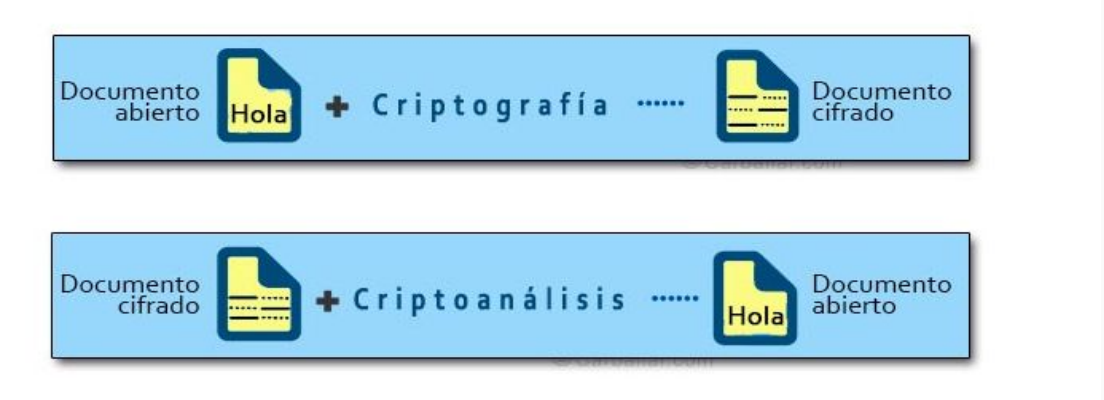
-Explorar herramientas de cifrado como GPG o Veracrypt (volúmenes)

-Aprender a cifrar y descifrar datos de manera segura

¿Qué es el cifrado?

El cifrado es básicamente una forma de transformar datos legibles en datos totalmente ilegibles.

Ejemplo:



Tipos de cifrado

Hay dos tipos de cifrado:

El cifrado simétrico: Este tipo de cifrado usa una única clave para cifrar los archivos. Algunos algoritmos son: DES, AES, IDEA...

El cifrado asimétrico: Este tipo de cifrado usa una clave pública para cifrar y otra clave privada para descifrar. Algunos algoritmos son: DSA o RSA

Curiosidad: La clave pública del cifrado asimétrico es posible compartirla pero la privada no se puede.

Cifrado simétrico

Cifrado asimétrico o de clave pública

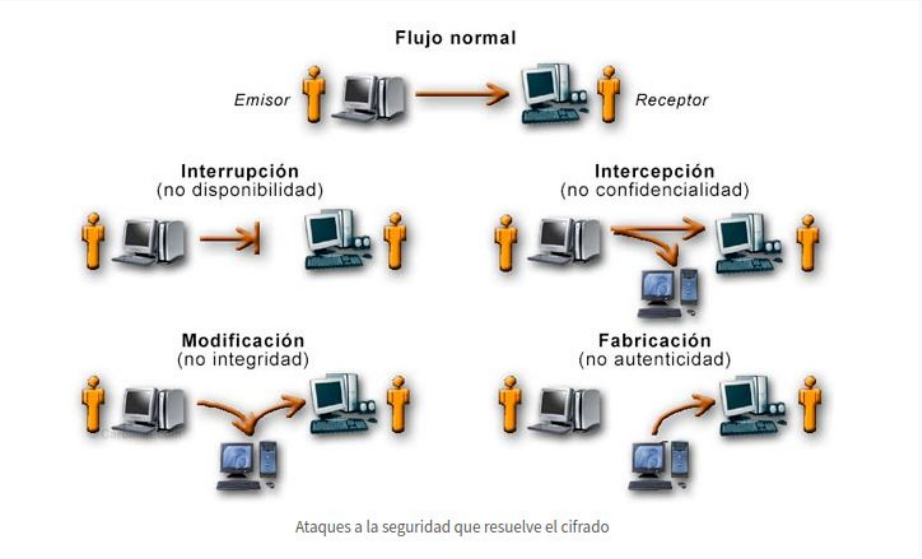
¿Por qué es importante el cifrado?

Gracias al cifrado internet puede asegurar:

- Confidencialidad (Privacidad de los datos)

- Integridad (NO se han manipulado los datos)

- Autenticación (Se verifica la identidad de las personas que envían y reciben los datos)



Ataques a la seguridad que resuelve el cifrado

Herramientas de cifrado

GNP (Asimétrico)

Veracrypt

Uso de GPG (Mini taller)

sudo apt install gnupg o instalar desde el sitio web de windows o mac.

gpg --gen-key (Para generar vuestras claves)

Si se lo vas a enviar a otra persona debes tener su clave pública (Más adelante conoceremos como hacerlo).

Para encriptar podemos usar este comando:

gpg --encrypt prueba.txt

#Encripta prueba.txt pero luego te pide tu usuario correo que hayas puesto o tu ID el nombre que te pide al principio.

gpg --encrypt --recipient "Juan Pérez" prueba.txt

#Lo mismo que el comando de arriba pero ya específicas para quién estás encriptando. Tanto ID como correo.

Desencriptar un archivo

Para desencriptar un archivo es tan fácil como usar el comando

gpg --decrypt archivo.txt.gpg

Y ya lo tendrias desencriptado.

En GPG además puedes usar desencriptado simétrico y hasta elegir el algoritmo que quieras:

gpg --symmetric --cipher-algo AES256 archivo.txt #Te pedirá una contraseña

Para desencriptar es más igual que antes.

Para pasarlo a un amigo tienes que enviarle la contraseña que pusiste al encriptarlo de forma simétrica.

Pasar Mensajes Encriptados

Tu amigo

gpg --gen-key #Si no tiene la clave generada

#Exportamos la clave de mi amigo y me la manda a mi

gpg --export --armor "Nombre o Correo de mi amigo" > clave_publica.asc

#Se usa armor para que la clave se exporte en un formato legible.

Tú

#Importa la clave que tu amigo te envío

gpg --import clave_publica.asc

#Te aseguras que la tienes

gpg --list-keys

#Encriptas el archivo para tu amigo y se lo mandas

gpg --encrypt --recipient "Nombre o Correo de mi amigo" archivo.txt

Uso de Veracrypt (Mini taller)

Instalación: En el buscador poneis veracrypt y el primer enlace en la parte de descargas.

Descarga Veracrypt

Una vez instalado vamos a crear un volumen.

Volúmenes > crear nuevo volumen > contenedor archivos cifrados > común/oculto > Seleccionamos donde queremos el volumen > Elige el algoritmo y el espacio del volumen >Establecer una contraseña > Formatear.

Una vez creado el volumen lo montamos en una de las ranuras disponibles en veracrypt.

Ahora ya podemos arrastrar archivos una vez abierto el volumen desde vera.

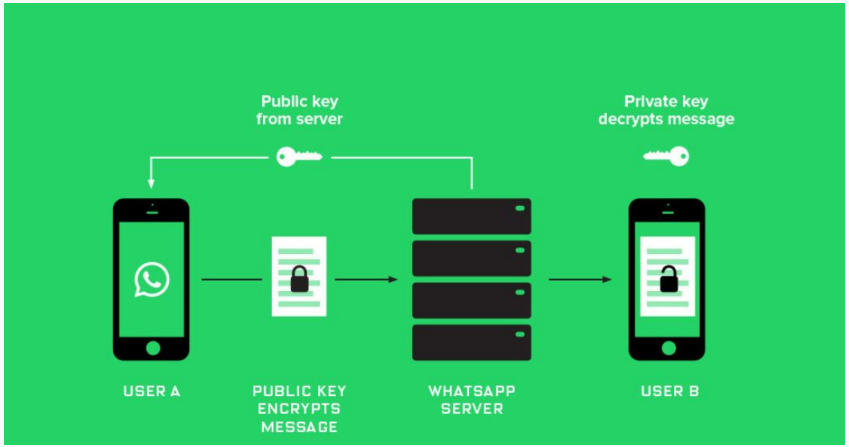
Una vez acabado es importante desmontar el volumen para que los archivos que hayas dejado se queden en oculto y no sean accesibles para nadie si no tienen la contraseña.

CURIOSIDAD

¿Alguna vez os han preguntado qué es el cifrado de extremo extremo y no sabías? Aquí os cuento.

Cuando se hacen cifrados de las comunicaciones se suele hacer entre la terminal del cliente y el servidor por ejemplo hay un protocolo famoso (https) que lo mantiene seguro.

Pero hay muchos servicios de internet que pone en contacto dos terminales de clientes (whatsapp) para estos casos no sirve el cifrado anterior porque deja expuesto la información del cliente, por lo que se hace un cifrado terminal a terminal o por el nombre que también se conoce como cifrado integral o cifrado de extremo a extremo.



El cifrado es necesario siempre que quieras transportar datos de forma segura.

¡GRACIAS!

Para más información:
https://carballar.com/que-es-el-cifrado-de-datos-y-para-que-sirve