

Escuela de Ingenierías

Informe de Laboratorio – Seguridad de la información (Practico)

[Taller #1]

Participantes	
---------------	--

Datos del Estudiante	
Nombre	



Escuela de Ingenierías
Medellín, [2024.Octubre.16]

INFORME DE LABORATORIO: CIFRADO CON KLEOPATRA

1. Introducción El cifrado de datos es una técnica fundamental en la seguridad de la información que permite proteger la confidencialidad de la información mediante la transformación de los datos en un formato ilegible para quienes no posean la clave adecuada. Kleopatra es una aplicación gratuita y de código abierto que permite gestionar claves y realizar cifrado de archivos y mensajes. En este laboratorio, exploraremos el uso de Kleopatra para cifrar y descifrar información, comprendiendo las diferencias entre el cifrado simétrico y asimétrico.

2. Objetivos

- Entender los conceptos básicos de cifrado de datos.
- Diferenciar entre cifrado simétrico y asimétrico.
- Aprender a utilizar Kleopatra para cifrar y descifrar archivos.
- Generar y gestionar claves públicas y privadas.
- Aplicar el cifrado en un escenario práctico.

3. Conceptos a Entender

3.1 Cifrado Simétrico El cifrado simétrico utiliza una única clave para cifrar y descifrar los datos. Este método es rápido y eficiente, pero presenta el problema de compartir la clave de forma segura. Algunos ejemplos de algoritmos simétricos son AES y DES.

3.2 Cifrado Asimétrico El cifrado asimétrico emplea un par de claves: una clave pública para cifrar y una clave privada para descifrar. Esto proporciona mayor seguridad en la transmisión de datos, pero es más lento que el cifrado simétrico. Algunos algoritmos asimétricos son RSA y ECC.

Punto 1: Instalación de Kleopatra

- Descarga e instala Gpg4win desde <https://www.gpg4win.org/>.
- Abre Kleopatra y familiarízate con la interfaz.

Punto 2: Generación de Claves

- En Kleopatra, selecciona "Archivo" > "Nuevo Certificado".
- Elige "Crear un par de claves personales".
- Introduce tu nombre y correo electrónico.
- Configura una contraseña segura para tu clave privada.
- Guarda y respalda tu clave privada.

Punto 3: Cifrado de un Archivo con Cifrado Asimétrico

- Crea un archivo de texto con información sensible.
- En Kleopatra, selecciona "Cifrar/Descifrar archivos".
- Elige la clave pública del destinatario para cifrar el archivo.
- Guarda el archivo cifrado con la extensión ".gpg".

Punto 4: Descifrado de un Archivo

- Envía el archivo cifrado a otro compañero que tenga tu clave pública.
- El destinatario usa su clave privada para descifrar el archivo en Kleopatra.
- Verifica que el archivo descifrado es idéntico al original.

Punto 5: Comparación entre Cifrado Simétrico y Asimétrico

- Cifra un archivo con cifrado simétrico (opción "Cifrado con contraseña").
 - Cifra otro archivo con cifrado asimétrico.
 - Compara los métodos en términos de seguridad y facilidad de uso.
-