

## TRABAJO FINAL, ENCRIPCIÓN TRADICIONAL

### ***Objetivo de aprendizaje***

Reforzar y profundizar los conocimientos adquiridos durante el curso en relación con los temas de cifrado simétrico y asimétrico. Durante la práctica, los estudiantes conocerán los diferentes bloques de cifrado que componen las soluciones de diferentes algoritmos cifradores comerciales, de igual modo adquirirán la capacidad de instalar y utilizar herramientas de protección y cifrado de información.

El desarrollo de esta práctica estará centralizado en el uso de mecanismos para cifrado tradicional.

*Se busca resolver los siguientes interrogantes:*

### ***Veracrypt***

1. ¿Qué algoritmos de cifrado usa el software para cifrado TrueCrypt utilizado en el laboratorio?
2. ¿En el procedimiento de creación del volumen el usuario puede seleccionar uno de tres algoritmos HASH, para que se usen tales algoritmos dentro del procedimiento? ¿Considera usted que es necesario el uso de tal mecanismo?
3. Haga pruebas reiniciando el sistema sin hacer el respectivo procedimiento para desmontar las unidades montadas en el proceso de cifrado. ¿Qué sucede con las unidades previamente montadas después del reinicio?, ¿Qué sucede cuando el sistema es apagado por un patrón externo anormal como una baja de luz o retirando el cable de alimentación de energía?
4. Se realizará el cifrado y montaje de volúmenes desde una unidad externa (Disco duro externo, Memoria USB), se creará un volumen normal de 300 MB y dentro del volumen un volumen oculto de 100 MB; para este paso del laboratorio se usarán capturas de pantalla que permitan evidenciar el proceso (Montar y desmontar las unidades, grabar archivos en ambos volúmenes y documentar el proceso.)

### ***GPA y Kleopatra***

Para la práctica de cifrado asimétrico, los estudiantes crearan un par de claves desde Kleopatra asociando sus datos personales y su dirección de correo electrónico institucional; al momento de crear la contraseña para el par de claves asegúrese de que la clave es 100% segura, puede usar una longitud de clave de 10 caracteres que combine mayúsculas y minúsculas, o también puede usar el sitio web: <https://www.lastpass.com/es/passwordgenerator> , para generarla. **Recuerde que debe tomar capturas y explicar las funcionalidades respectivas.**

1. Subir las claves generadas al servidor para que estas puedan ser buscadas de forma remota a través de GPA. Documentar el proceso y problemas encontrados.
2. Envíe un correo electrónico al Docente del curso [madnarvaez@umariana.edu.co](mailto:madnarvaez@umariana.edu.co) siguiendo los pasos de integración por Thunderbird u otro software.

Finalmente, en el documento deberá describir algunas conclusiones de las herramientas aplicadas.