LABORATORIO DE ENCRIPCION TRADICIONAL

Objetivo de aprendizaje

Reforzar y profundizar los conocimientos adquiridos durante el curso en relación a 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.

Planteamiento

Las aplicaciones que se utilizarán durante el desarrollo de la práctica serán

- Truecrypt for Windows ver 6.3A

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

Se aplicara los conceptos propios de la encripción tradicional, por lo cual lo primero que se realizará, será una breve explicación sobre cifradores, bloques de cifrado y el uso en algoritmos comerciales de cifrado como DES, 3DES, Serpent, Blowfish, etc. 1.

Se proporciona el software TrueCrypt for Windows versión 6.3A, aunque también se puede descargar las ultimas versiones del programa desde el website oficial de truecrypt **http://www.truecrypt.org/downloads.**

Se busca resolver los siguientes interrogantes:

1. ¿Qué algoritmos de cifrado usa el software para cifrado TrueCryp utilizado en el laboratorio?

2. ¿Para que se utiliza el montaje/desmontaje de unidades?

3. ¿Cuál es la limitante para la definición del tamaño del volumen en el que se almacenaran los datos a cifrar?

4. ¿En el procedimiento de creación del volumen el usuario puede seleccionar uno de tres algoritmos HASH, para que se usan tales algoritmos dentro del procedimiento? ¿Considera usted que es necesario el uso de tal mecanismo?

7. 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?, Que sucede cuando el sistema es apagado por un patrón externo anormal como una baja de luz o retirando el cable de alimentación de energía?.

8. Se realizara el cifrado y montaje de volúmenes desde una unidad externa (Disco duro externo, Memoria USB), se creara un volumen normal de 300 MB y dentro del volumen un volumen oculto de 100 MB; para este paso del laboratorio se usaran capturas de pantalla que permitan evidenciar el proceso (Montar y desmontar las unidades, grabar archivos en ambos volúmenes y documentar el proceso.)

Parte 2 – 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 12 caracteres que combine mayúsculas y minúsculas, o también puede usar el sitio web: https://www.lastpass.com/es/password-generator, para generarla.

Tomar capturas y explicar las funcionalidades respectivas.

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.

Envíe un correo electrónico al Docente del curso siguiendo los pasos de integración por Thunderbird.

9. ¿Qué conclusiones adicionales puede aportar respecto al laboratorio realizado.