UNIVERSIDAD TECNOLÓGICA DE PANAMÁ
FACULTAD DE INGENIERÍA DE SISTEMAS COMPUTACIONALES
DEPARTAMENTO DE PROGRAMACION DE COMPUTADORAS

TRABAJO GRUPAL N° 5

Facilitador(a): _____ Asignatura: _____
Estudiante: _____ Fecha: _____ Grupo: _____
_____, _____

A. TÍTULO DE LA EXPERIENCIA: *Técnicas de Cifrado*

B. TEMAS:

Concepto relacionado con los algoritmos simétricos y asimétricos.

C. OBJETIVO(S):

- *Comprender la importancia del uso de las diversas técnicas de cifrado.*
- *Analizar casos de estudio que permitan el reforzamiento de conceptos relacionados con cifrado.*

D. RECURSOS:

- *Dispositivo portátil o de escritorio con procesador de palabras.*
- *Plataforma Moodle.*

E. METODOLOGÍA:

El alumno realizará búsqueda de material y leerá el contenido del capítulo y entregará lo resuelto en la plataforma Moodle.

F. ENUNCIADO DE LA EXPERIENCIA O PROCEDIMIENTO:

Cifrar o encriptar datos significa alterarlos, generalmente mediante el uso de una clave, de modo que no sean legibles para quienes no posean dicha clave. Luego, a través del proceso de descifrado, aquellos que sí poseen la clave podrán utilizarla para obtener la información original.

Esta técnica protege la información sensible de una organización, ya que si los datos cifrados son interceptados, no podrán ser leídos.

Al hablar de esta área se debería hablar de criptologia que a su vez engloba las técnicas de cifrado (criptografía) y sus técnicas complementarias donde se incluye el **criptoanálisis** (*técnica que estudia los métodos para romper textos cifrados con objeto de recuperar la información original en ausencia de claves*).

Tipos de algoritmo de cifrado

- **Simétricos o de clave simétrica o privada**: son los algoritmos que usan una clave única tanto para cifrar como para descifrar.
- **Asimétricos o de clave asimétrica o pública**: son los algoritmos que utilizan una clave para cifrar y otra clave distinta para descifrar.

Los **hash** o **funciones de resumen** son algoritmos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo, por ejemplo) una salida alfanumérica de longitud normalmente fija que representa un

resumen de toda la información que se le ha dado (es decir, a partir de los datos de la entrada crea una cadena que *solo* puede volverse a crear con esos mismos datos).

En cada sentido del envío y recepción de información, se cifra el mensaje con la clave pública de la persona a la que se envía y esta lo descifra con su clave privada que solo él conoce, cada interlocutor tiene que tener la clave pública del otro.
Algunos **programas** o herramientas **de cifrado** simétrico son:

- **PGP** (Pretty Good Privacy) es el programa más popular de encriptación y creación de llaves públicas y privadas, su pega es que es un algoritmo propietario.
- **GPG** (GNU Privacy Guard) es una herramienta para el cifrado similar al PGP pero de software libre bajo licencia GPL, utiliza **algoritmos** no patentados como **ElGamal**, **CAST5**, **Triple DES** (**3DES**), **AES** y **Blowfish**, viene pre-instalada en distribuciones Linux, *algunas opciones del comando:
    - **gpg** --version muestra la versión y algoritmos soportados.
    - **gpg -c** archivo.txt **-c** encripta el archivo con cifrado simetrico, da archivo.gpg
    - **gpg -c -a** archivo.txt **-c -a** encripta en formato legible (ASCII), da archivo.asc
    - **gpg -d** archivo.asc **-d** desencripta el archivo.
    - **gpg** -c -a **--cipher-algo** AES192 archivo **--cipher-algo** determino que algoritmo usar.

Algunas opciones el comando GPG en criptografía asimétrica:

- **gpg** --gen-key genera un par de claves (privada y pública).
- **gpg** --list-keys lista las claves públicas que tenemos, propia y ajenas.
- **gpg** --import clave.asc importo la clave pública de un interlocutor.
- **gpg** --armor --output miclave_publica.asc --export ClaveID exporto mi clave pública a un fichero (armor es para que se vea en caracteres ASCII).
- **gpg** --armor --output claveprivada --export-secret-key ClaveID exporto mi clave privada a un fichero como backup.
- **gpg** --armor --recipient ClaveID_destinatario --encrypt fichero encripto un fichero con la clave pública del destinatario (para desencriptar se usa gpg -d fichero.gpg > fichero.xxx).

G. RESULTADOS:

1. Revise todas las veces que se utiliza criptografía en la película *El Código Da Vinci* (2006).
2. Investigue el cifrado del programa Skype.
3. Investigue el cifrado utilizado por los dispositivos móviles con Android.
4. Investigue cómo y dónde se guardan las claves de los usuarios en Linux.
5. Idear mecanismos para hacer llegar la clave simétrica a los participantes de una comunicación.
6. Un método sencillo de cambiar la clave simétrica sería avisarlo en el último mensaje intercambiado. ¿Te parece adecuado?
7. Para cifrar y descifrar no necesitamos privilegios especiales en Linux. ¿Por qué?
8. ¿Cómo haría para llegar al servidor, de manera segura, las claves públicas de los clientes?
9. Investigue cómo confirma un cliente que el servidor al que se conecta es el auténtico y no un impostor.
10. Envíe a un compañero un archivo ejecutable firmado. Él deberá comprobar la firma, extraer el fichero y ejecutarlo para confirmar que ha llegado bien.
11. ¿Por qué se firma solo el resumen del documento, y no el completo?

H. RÚBRICAS:

Desarrolle el punto **G. Resultados**, donde deberá responder a las preguntas señaladas.

I. CONSIDERACIONES FINALES:

Opinión del estudiante sobre el logro del objetivo y el desarrollo de la tarea relacionada con el capítulo.

J. REFERENCIAS BIBLIOGRÁFICAS:

- Material dado en clases.
- El algoritmo RSA. http://www.criptored.upm.es/crypt4you/temas/RSA/leccion0/leccion00.html
- Criptografía simétrica y asimétrica. https://infosegur.wordpress.com/unidad-4/criptografia-simetrica-y-asimetrica/
- Criptografía. http://www.matem.unam.mx/rajsbaum/cursos/web/presentacion_seguridad_1.pdf