Universidad Nacional ARTURO JAURETCHE

Ingeniería Informática Sistemas Operativos II

Protección y Seguridad

PRACTICA de SEGURIDAD

1) Utilice alguna clave criptográfica para el método DES para cifrar la palabra SECRETO escrita en ASCII. Verifique su descifrado. (Opcional)

2) En un sistema de Administración de Memoria Paginada por Demanda, ¿cuándo es necesario utilizar claves de protección para las Páginas/Bloques ?

3) Algunos sistemas reescriben las áreas que fueron ocupadas por archivos ya borrados. Comente qué problema solucionaría esta metodología.

4) Verifique para algún mensaje que el método RSA funciona con p = 7 q = 13 e = 5 y d = 29.

5) La lista de todas las passwords se mantiene dentro del sistema operativo. Luego, si un usuario administra en forma de lectura tal lista el sistema de protección de passwords se torna muy débil. Sugiera un esquema que impida este problema (Ayuda: Utilice una representación interna que difiera de la representación externa)

6) Realizar el encifrado de la palabra ABEJA por:
a) el método de sustitución con la palabra clave "SISTEMAS OPERATIVOS". Detalle los pasos que realiza.
b) el método de encifrado por sustitución para el entero N = 4. Detalle los pasos realizados.

7) Juan se quiere comunicar con María utilizando el método de encifrado RSA. Indique cuáles son las acciones que alcanzan para que **solamente** se pueda enviar el mensaje de Juan a María:

a) Juan genera su par de claves publica/privada
b) María genera su par de claves pública/privada
c) María envía a Juan su clave pública
d) María envía a Juan su clave privada
e) Juan envía a María su clave pública
f) Juan envía a María su clave privada

8**)** Suponga una instalación en la que existen 2000 usuarios que operan sobre 100 recursos distintos. Solamente 10 usuarios son los dueños de los recursos en tanto que el resto de usuarios puede acceder a distintos recursos (aunque no a todos ellos) en diversas modalidades.
a) Qué esquema de protección implementaría?, Justifique.
b) Suponga que el 80 % de los recursos son accedidos por todos los usuarios en la misma modalidad (lectura, grabación, etc.) alteraría esta circunstancia la implementación por usted elegida en el punto a) ? De qué forma?, Justifique.
c) En el supuesto del punto b) existe una implementación más eficiente?

9) Investigue y describa alguna de las funciones de encriptado por hash. Po4r ejemo SHA-1. Realice un ejemplo.