Facultad: Ingeniería
Escuela: Electrónica
Asignatura: Seguridad en redes

Tema: Cifrados simétricos y asimétricos.

Contenidos

- Funcionamiento del Algoritmo DES
- Operaciones de cifrado sobre archivos
- Funcionamiento del algoritmo RSA
- Funcionamiento del algoritmo RABIN

Objetivos Específicos

- El estudiante deberá ser capaz de describir los procesos que se ejecutan en el algoritmo de cifrado simétrico DES.
- Observar el comportamiento del algoritmo DES sobre archivos de texto
- Que el estudiante compruebe, de manera experimental, el comportamiento del algoritmo DES cuando se utilizan las claves débiles.
- Que el estudiante compruebe, de manera experimental, el comportamiento del algoritmo DES cuando se utilizan las claves semi débiles.
- El estudiante deberá ser capaz de describir los procesos que se ejecutan en cada uno de los algoritmos de cifrado asimétrico tratados en la presenta práctica de laboratorio: RSA y Rabin.

Materiales y Equipo

- PC con MV Windows XP.
- Software safeDES instalado.
- Software simulador de criptografía instalado.

Procedimiento

Inicie la máquina virtual de Windows XP y realice lo siguiente:

Parte I. Cifrado Simétrico.

Comprobación del Funcionamiento del Algoritmo DES con entradas desde teclado

1. Ejecute el programa *safeDES*. Se nos desplegará la pantalla principal de la aplicación que se observa en la figura 1.

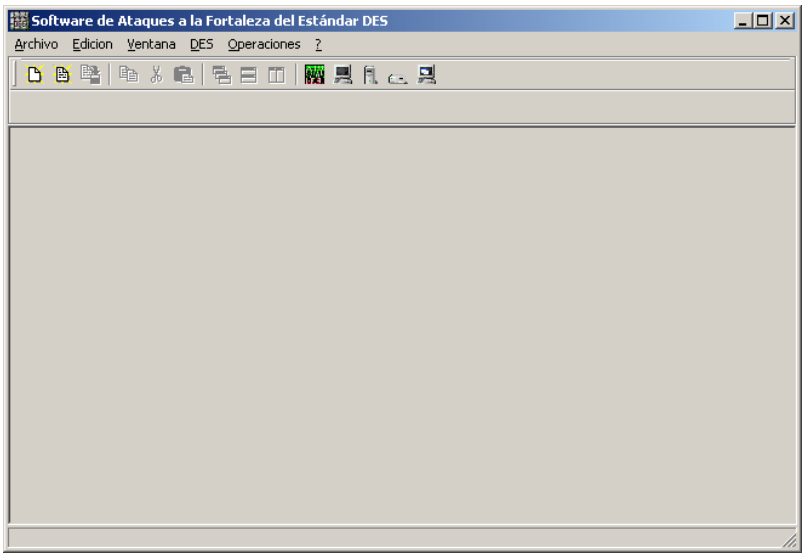

Figura 1: Ventana principal de aplicación safeDES.

2. Hacer clic en el botón *DES* y seleccione la opción *Cifrar/Descifrar*. Se nos despliega la ventana titulada DES Cifrar/Descifrar (Modo E.C.B.) que se observa en la figura 2.

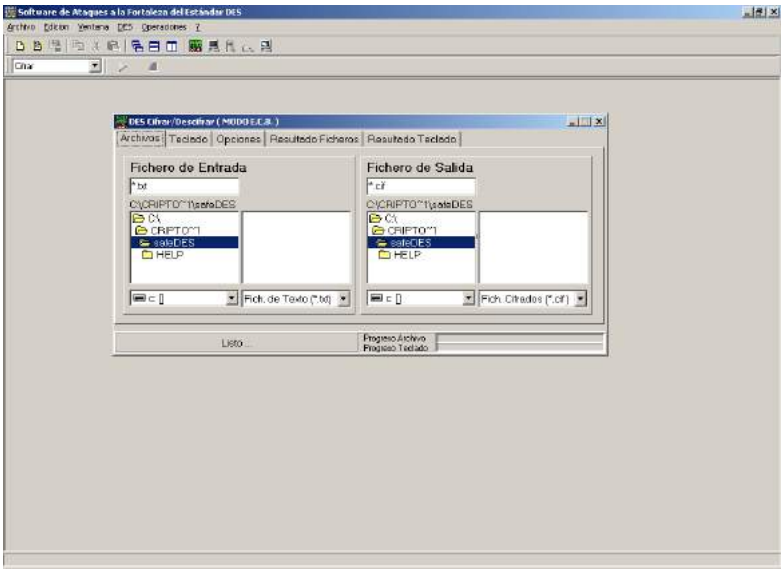

Figura 2: Área de trabajo de aplicación safeDES.

3. Hacer clic en la pestaña Teclado.

4. En el área de "Entrada de Texto en Modo" seleccionar la opción Hexadecimal.

5. En la caja de texto digitar el siguiente mensaje en hexadecimal:

MHEX = 2525252525252525

6. Luego, hacer clic en la pestaña Opciones.

7. En el área de "Clave" seleccionar la opción Hexadecimal. En la caja de texto, digitar la clave en hexadecimal: ***KHEX = 0E329232EA6D0D73***

8. En el área "Procesar" seleccionar la opción Teclado.

9. Luego, en la barra de herramientas del menú desplegable, seleccionar la opción Cifrar y hacer clic en el botón Comenzar. Con lo que el proceso de cifrado del mensaje se ejecutará.

10. Para observar el resultado de la operación, hacer clic en la pestaña Resultado Teclado. Anote el resultado en formato hexadecimal:_____

11. Realice el procedimiento necesario para descifrar el mensaje obtenido en el numeral anterior ¿Corresponde el valor obtenido al mensaje original? Justifique su procedimiento para descifrar :_____

12. Realizar el procedimiento de cifrado ahora con los siguientes conjuntos de mensajes y claves en formato hexadecimal. Anotar el valor correspondiente al mensaje cifrado en el espacio destinado.
    a. *MHEX = 7003000E95ACBDEE* *KHEX = 0123456789ABCDEF*
       CHEX = _____
    b. *MHEX = 56003000E000F08B* *KHEX = 45BF3908AC3*
       CHEX = _____

13. ¿Es posible realizar el literal "b" del numeral anterior?
    Explique:_____

14. Realizar el procedimiento de cifrado ahora con los siguientes conjuntos de mensajes y claves en formato ASCII. Anotar el valor correspondiente al mensaje cifrado en el espacio destinado.
    a. *MASCII = TELECOMUNICACIONES* *KASCII = CLAVEDES*
       CHEX = _____
    b. *MASCII = INFORMATICA* *KASCII = CLAVE*
       CHEX = _____

15. ¿Es posible realizar el literal "b" del numeral anterior?
    Explique:_____

16. Si se cifra el siguiente mensaje en ASCII MASCII = "*Seguridad en Redes con la clave en ASCII"* y clave *KASCII = 77777777*. El mensaje cifrado es: *CHEX =* _____

17. Si se repite el procedimiento del numeral anterior, pero ahora con la clave *KASCII = 66666666.* ¿Cuál es el mensaje cifrado que se obtiene? *CHEX =* _____.
    ¿Cuál es la razón del comportamiento que ha observado, son iguales o no el texto cifrado?
    _____

18. Utilizando la clave *KASCII = CLAVEDES*, cifrar el mensaje de 8 caracteres MASCII = *CIFRADOR*. Observe el resultado obtenido y cópielo en un archivo de texto sobre el escritorio de la PC. Repetir la operación de cifrado pero ahora con el mensaje de 12 caracteres *MASCII = CIFRADOR DES.* Este último resultado también cópielo en el archivo de texto. Compare ambos resultados y anote sus conclusiones a continuación:
    _____
    _____

Operaciones de cifrado sobre archivos de texto.

1. Cree un archivo ***sucarnet.txt*** en la dirección **C:\SER**
2. Ingrese al archivo creado y Escriba su nombre completo y carnet, guarde y salga del archivo.
3. En el programa SafeDES hacer clic en el botón *DES>Cifrar/Descifrar* y hacer clic en la pestaña Archivos.

4. Bajo el área "Fichero de Entrada" ir a la ruta **C:\SER** y seleccionar como tipo de archivo *Fich. Texto (*.txt)*

5. Seleccionar el archivo creado *sucarnet.txt*.

6. En la sección "Fichero de Salida" ir a la ruta **C:\SER** y seleccionar como tipo de archivo *Fich. Cifrados (*.cif)* y nombrar al archivo ***sucarnet.cif***.

Figura 3: Proceso de cifrado de archivo.

7. Hacer clic en la pestaña Opciones. En la sección "Procesar:" y "Mostrar Resultados:" seleccionar la opción *Archivos*. En el campo ***Clave*** ingrese una clave de su selección de 8 caracteres en modo ASCII.

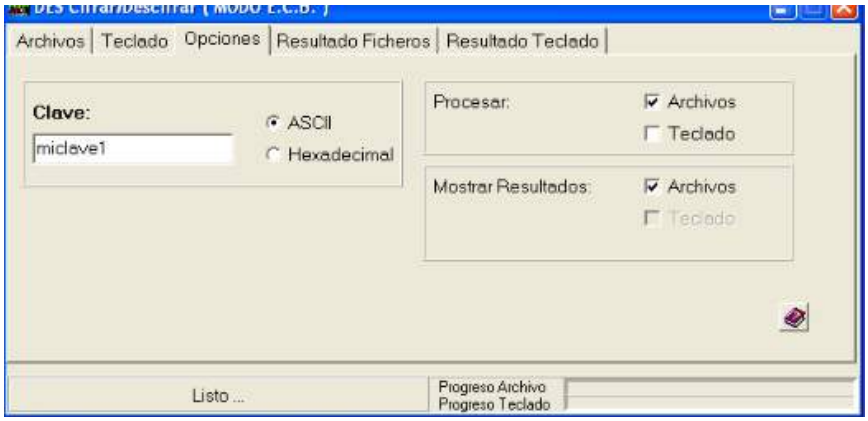

Figura 4: Proceso de cifrado de archivo, clase y tipo de entrada.

8. Asegúrese que la operación sea *Cifrar*, luego clic en el botón comenzar.

9. Observe el archivo cifrado que se ha generado en la ruta **C:\SER**. Abra el *archivo.cif* con la aplicación bloc de notas.

10. Borre el archivo original ***sucarnet.txt***.

11. Analice y efectué la forma de descifrar el archivo ***sucarnet.cif*** con el programa SafeDES.

Operaciones de cifrado con claves débiles y semidébiles del algoritmo DES

NOTA: En este apartado se debe hacer uso del portapapeles y usar la entrada de texto en formato hexadecimal para asegurar un correcto funcionamiento.

1. Cifrar el mensaje M = *"Ya casi termina la primera parte de la práctica con todas las claves débiles de DES que se indican a continuación"*. A continuación comprobar que se cumple la siguiente expresión: Ek[Ek(M)] = M

K1 HEX = 0101010101010101
K2 HEX = E0E0E0E0F1F1F1F1
K3 HEX = 1F1F1F1F0E0E0E0E

2. Cifrar el mensaje M = *"Hoy si ya terminó la primera parte de la práctica con todos los pares de claves semidébiles de DES que se indican a continuación"*. Y comprobar que se cumple la siguiente expresión: Ek1[Ek2(M)] = M

K1 HEX = 01FE01FE01FE01FE	K2 HEX = FE01FE01FE01FE01
K1 HEX = 1FE01FE00EF10EF1	K2 HEX = E01FE01FF10EF10E

Parte II. Cifrado Asimétrico.

Funcionamiento del algoritmo de cifrado asimétrico RSA

1. Ejecute la aplicación *Laboratorio RVC*. Con lo cual iniciará la pantalla que se observa en la figura 5.

Figura 5: Menú Principal del Simulador del Laboratorio de Criptografía.

2. En el menú, seleccionar la opción **RSA → Paso a Paso.** Con ello, se nos despliega la pantalla que aparece en la figura 6, La cual será nuestra área de trabajo para observar el comportamiento del algoritmo RSA.

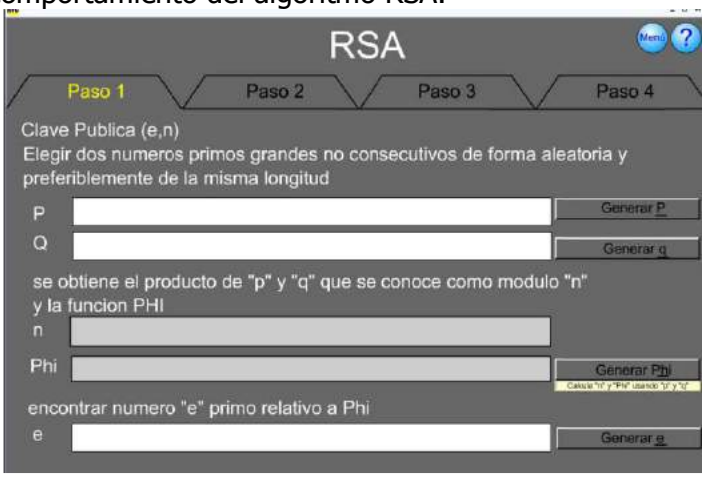

Figura 6: Pantalla Paso a Paso del Algoritmo RSA.

3. En la pestaña **Paso 1**, introducir dos números primos grandes no consecutivos y que tengan la misma longitud. Ingresar dichos valores en las casillas **P** y **Q** correspondientes (no utilice los botones generar para estos dos datos, ya que los generados son demasiado cortos). Puede utilizar los siguientes números primos:
   P = 99017 Q = 99991

4. Obtener los valores correspondientes a **n, Phi** y **e** con los botones ***generar Phi*** y ***generar e***. Anotar dichos valores a continuación:
   n = _____ Phi = _____ e = _____

   La clave pública será la combinación de **e** y **n** "CPrivada(e,n)"

5. Hacer clic en la pestaña **Paso 2** obtener el valor de **d.** Y anotarlo a continuación:
   d = _____

   La clave privada será la combinación de **d** y **n** "CPublica(d,n)"

6. Hacer clic en la pestaña **Paso 3**, y digitamos el mensaje a cifrar en el área dispuesta para ello. El mensaje a ingresar será la palabra **"hola"**. Presione el botón convertir.

7. Presione el botón cifrar y obtenga el mensaje cifrado C:

   C=_____

8. Hacer clic en la pestaña del **Paso 4**.

9. Hacer clic en el botón de **Descifrar** y anotar el valor descifrado a continuación: _____

10. Convertir a texto el mensaje obtenido.

Funcionamiento del algoritmo de cifrado asimétrico Rabin.

1. En el menú de la figura 3, seleccionar la opción **Rabin → Paso a Paso** que se encuentra bajo el título "Algoritmos Asimétricos".

2. Con ello, se nos despliega la pantalla que aparece en la figura 5. La cual será nuestra área de trabajo para observar el comportamiento del algoritmo Rabin.

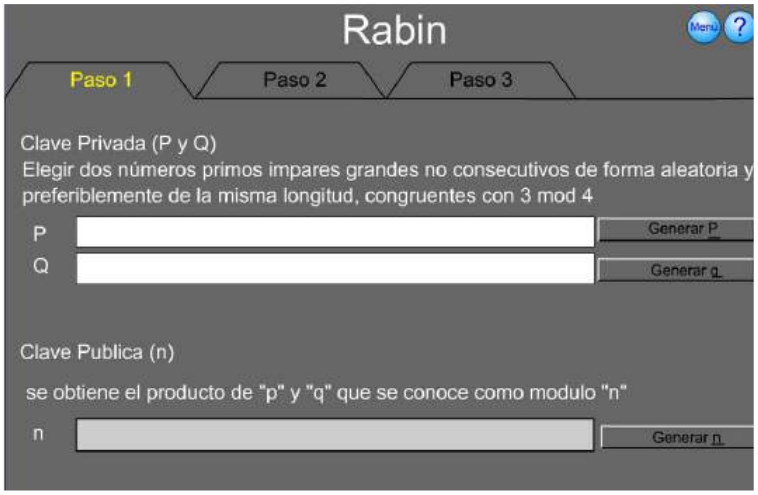

Figura 7: Pantalla Paso a Paso del Algoritmo Rabin.

3. Introducir los valores de **P=35407** y **Q=52363** en las casillas correspondientes de la ventana del **Paso 1.**
4. Obtener el valor de la clave pública ***(n)*** y anotarlo a continuación:
   n = _____
5. Hacer clic en la pestaña del **Paso 2**.
6. Escribir el mensaje **"hola"** y hacer clic en el botón **Convertir**.
7. Clic en el botón **Cifrar**. Anotar el valor del cifrado a continuación:
   C = _____
8. Hacer clic en la pestaña del **Paso 3**.
9. Hacer clic en el botón **Descifrar** y anotar los resultados correspondientes a continuación:
   M1= _____ _____
   M2= _____ _____
   M3= _____ _____
   M4= _____ _____

Investigación

- ¿A expensas de qué incrementa Triple DES la seguridad de DES?
- ¿Cuál es la principal debilidad de DES?
- Explique cuales de los servicios de seguridad de la información son protegidos con el uso de la criptografía.
- ¿Cuál es la razón por la que los valores de P y Q que se utilizan en los algoritmos RSA y Rabin deben ser primos?
- ¿Qué es lo que ocurre si se ocupan números de longitudes diferentes para los valores de P y Q?
- ¿Cuáles son las diferencias entre el algoritmo de RABIN con el RSA?
- Presentar un cuadro comparativo en el cual se reflejen las velocidades de los algoritmos de cifrado simétrico y asimétrico más utilizados.
- ¿Qué características deben poseer los valores de P y Q en el algoritmo Rabin?

Bibliografía

- Técnicas Criptográficas de Protección de Datos, A. Fuster, D. de La Guía, L. Hernández, F. Montoya y J. Muñoz, Ed. Ra-Ma, España, 2000.
- Diseño e Implementación de Prototipo de Laboratorio de Criptografía, VíctorEscobar, Rafael Gallardo, Carlos Zelaya, Tesis Universidad Don Boso, 2005.

Hoja de cotejo: 3

Guía 2: Cifrados Simétrico y Asimétricos

Alumno: Máquina No:

Docente: GL: Fecha:

EVALUACION					
	%	**1-4**	**5-7**	**8-10**	**Nota**
CONOCIMIENTO	25	Demostró poco conocimiento sobre el tema de la práctica.	Demostró conocimiento medio sobre el tema de la práctica.	Demostró buen conocimiento sobre el tema de la práctica.	
APLICACIÓN DEL CONOCIMIENTO	70	Cifra y descifra contenidos de entrada de teclado, utilizando diferentes claves	Cifra y descifra contenidos de entrada de teclado, utilizando diferentes claves. Cifra y descifra archivos de texto con diferentes claves	Cifra y descifra contenidos de entrada de teclado, utilizando diferentes claves. Cifra y descifra archivos de texto con diferentes claves Comprueba las expresiones Ek[Ek(M)] =M y Ek1[Ek2(M)] = M	
ACTITUD	2.5	Es un observador pasivo.	Participa ocasionalmente o lo hace constantemente pero sin coordinarse con su compañero.	Participa propositiva e integralmente en toda la práctica.	
	2.5	Es ordenado pero no hace un uso adecuado de los recursos.	Hace un uso adecuado de recursos respetando las pautas de seguridad, pero es desordenado.	Hace un manejo responsable y adecuado de los recursos conforme a pautas de seguridad e higiene.	
TOTAL	100				