SEGURIDAD INFORMÁTICA

3º Curso – GRADO DE INGENIERÍA EN INFORMÁTICA

(2020/2021)

Práctica 3b
CRIPTOLOGÍA MODERNA

CRIPTOLOGÍA MODERNA

Es fundamental comprobar y en su caso, corregir todo lo incluido en esta práctica. Habrá alguna de las aplicaciones que no funcione correctamente y se debe determinar las causas (32/64 bits...)

1. Relación de Software disponible

CML – Cripto MiniLab: Software para prácticas de criptografía clásica (incluye criptoanálisis) y sistemas de clave pública RSA, Mochilas y ElGamal. Contiene utilidades para cálculos de primalidad y características del lenguaje.

Archivo: *criptominilab*

Software para Generación de Claves, Cifra y Firma RSA, ElGamal y DSS: Software para prácticas de cifrado exponencial de números decimales, valores hexadecimales y texto ASCII, realizado con librerías propias y eficiente para operaciones de hasta centenas de bits.

Archivo: *ExpoCrip*

Software para la Generación de Claves RSA, Cifra, Firma y Ataques: Software desarrollado en Java y JavaFX que implementa toda la lógica de la aplicación gracias al uso de la clase BigInteger. El software incluye manual de usuario y banco de pruebas, accesibles además desde la misma aplicación.

Archivo: genRSA

legionRSA: Software de laboratorio para la realización de ataques a RSA basados en la paradoja del cumpleaños, tanto en modo local como en red. Permite comprobar la linealidad de este ataque, a diferencia de otros ataques como los de factorización entera, y además verificar es posible realizar un ataque distribuido en red y comprobar el principio de divide y venceras.

Archivo: *LegionRSA*

Mochilas de Merkle-Hellman: Software para prácticas de sistemas de cifra con mochilas de Merkle-Hellman realizado en Delphi. Se ha incluido una librería para trabajar con números grandes: decenas o centenas de dígitos. Permite el diseño de mochilas del tamaño y datos que desee el usuario, mochilas con tamaño recomendable M-H y mochilas proporcionales. Cifrado, descifrado y criptoanálisis de Shamir y Zippel.

Archivo: *mochilas*

RingRSA: Software con carácter educativo para laboratorio de criptografía en la realización de prácticas de ataques a RSA mediante el cifrado cíclico.

Archivo: RingRSA_VersionBeta2016

Software de Ataque a la Fortaleza del Estándar DES: Software de cifrado, descifrado y ataques por fuerza bruta de forma similar a los desarrollados por RSA Challengue al algoritmo Data Encryption Standard DES.

Archivo: safeDES

2. Ejercicios prácticos

Los ejercicios versarán sobre los siguientes tipos de criptosistemas:.

- ✔ Criptosistemas modernos:
  - ◆ Cifradores de clave secreta:
    - ◆ Cifrador DES.
  - ◆ Cifradores de clave pública:
    - ◆ Cifrador de Mochila de Merkle-Hellman.
    - ◆ Cifrador RSA.
    - ◆ Cifrador ElGamal.

✔ Criptosistemas modernos

- ◆ ***Cifradores de clave secreta***

Este tipo de cifradores utiliza una única clave que debe guardarse en secreto ya que en ella reside la seguridad de los mismos. Se les denomina también simétricos puesto que usan la misma clave para cifrar y descifrar. El DES, acrónimo de Data Encryption Standard es uno de los algoritmos de cifra con clave secreta más utilizados en los años 70 y 80 y sigue aún vigente en innumerables equipos de transmisión de datos.

- ▪ **Cifrador DES.**

PRÁCTICA:

Apartado 1: Archivos de texto

a) Intente descifrar el fichero PROMETEICO.CIF llamando al fichero de salida PROMETEICO.DCF si nos han dicho que la clave puede ser cualquiera de las siguientes: ¿Franki?; Frankens; Prometeo; prometeo; 1234Mary; MaryShel; marymary. Se sabe que la cifra se ha realizado con el modo ECB.
b) Observe el fichero PROMETEICO.DCF en hexadecimal y su representación en forma de texto. Editelo luego con el Bloc de Notas.
c) Cifre el fichero PROMETEO.TXT con la clase K=MShelley y anote los 8 primeros caracteres en hexadecimal del criptograma.

Apartado 2: Archivos con formato

a) Cree un documento cualquiera con Word, Wordperfect u otro programa de texto y cífrelo usando como clave K=MiClavel. El fichero cifrado se llamará igual que el original pero con extensión CIF.
b) Cifre ahora el mismo documento pero con la clave K=MiClave2. Llame al fichero cifrado con distinto nombre que el anterior pero con extensión CIF.
c) Descifre ahora los criptogramas obtenidos llamando a los ficheros con su respectivo nombre y la extensión DCF.
d) Intente abrir los archivos cifrados anteriormente con el programa o aplicación que generó el fichero.
e) Compruebe que los ficheros descifrados son idénticos a los ficheros.

Apartado 3: Archivos ejecutables

a) Cifre el archivo CALC.EXE que encontrará en la carpeta C:\WINDOWS\SYSTEM32 con la clave K=calcular. Llame al fichero de salida CALCUCIF.EXE.
b) Intente ejecutar el archivo CALCUCIF.EXE.
c) Descifre el archivo CALCUCIF.EXE llamándolo CALCUDES.EXE y

compruebe que el archivo descifrado se ejecuta perfectamente.

INFORME:

1. ¿Con qué clave ha podido descifrar el fichero del apartado 1?
2. ¿Se corresponden los 8 primeros bytes en hexadecimal del texto recuperado en el apartado 1.c con los caracteres ASCII del texto en claro.
3. ¿Le llama algo la atención los valores en hexadecimal del comienzo y del final de los ficheros con formato que se han cifrados con DES?
4. Comente lo sucedido en el apartado 3. ¿Son exactamente iguales los ficheros CALC.EXE y CALCUDES.EXE.

◆ ***Cifradores de clave pública***

Este tipo de cifradores usan un par de claves, inversas entre sí dentro de un cuerpo, de forma que una de ellas se denomina clave pública y la otra clave privada. En la operación de cifra se usan funciones matemáticas unidireccionales como, por ejemplo, el problema de la mochila, el problema de la factorización o el problema del logaritmo discreto.

- **Cifrador de Mochila de Merkle-Hellman.**

PRÁCTICA:

[*u* hace referencia al módulo y *w* al multiplicador]

Apartado 1

a) Cifre el mensaje M = "Esta es la mochila de <Nombre_Alumno/s>", usando la mochila simple [1,2,4,8] con u=16 y w=7.
b) Descifre el criptograma anterior.
c) Con la mochila simple [1,2.4,8,16,32,64,128], u=256 y w=13, repita la cifra del punto a).
d) Descifre el criptograma anterior.
e) Cifre el mensaje M="Errar es humano, usando la mochila de <Nombre_Alumno/s>" con valores de Merkle-Hellman proporcionales de tamaño n=15, garantizando el criptoanálisis. Anote la mochila fácil, la mochila difícil y sus parámetros.
f) Descifre y criptoanalice el criptograma anterior.

Apartado 2

a) Cifre el fichero ROSITA1.TXT usando la mochila simple [2,3,7,13,26,53] con u=110 y w=21. El fichero de salida se llamará ROSITA1.CIF.
b) Descifre el fichero ROSITA1.CIF, guardándolo como ROSITA1.DCF.
c) Intente criptoanalizar el fichero ROSITA1.CIF.
d) Cifre el fichero ROSITA2.TXT usando una mochila de Merkle-Hellman con valores proporcionales a n=20. Anote la mochila fácil, la mochila difícil y sus parámetros propios. Asegúrese de tener activada la posibilidad de criptoanálisis. El fichero de salida llamará ROSITA2.CIF.
e) Descifrar el fichero ROSITA2.CIF, guardándolo como ROSITA2.DCF.
f) Vuelva a cifrar el fichero ROSITA2.TXT usando ahora una mochila de Merkle-Hellman no proporcional con n=20. Descifre el criptograma y compare el resultado con el fichero recuperado anteriormente ROSITA2.DCF.
g) Descifre el fichero MOCHILA.CIF (o MOCHILA3.CML si se usa CriptoMiniLab), si se sabe que ha sido cifrado con alguna de estas tres mochilas de Merkle-Hellman: [23,47,111,239,495] u=4005, w=3994;

[29,61,125,253,509] u=3748, w=3743; [26,64,122,256,506] u=4015, w=3198. ¿De qué archivo se trata?

INFORME:

1. Comente los resultados obtenidos en el apartado 1. ¿Es una buena opción elegir mochilas de tamaño 8 o de tamaño 4?
2. Compruebe teóricamente los dos primeros valores del criptograma obtenido en el apartado 2a.
3. ¿Qué puede decir de los valores de las mochilas fácil y difícil generadas en los apartados 2d y 2f?
4. ¿Qué sucede si en el apartado 2g modifica algún valor de la mochila de cifra encontrada?.

- **Cifrador RSA**

PRÁCTICA:

Apartado 1

a) Con p=11, q=13 y e=1 cifre el mensaje M=OLA.
b) Con p=13, q=17 y e=5 cifre el mensaje M=3C2B1A.
c) Descifre el criptograma del punto anterior.
d) Con p=41, q=37 y e=13, cifre el mensaje M=Pienso, luego existo.
e) Descifre el criptograma del punto anterior.
f) Repita la cifra del punto d) usando ahora los primos p=89 y q=97.

Apartado 2

a) Cifre con los valores p=17, q=23 y e=29 el fichero ESPIRIT.TXT. El fichero de salida se llamará ESPIRIT.CIF..
b) Descifre el fichero ESPIRIT.CIF guardándolo como ESPIRIT.DCF..

INFORME:

1. Explique y justifique qué ha sucedido en la cifra del punto 1a.
2. Compruebe los valores de cifra y descifrado del mensaje del apartado 1b.
3. ¿Podría cifrar cualquier mensaje en ANSI con el grupo del apartado 1a?
4. Compruebe la cifra y el descifrado de los dos primeros bytes del fichero ESPIRIT.TXT del apartado 2a.
5. Si tuviera que elegir un sistema de cifra, ¿elegiría este sistema RSA en el que se cifra el mensaje por bytes? ¿Por qué?

- **Cifrador ElGamal**

PRÁCTICA:

Apartado 1

a) Con p=71, alfa=7, v=19 y b=23 cifre el mensaje M=ZYX.
b) Descifre el criptograma del punto anterior.
c) Si ahora alfa=5, repita la cifra del punto 1a para b=4 y b=9.

Apartado 2

a) Con p=1997, a =7, v=25 y b=32 cifre el fichero AGUITA.TXT. El fichero de salida se llamará AGUITA.CIF.
b) Descifre el fichero AGUITA.CIF, guardándolo como AGUITA.DCF.

INFORME:

1. Compruebe la cifra y el descifrado del mensaje del apartado 1a.
2. ¿Podría cifrar con los parámetros del apartado 1a el mensaje M=Hola?
3. ¿Qué puede decir de los criptogramas encontrados en el apartado 1c?

4. Compruebe la cifra y el descifrado de los dos primeros bytes del fichero AGUITA.TXT del apartado 2a.
5. En general, ¿puede usar cualquier valor del CRR(p) como generador a?