SEGURIDAD INFORMÁTICA

3º Curso – GRADO DE INGENIERÍA EN INFORMÁTICA

(2020/2021)

Práctica 3
CRIPTOLOGÍA BÁSICA

CRIPTOLOGÍA BÁSICA

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

Cripto Clásicos: Software para prácticas de criptografía clásica, desarrollado en Java, no requiere instalación sino solamente descomprimir el archivo zip en la carpeta que se desee. Cuenta con las siguiente utilidades: Cifrado, descifrado y criptoanálisis de sistemas de cifra por sustitución y permutación. Además cuenta con herramientas comunes de aritmética modular.

Archivo: *Criptoclasicos*
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*
ExpoCrip: Software para prácticas de cifrado exponencial de números decimales, hexadecimales y texto ASCII. Incluye los sistemas RSA y ElGamal y su variante DSS. Además tiene un menú de herramientas matemáticas con números primos.

Archivo: ExpoCrip
Libro Electrónico de Criptografía Clásica: Software hecho en ToolBook para el aprendizaje de los sistemas, máquinas, artilugios y algoritmos de cifra clásica. Además de las páginas del libro con fotografías y animaciones, incluye un apartado con opciones de cifrado y descifrado de los sistemas más comunes: César, Desplazamiento, Afin, Vigenère, Beaufort, Clave Continua, Beale, Homofonías de Orden Superior, Vernam, Playfair, Hill Dinámico y Transposiciones.

Archivo: *setuplecc*

2. Ejercicios prácticos

Los ejercicios versarán sobre los siguientes tipos de criptosistemas:

- ✔ Fundamentos teóricos:
  - Teoría de la información y matemática discreta.
- ✔ Criptosistemas clásicos:
  - Cifradores monoalfabéticos por sustitución:
    - Cifradores por Desplazamiento Puro.
    - Cifradores por Decimación Pura.
  - Cifradores polialfabéticos por sustitución:
    - Cifradors Periódicos:
      - Cifrado de Vigenère.
      - Cifrado de Beaufort.
      - Cifrado Variante de Beaufort.
    - Cifradores no Periódicos:
      - Cifrado de Clave Continua.
      - Cifrado de Vernam.
  - Cifradores por Transposición:

- Cifradores por Transposición de Filas.
- Cifradores por Transposición de Columnas.

✔ Fundamentos teóricos:

- ***Teoría de la información y matemática discreta.***

Alguna de las operaciones más comunes en la aritmética modular de los sistemas criptográficos son los cálculos de primalidad, exponenciación modular, obtención del Indicador de Euler y cálculo de inversos dentro de un cuerpo.

PRÁCTICA:

Apartado 1: Primalidad

a) Confeccione una tabla con los 100 primeros números primos.
b) Compruebe si los siguientes números son primos.
97; 981; 1283; 14371; 27773; 27777; 30011.
c) Encuentre los primos que hay en los siguientes intervalos: [500, 550], [5000, 5050] y [50000, 50050].

Apartado 2: Modularidad

a) Encuentre los siguientes restos:
487 mod 13; 12532 mod 493; 8440 mod 97; 955 mod 15; 5202 mod 867; 31551 mod 123; 2001 mod 77; 1997 mod 19.

Apartado 3: Máximo Común Divisor

a) Encuentre el Máximo Común Divisor (mcd) entre:
mcd (35,16); mcd (2488,390); mcd (186,21); mcd (448,196); mcd (599,131); mcd (1573,913); mcd (1350,1005); mcd (2488,392)

Apartado 4: Conjunto Reducido de Restos

a) Encuentre el Conjunto Reducido de Restos CRR, de los cuerpos que se indican:
CRR (4); CRR(6); CRR(7); CRR(9); CRR(74); CRR(100); CRR(1001); CRR(1213).

Apartado 5: Indicador de Euler

a) Encuentre los siguientes Indicadores de Euler:
Φ(1); Φ(2); Φ(4); Φ(6); Φ(7); Φ(9); Φ(74); Φ(100); Φ(1001); Φ(1213)

Apartado 6: Inversos

a) Encuentre los siguientes inversos:
inv (3,7); inv (7,9); inv (17, 40); inv (28,39); inv (85,166); inv (150,2999); inv (1234,4321); inv (3311,1133)

Apartado 7: Exponenciación dentro de un cuerpo

a) Usando la calculadora de Windows encuentre los siguientes valores:
59 mod 13; 210 mod 31; 198 mod 77; 39737 mod 141; 2011 mod 51

INFORME:

1. ¿Qué puede concluir de los valores encontrados en el apartado 1.c?
2. Calcule y compruebe los valores de mcd (186,21) y mcd (2488,392).
3. Calcule y compruebe los valores de Φ(9), Φ(74) y Φ(100).
4. Calcule y compruebe los valores inv (7,9), inv (17,40) e inv (85,166).
5. Calcule y compruebe mediante reducción del exponente 198 mod 77.
6. Mediante la reducción del exponente calcule los valores 39737 mod 141 y 2011 mod 51. ¿Qué puede concluir de estos resultados?.

✔ Criptosistemas clásicos

◆ *Cifradores monoalfabéticos por sustitución*

Este tipo de cifradores usan un único alfabeto para cifrar los mensajes. El método consiste en sustituir cada carácter del texto en claro por otro carácter en el texto cifrado o croptograma. Los cifradores monográmicos, de los que trata este bloque, hacen corresponder una letra del texto en claro a una única letra del criptograma, es decir, cifran monogramas.

▪ Cifradores por Desplazamiento Puro.

Este tipo de cifradores aplica un desplazamiento de b espacios dentro de un alfabeto sobre el texto en claro. En la transformación Ci = (Mi+b) mod n; b es una constante de desplazamiento y n el orden del grupo, El famoso Cifrador del César usa una constante b igual a 3.

PRÁCTICA:

Apartado 1

a) Cifrar con un desplazamiento b=3 el siguiente mensaje:
   M = EN TIEMPOS DE LOS CESARES SE CIFRABA ASI DICE <NombreAlumno/s>
b) Descifrar el criptograma obtenido.

Apartado 2

a) Cifrar con un desplazamiento b=7 el fichero DIDIO.TXT. El fichero de salida se llamará DIDIO.CIF.
b) Descifrar el fichero DIDIO.CIF, guardándolo como DIDIO.DCF.
c) Criptoanalizar el fichero DIDIO.CIF, guardándolo como DIDIO.CRI.

INFORME:

1. ¿Qué resultados obtiene si intenta descifrar o atacar un mensaje que ya está en claro?
2. Explique la relación que existe entre el valor de b de cifra y el valor de desplazamiento encontrado en el criptoanálisis.
3. ¿Qué sucede si se cifra con desplazamiento b=31, b=58 y b=-27?

▪ Cifradores por Decimación Pura.

En este tipo de cifradores la operación de sustitución se realiza mediante la transformación Ci = (a*Mi) mod n, en donde a es la constante de decimación y n el orden del grupo que deben ser primos entre si para que exista el inverso dentro del cuerpo.

PRÁCTICA:

Apartado 1

a) Cifrar con un valor de a=5 el siguiente mensaje:
   M = EN DECIMACIÓN PURA LA CONSTANTE B ES CERO DICE <NombreAlumno/s>.
b) Descifrar el criptograma obtenido.
c) Intente volver a cifrarlo con los valores a=0, a=-6, a=12 y a=1.

Apartado 2

a) Cifrar con un valor de a=10 el fichero INVISIB1.TXT. El fichero de salida se llamará INVISIB1.CIF.
b) Descifrar el fichero INVISIB1.CIF, guardándolo como INVISIB1.DCF.
c) Criptoanalizar el fichero INVISIB1.CIF, guardándolo como INVISIB1.CRI.

INFORME:

1. Indique qué ha sucedido al intentar cifrar el mensaje en el apartado 1c. ¿Cuál es el motivo de que no lo permita el software?
2. Si cifra con a=14 los mensajes M1=MARIA, M2=Maria y M3=María, ¿los criptogramas son iguales o distintos? ¿Por qué?
3. Si cifra el mensaje M=ABCDEFGHIJKLMÑOPQRSTUVWXYZ con el factor de decimación a=-1, ¿qué obtiene como salida?
4. ¿Cuántas opciones para romper el criptograma tiene de acuerdo a la pantalla que le muestra la aplicación en el apartado 2.c? ¿Cuál sería el método óptimo en función del tiempo necesario para romper la cifra?

- ***Cifradores polialfabéticos por sustitución***

Este tipo de cifradores usan más de un alfabeto para cifrar los mensajes. La técnica consiste en aplicar dos o más alfabetos de cifra de forma que cada uno de ellos sirva para cifrar los caracteres del texto en claro dependiendo de la posición relativa de éstos en dicho texto. De esta forma se produce una distribución plana de la frecuencia relativa de los caracteres en el criptograma.

Podemos clasificar a estos cifrados como periódicos y no periódicos. Los primeros tienen un período que vendrá dado por la longitud de la clave de cifra y los segundos utilizan una clave de tamaño igual o mayor al mensaje, con lo cual no existe periodicidad.

- **Cifradores Periódicos.**
  - **Cifrado de Vigenère.**

    El cifrado de Vigenère aplica un desplazamiento de k espacios a los caracteres del texto en claro según el valor numérico asociado a cada uno de los caracteres de una clave que se escribe cíclicamente bajo el mensaje y cuya longitud determinará el valor del período de cifra. La transformación es Ci = (Mi + ki) mod n.

    PRÁCTICA:

    Apartado 1

    a) Cifrar con clave K = AZUL el siguiente mensaje:
       M = ERASE UNA HERMOSA PRINCESA QUE SOLÍA PASEAR POR LOS JARDINES DEL PALACIO REAL.
    b) Descifrar el criptograma obtenido.
    c) Intente romper la cifra obtenida en el punto anterior.
    d) Con la misma clave cifrar el mensaje anterior modificado como se indica:
       M = ERASE UNA HERMOSA PRINCESA QUE SOLÍA PASEAR POR LOS JARDINES DEL PALACIO REAL CON LA ESPERANZA DE ENCONTRAR DETRAS DE UN ARBOL AL PRINCIPE AZUL DE SUS SUEÑOS.
    e) Criptoanalizar el texto cifrado obtenido en el punto anterior.
    f) Repetir la cifra y el criptoanálisis del mensaje del punto 1.d) usando ahora la clave K = AMORES.

    Apartado 2

    a) Cifrar con la clave K = ANDERSEN el fichero SIRENITA.TXT. El fichero de salida se llamará SIRENAV1.CIF.
    b) Descifrar el fichero SIRENAV1.CIF, guardándolo como SIRENAV1.DCF.
    c) Criptoanalizar el fichero SIRENAV1.CIF, guardándolo como

SIRENAV1.CRI.

d) Repetir los puntos a), b) y c) usando como clave K = UN HERMOSO CUENTO. Los ficheros de salida serán SIRENAV2.CIF, SIRENAV2.DCF y SIRENAV2.CRI.
e) Repetir el punto anterior usando ahora como clave K = ME GUSTAN LOS CUENTOS DE ANDERSEN. Los ficheros de salida serán SIRENAV3.CIF, SIRENAV3.DCF y SIRENAV3.CRI.

INFORME:

1. ¿Por qué falla el criptoanálisis en el apartado 1.c?
2. Justifique porqué se rompe el criptograma en el apartado 1.e con cadena de repeticiones de 3 caracteres y no con 2.
3. ¿Se podría utilizar como clave K = "123 SOY YO OTRA VEZ" ¿En qué caso sería posible?
4. Comente y justifique qué ha sucedido en el ataque realizado en el apartado 2.c.
5. ¿Cómo justifica que usando la clave K = UN HERMOSO CUENTO de longitud 15 no se haya podidio romper completamente el criptograma en el apartado 2.d y, por el contrario, para la clave K = ME GUSTAN LOS CUENTOS DE ANDERSEN de longitud 28 si se haya logrado?

- **Cifrado de Beaufort**

En este tipo de cifradores la operación de sustitución se realiza mediante la fórmula Ci = (ki-Mi) mod n. Por tanto, se invierte el orden de las letras del alfabeto A y luego se le aplica un desplazamiento de ki posiciones hacia la derecha. Una de las particularidades de este método es que la operación de cifrado es igual que la de descifrado, se trata de una función involutiva.

PRÁCTICA:

Apartado 1

a) Cifrar con clave K = LIBROS el siguiente mensaje:
M = LOS CUENTOS DE ANDERSEN SON FAMOSOS MUNDIALMENTE DICE <NombreAlumno/s>
b) Descifrar el criptograma obtenido

Apartado 2

a) Cifrar con clave K = ROJAS el fichero ZAPATI.TXT. El fichero de salida se llamará ZAPATIBA.CIF.
b) Descifrar el fichero ZAPATIBA.CIF, guárdelo como ZAPATIBA.DCF.
c) Criptoanalizar el fichero ZAPATIBA.CIF, guárdelo como ZAFATIBA.CRI.
d) Repita los puntos a), b) y c) primero usando la clave K = ZAPATILLA y luego con K = ZAPATILLAS. Los archivos de salida serán ZAPATIBB.CIF, ZAPATIBB.DCF, ZAPATIBB.CRI Y ZAPATIBC.CIF, ZAPATIBC.DCF y ZAPATIBC.CRI.

INFORME:

1. Compruebe la cifra del mensaje del apartado 1.a aplicando directamente aritmética modular.
2. Explique brevemente cómo se ha realizado el criptoanálisis al archivo del apartado 2.c.
3. Explique qué sucede en los ataques a la cifra del apartado 2.d.

- **Cifrado Variante de Beaufort**

La cifra se realiza mediante la ecuación Ci = (Mi – ki) mod n. Esta operación es equivalente a cifrar con el algoritmo de Vigenère siendo ahora la clave (n-ki).
PRÁCTICA:
Apartado 1

a) Cifrar con clave K = AZUL el mensaje de la práctica de Vigenère: M = ERASE UNA HERMOSA PRINCESA QUE SOLIA PASEAR POR LOS JARDINES DEL PALACIO REAL.
b) Descifrar el criptograma obtenido pero volviendo a cifrarlo ahora con el algoritmo de Vigenère.

Apartado 2

a) Cifrar con clave K = ANDERSEN el fichero SIRENITA.TXT. El fichero de salida se llamará SIRENAVB.CIF.
b) Descifrar el fichero SIRENAVB.CIF, guardándolo como SIRENAVB.DCF.
c) Criptoanalizar el fichero SIRENAVB.CIF, guardándolo como SIRENAVB.CRI.

INFORME:

1. Explique qué ha sucedido al cifrar con Vigenère lo cifrado antes por Variante de Beaufort.
2. Compare los cinco primeros caracteres del cirptograma SIRENAVB.CIF con el criptograma obtenido con Vigenère SIRENAV1.CIF. ¿Qué puede concluir de los valores encontrados?

- **Cifradores no Periódicos**

  - **Cifrado de Clave Continua**

En este tipo de cifradores se aplica el mismo método de cifrado que en Vigenère o Beaufort pero como clave se usa un texto que tiene una longitud igual o mayor que el texto a cifrar. Por tanto, ya no se habla del uso de una clave, sino de una secuencia de clave.

  - **Cifrado de Vernam**

En este tipo de cifradores cada carácter Mi se suma or exclusivo con la correspondiente clave ki de una secuencia binaria aleatoria. Como la función XOR es involutiva, el descifrado usa el mismo algoritmo. Una representación orientada a caracteres contempla desplazamientos en módulo n con una secuencia de clave compuesta por números aleatorios.
PRÁCTICA:
Apartado 1

a) Cifrar con Vernam orientado a caracteres o XOR el siguiente mensaje:
   M = Asi se cifra con Vernam en modo normal.
b) Utilizar para ello las siguiente secuencias:
   1. 00000000000000000000000000000000
   2. 01234567890123456789012345678 90
c) Cifrar con Vernam binario el siguiente mensaje:
   M = Y ahora ciframos con Vernam binario.
d) Utilizar para ello las siguiente secuencias:
   1. VERNAM VERNAM VERNAM VERNAM VERNAM VERNAM

2. vernam vernam vernam vernam vernam vernam

Apartado 2

a) Cifrar con el método de Vernam binario el fichero ZAPATI.DOC que tiene formato Microsoft Word. Use como clave un archivo de mayor longitud, por ejemplo SIRENITA.TXT. El fichero de salida se llamará VERNAM.CIF.
b) Descifrar el fichero VERNAM.CIF, guardándolo como VERNAM.DCF. Observe si se obtenido el mismo archivo.

INFORME:

1. Comente qué ha sucedido en las operaciones de cifra del apartado 1.
2. ¿Daría el mismo resultado si se usará el método de Vernam orientado a caracteres en la cifra del apartado 2.a?
3. Al descifrar el fichero VERNAM.CIF en el apartado 2.b, ¿se recupera el formato de Word 7.0. ¿Por qué?

- ***Cifradores de transposición.***

En este tipo de cifradores se realiza una reordenación o permutación de los caracteres del texto en claro. El resultado de tal acción es la dispersión de los elementos de la información propuesto por Shannon.

Según el método utilizado en esta permutación, hablamos de cifradores por transposición de grupos, por transposición de series, por transposición de filas y por transposición de columnas.

- **Cifradores por Transposición de Filas.**

En este tipo de cifradores se escribe el mensaje en forma vertical con un cierto nivel de profundidad. El cifrado se obtiene leyendo en forma horizontal, es decir por filas, dando lugar al criptograma.

PRÁCTICA:

Apartado 1

a) Cifrar para valores distintos de filas (en concreto 1, 2, 3, 4 y 5) el siguiente mensaje:
   M = VAMOS A CIFRAR POR TRANSPOSIC DE FILAS DICE <NombreAlumno/s>
b) Repetir cifrando con 20 y 30 filas.
c) Descifrar los cirptogramas obtenidos con 2 y 4 filas.

Apartado2:

a) Cifrar con un valor de 16 filas el fichero MERLIN1.TXT. El fichero de salida se llamará MERLIN1.CIF.
b) Descifrar el fichero MERLIN1.CIF, guardándolo como MERLIN1.DCF.
c) Criptoanalizar el fichero MERLIN1.CIF, guardando el fichero como MERLIN1.CRI.

- **Cifradores por Transposición de Columnas.**

En los cifrados por columnas, se escribe el mensaje de izquierda a derecha cambiando de linea cada n columnas, valor que hace las veces de clave. El criptograma se obtiene enviando el texto que resulta de la lectura, en un cierto orden, de cada una de las columnas.

PRÁCTICA:

Apartado 1

a) Cifar con 8 columnas el siguiente mensaje:

M = AHORA PROBAMOS COMO SE CIFRA POR COLUMNAS DICE <NombreAlumno/s>

b) Descifrar el criptograma obtenido.
c) Intente criptoanalizar el criptograma obtenido con un valor de ventana mayor que 5.

Apartado 2

a) Cifrar con una valor de 30 columnas el fichero MERLIN2.TXT. El fichero de salida se llamará MERLIN2.CIF.
b) Descifrar el fichero MERLIN2.CIF, guardándolo como MERLIN2.DCF.
c) Criptoanalizar el ficheor MERLIN2.CIF, guardándolo como MERLIN2.CRI. Usar para ello distintas longitudes de ventana.

INFORME:

1. Indique porqué no se puede romper el cifrado en el apartado 1.c.
2. Elija una ventana de tamaño 20 y demuestre que, según el método de anagramación, en el período de cifra se cumple que la media de los diagramas es un valor alto y la desviación estándar tiende a ser baja.