Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ciencias y Sistemas
Introducción a la Programación y Computación 1
Ing. Cesar Batz
Aux. Eduardo Álvarez
Aux. Luis Rodríguez

Práctica No. 1(Criptografía)

El alto crecimiento de la tecnología en el manejo de información, ha obligado que las medidas de seguridad tomadas en el cuidado de información sean garantizadas en un alto porcentaje, permitiendo que la confiabilidad en la tecnología se incremente cada vez más.

Para estudiar la aplicación de diferentes conceptos matemáticos aplicados a la computación, se le solicita que por medio de álgebra lineal usted pueda ser capaz de implementar en lenguaje Java él un algoritmo de encriptación.

Para esto, se inicia asignando un número entero consecutivo a cada letra del alfabeto. En este caso se iniciará con el espacio en blanco hasta la letra "Z", los números asignados iniciarán desde 0 hasta 27.

Número	Letra	Número	Letra
0	" " (Espacio en blanco)	14	N
1	A	15	O
2	B	16	P
3	C	17	Q
4	D	18	R
5	E	19	S
6	F	10	T
7	G	21	U
8	H	22	V
9	I	23	W
10	J	24	X
11	K	25	Y
12	L	26	Z
13	M	27	.

La aplicación no debe distinguir entre mayúsculas y minúsculas deben ser tratadas por igual.

Se debe definir una matriz cuadrada de n*n la cual, será llamada Matriz A. La matriz a utilizar para esta práctica será:

$$A = \begin{bmatrix} 1 & 2 & 0 & 3 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 2 & 0 & 2 \end{bmatrix}$$

Esto con el fin de hacer uso de un estándar y conocer si se hizo uso correcto del algoritmo de encriptación.

La matriz "A" presentada en este documento será almacenada directamente en la aplicación como una matriz de enteros, ésta será utilizada como matriz default.

Codificación:

Paso 1)
Dividir la cadena de entrada y asociarla con cada uno de los valores numéricos establecidos al inicio del enunciado.

Ejemplo:

H	O	L	A		M	U	N	D	O
8	15	12	1	0	13	21	14	4	15

Paso 2)
Almacenar los valores en una matriz de m*4, es decir "m" filas por 4 columnas en este caso, m no tiene límite. La matriz contendrá el código del mensaje a encriptar, los espacios de la matriz que no contengan valores propios de la cadena deberán ser rellenados con espacios en blanco "0"s.
Ejemplo:

$$Valores\ a\ Encriptar \begin{bmatrix} 8 & 15 & 12 & 1 \\ 0 & 13 & 21 & 14 \\ 4 & 15 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ . & & & \\ . & & & \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Paso3)

Multiplicar cada elemento de la matriz de valores por la matriz A, de esta forma se obtendrá la matriz con el mensaje encriptado.

La multiplicación de las matrices se realiza de la siguiente manera:

Se toma cada fila de la matriz de valores y se multiplica por cada columna de la matriz A, a continuación se muestra la secuencia a seguir para realizar la multiplicación.

1) 8*1+15*0+12*0+1*1=9

8	15	12	1
0	13	21	14
4	15	0	0
0	0	0	0
.			
.			
0	0	0	0

*

1	2	0	3
0	1	1	1
0	1	0	1
1	2	0	2

=

9			

2)8*2+15*1+12*1+1*2=45

8	15	12	1
0	13	21	14
4	15	0	0
0	0	0	0
.			
.			
0	0	0	0

*

1	2	0	3
0	1	1	1
0	1	0	1
1	2	0	2

=

9	45		

3)8*0+15*1+12*0+1*0=15

8	15	12	1
0	13	21	14
4	15	0	0
0	0	0	0
.			
.			
0	0	0	0

*

1	2	0	3
0	1	1	1
0	1	0	1
1	2	0	2

=

9	45	15	

4) 8*3+15*1+12*1+1*2= 53

8	15	12	1
0	13	21	14
4	15	0	0
0	0	0	0
.			
.			
0	0	0	0

*

1	2	0	3
0	1	1	1
0	1	0	1
1	2	0	2

=

9	45	15	53

5) 0*1+13*0+21*0+14*1=14

8	15	12	1
0	13	21	14
4	15	0	0
0	0	0	0
.			
.			
0	0	0	0

*

1	2	0	3
0	1	1	1
0	1	0	1
1	2	0	2

=

9	45	15	53
14			

6) 0*2+13*1+21*1+14*2=62

8	15	12	1
0	13	21	14
4	15	0	0
0	0	0	0
.			
.			
0	0	0	0

*

1	2	0	3
0	1	1	1
0	1	0	1
1	2	0	2

=

9	45	15	53
14	62		

7) 0*0+13*1+21*0+14*0=13

8	15	12	1
0	13	21	14
4	15	0	0
0	0	0	0
.			
.			
0	0	0	0

*

1	2	0	3
0	1	1	1
0	1	0	1
1	2	0	2

=

9	45	15	53
14	62	13	

8) 0*3+13*1+21*1+14*2= 62

8	15	12	1
0	13	21	14
4	15	0	0
0	0	0	0
.			
.			
0	0	0	0

*

1	2	0	3
0	1	1	1
0	1	0	1
1	2	0	2

=

9	45	15	53
14	62	13	62
…			
…			
…			
…			
…			

El proceso continúa de la misma forma hasta completar la multiplicación entre cada una de las filas de la matriz de valores por cada una de las columnas de la matriz “A”. Al final del proceso lo que se tiene en la matriz resultado es la cadena encriptada y únicamente puede ser decodificada si se posee la matriz “A”.

Para aumentar el nivel de seguridad de la encriptación, se sustituirán estos valores por

el correspondiente binario de cada valor y esta será la salida de la cadena encriptada. Para esto deberá hacer uso de la siguiente tabla:

Decimal	Binario	Decimal	Binario
0	0000	5	0101
1	0001	6	0110
2	0010	7	0111
3	0011	8	1000
4	0100	9	1001

Decodificación:

Paso 1)
Calcular la matriz inversa de la matriz A.
La matriz inversa correspondiente para la matriz A, en esta práctica es la siguiente:

$$A^{-1} = \begin{bmatrix} 0 & 0 & -2 & 1 \\ -1 & 0 & 1 & 1 \\ 0 & 1 & -1 & 0 \\ 1 & 0 & 0 & -1 \end{bmatrix}$$

Para llegar a este resultado se deberá tener una matriz que contenga la matriz identidad:

$$I = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Sobre esta matriz deben ser realizadas las siguientes operaciones:

1) Restar R4-R1 el resultado colocarlo en R4
2) Restar R1-2*R2 el resultado almacenarlo en R1
3) Restar R3-R2 el resultado almacenarlo en R3
4) Multiplicar R3 por -1 el resultado almacenarlo en R3
5) Restar R2-R3 el resultado almacenarlo en R2
6) Sumar R1+2*R3 el resultado almacenarlo en R1
7) Multiplicar R4*-1 el resultado almacenarlo en R4
8) Restar R2-R4 el resultado almacenarlo en R2
9) Restar R1-R4 el resultado almacenarlo en R1

Al final se tendrá la matriz inversa de la matriz “A”.

Paso 2)
Ordenar el mensaje encriptado en una matriz de m*n filas, en este caso “n=4”. Para esto deberá leer la cadena de binarios y separarla por cuartetos, luego convertir el binario a su correspondiente valor para luego ordenarlo dentro de la tabla mencionada.

Paso 3)
Se debe realizar la multiplicación entre la matriz con la cadena encriptada y la matriz A-1 de esta forma se obtiene la matriz con la cadena desencriptada, el proceso de multiplicación de matrices fue explicado en la codificación.

Paso 4)
Cambiar los valores encontrados por el valor del alfabeto correspondiente.

Consideraciones:

- La cadena a encriptar podrá tener cualquier tamaño.
- El proceso debe realizarse de forma transparente al usuario, esto quiere decir, que el usuario no deberá saber que ocurre durante todo el proceso la única salida de la aplicación es la cadena encriptada o desencriptada según sea el caso.
- El lenguaje a utilizar para implementar la aplicación será Java(consola).
- La aplicación debe poseer entorno intuitivo para el usuario.
- Está totalmente prohibido hacer copy/paste de código de internet, si es así no se podrá calificar pues no se estará cumpliendo con los objetivos de esta práctica.
- Toda copia detectada tendrá una nota negativa completa igual al valor de la practica.
- Durante la calificación se realizaran 2 preguntas acerca del funcionamiento de la práctica de no responder correctamente su nota se verá afectada en 20 puntos por cada respuesta incorrecta.

Entregables:

- Documento PDF, con los diagramas de flujo de los principales algoritmos.
  - Proceso general de la funcionalidad de la aplicación
  - Proceso de encriptación
  - Proceso de desencriptación
- CD con el código fuente(#carnet.java, ejemplo 201214562.java) y documentación.
- Fecha de Entrega disco y documentación (digital) 03/09/2013 enfrente de Escuela de Ciencias y Sistemas Edficio T-3 de 08:50 a.m. a 9:00 a.m.
- Fecha de Calificación 3/09/2013 de 9:00 a.m. en adelante.