Universidad Nacional de Ingeniería
Facultad de Ciencias

Curso : SEGURIDAD COMPUTACIONAL

Tema : ESCITALA

Profesor : Arrunátegui Angulo, Gipsy Miguel
Alumno : Arotoma Bacilio, Bitzer
Ruta del trabajo en github

April 5, 2017

1 Criptografia : La Escitala Espartana

1.1 Explicación de como compilar el programa:

Se desarrollo tres programas en c **(EscitalaEncriptar.c, EscitalaDesencriptar.c y EjemploClase.c)**, la forma de ejecución en una distribución Linux es mediante terminal primero ubicándonos en la ruta donde se descarga y de ahi usar el comando **gcc EscitalaEncriptar.c -o encriptar**, luego de esto se creara el ejecutable encriptar que se ejecuta así **./encriptar**, en el caso de un sistema Windows descargar codeblock o turbo c++.

1.2 Uso del programa:

El programa **EscitalaEncriptar.c** lo que hace es pedir que ingreses un texto, luego pide el numero de columnas para almacenar carácter por carácter del texto en cada posición de una matriz, el numero de filas se halla dividiendo la longitud de la cadena entre el numero de columnas, si el resultado es con decimal se convierte en un entero y se le suma 1, si es de tipo entero se mantiene.
La siguiente imagen muestra el código para hallar el numero de filas

```
float filas(int columnas){
   float filas1;
   int bandera;
   lon= strlen(text);
   filas1 =  lon/(columnas*1.0);
   bandera = (int) filas1;
   if( filas1/bandera == 1)
      return filas1;
   else
      return filas1+1;
}
```

En la siguiente imagen se muestra el código de como se almacena carácter del texto en cada elemento de la matriz; en la linea 41 cuando se termino de almacenar todo el texto y quedan elementos en la matriz se completa con el carácter ' ', ya que para desencriptar se tendra problemas.

```
32    printf("Numero de columnas :");
33    scanf("%d",&columnas);
34    filas1=(int)filas(columnas);
35
36    char matriz[filas1][columnas];
37
38    for(i = 0 ; i < filas1; i++)
39       for(j = 0 ; j < columnas; j++, k++){
40          matriz[i][j] = text[k];
41          if(k >= lon)
42             matriz[i][j] = ' ';
43       }
```

Después la matriz en la que se almaceno el texto, hacemos que nos muestre el texto encriptado, este se formo leyendo columna por columna de la matriz, el orden para leer las columnas es desde el 0 al n-1, donde n-1 es el numero de columnas.

```
56    for(i=0; i<columnas ; i++){
57       for(j=0; j<filas1 ;j++){
58          printf("%c",matriz[j][orden[i]]);
59          fprintf(fp,"%c",matriz[j][orden[i]]);
60       }
61    }
```

El texto encriptado lo almaceno en un archivo llamado **texto** y a la vez lo muestro en la terminal.La siguiete imagen muestra el texto encriptado, y **cat texto** nos muestra lo que hay en el archivo **texto**.

```
bitzer@bitzer-Satellite-L45-B ~/D/S/Escitala> ./encriptar
Ingresar texto :uni campeon
Numero de columnas :3
u moncpniae
bitzer@bitzer-Satellite-L45-B ~/D/S/Escitala> cat texto
u moncpniae
bitzer@bitzer-Satellite-L45-B ~/D/S/Escitala>
```

En el programa **EscitalaDesencriptar.c** se lee el archivo texto que se creo en el programa anterior y se almacena en una matriz, al igual que el anterior te pedira el numero de columnas el cual debe ser igual al que le diste en el programa anterior, el texto se almacena en una matriz pero esta matriz el numero de columnas representa al numero de filas y el numero de columnas representara a numero de filas que se halla igual que en el programa anterior.
La siguiente imagen se ve que i es el numero de columnas y j igual al numero de filas, lo contrario al programa anterior **EscitalaEncriptar.c**.

```
printf("Numero de columnas :");
scanf("%d",&columnas);
filas1=(int)filas(columnas);

char matriz[columnas][filas1];
for(i=0 ; i<columnas; i++)
   for(j=0 ; j<filas1; j++,k++){
      matriz[i][j] = text[k];
      if(k >= lon)
         matriz[i][j] = ' ';
   }
```

La siguiente imagen muestra la ejecucion de este programa y el texto desencriptado

```
bitzer@bitzer-Satellite-L45-B ~/D/S/Escitala> ./desencriptar
Numero de columnas :3
uni campeon
bitzer@bitzer-Satellite-L45-B ~/D/S/Escitala>
```

1.3 Mostrando encriptacion y desencriptacion con otro ejemplo

Imagen que muestra ejecucion de los dos programas anteriores con otro ejemplo.

```
bitzer@bitzer-Satellite-L45-B ~/D/S/Escitala> ./encriptar
INGRESAR TEXTO : Universidad Nacional de Ingenieria
Numero de columnas :4
UedNo Ininraandniaisdcaege vi il er
bitzer@bitzer-Satellite-L45-B ~/D/S/Escitala> ./desencriptar
Numero de columnas :4
Universidad Nacional de Ingenieria
bitzer@bitzer-Satellite-L45-B ~/D/S/Escitala>
```

1.4 Ejemplo que se dio en clase

En el ejemplo que se dio en clase el orden de encriptacion es de forma aleatoria el orden es 6, 0, 2, 4, 1, 3 y 5; el programa del ejemplo se llama **EjemploClase.c**.
La siguiente imagen muestra el orden que se dio, y la impresion de este columna por columna.

```
int orden[columnas];

   orden[6]=0;
   orden[0]=1;
   orden[2]=2;
   orden[4]=3;
   orden[1]=4;
   orden[3]=5;
   orden[5]=6;

for(i=0; i<filas1 ; i++){
   for(j=0; j<columnas ;j++){
      printf("%c",matriz[orden[j]][i]);
   }
}
printf("\n");
```

Resultado de la desencriptacion del ejemplo dado en clase, el numero de columnas es 7.

```
bitzer@bitzer-Satellite-L45-B ~/D/S/Escitala> ./ejemplo
Ingresar texto :
 N..NAEEA.ENEH.GR.SAOTQ.C....N.RBS.T.IQIAEI.BRUEEAUIP...LUBNRE.OTDAES.TUI..BISU.T.S
TRSTESED.SOBO.IP...
Ingresar numero de columnas :7
CUENTAN.DE.UN..SABIO..QUE.UN.DIA.TAN.POBRE.Y.MISERO.ESTABA.QUE.SOLO.SE.SUSTENTABA.D
.Y.TRISTE.QUE.YO..
bitzer@bitzer-Satellite-L45-B ~/D/S/Escitala>
```