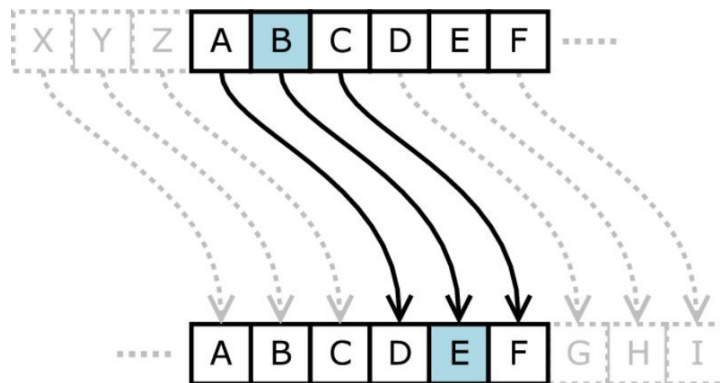


Instituto Politécnico Nacional

Escuela Superior de Cómputo

Cryptography

Practica 1: Substitution cipher 6/02/19



Nombres:

- Santuario Parra Luis Fernando
- Varela Cruz Cesar Alejandro

Grupo: 3CM6

Introducción	3
Objetivo	3
Desarrollo	3
Shift Cipher	3
Funciones para shift cipher	4
Ejemplo shift cipher	4
Afín Cipher	5
Funciones afín cipher	5
Ejemplo cifrado afín	7
Conclusión	8
Referencias	8

Introducción

Desde el principio de la comunicación el hombre a tratado de mantener cierta información alejada de las miradas curiosas, ya sea para proteger información delicada o simplemente para que otras personas no se enteren de sus secretos.

La criptología se puede dividir en dos grandes grupos:

- ❖ La criptografía: Encargada de las técnicas para poder cifrar la información.
- ❖ El criptoanálisis: Se basa en los mecanismos utilizados para decodificar dicha información, osea busca mecanismos para poder descifrar un mensaje y obtener su contenido.

Durante todo este tiempo han surgido numerosos métodos de ocultar información que varían en la forma en la que lo consiguen, aunque cabe aclarar que hay métodos más o menos seguros, así como más fáciles de romper que otros.

Objetivo

Implementar el cifrado Afín y el cifrado por sustitución utilizando los caracteres del ASCII imprimibles y que sea capaz de recibir el mensaje por un archivo de texto dando a la salida un archivo con el mensaje cifrado.

Desarrollo

Shift Cipher

Para poder utilizar shift cipher con los caracteres imprimibles de ascii se sabe que va desde el 32 al 126 con lo cual para poder hacer el cambio la fórmula de cifrado queda como

$$c = (((mi - 32) + k) \% 94) + 32$$

y para poder descifrar se usa

$$m = (ci - 32 - k) \% 94 + 32 \text{ si } ci - 32 < 0 \text{ entonces } (ci - 32) + 94$$

Funciones para shift cipher

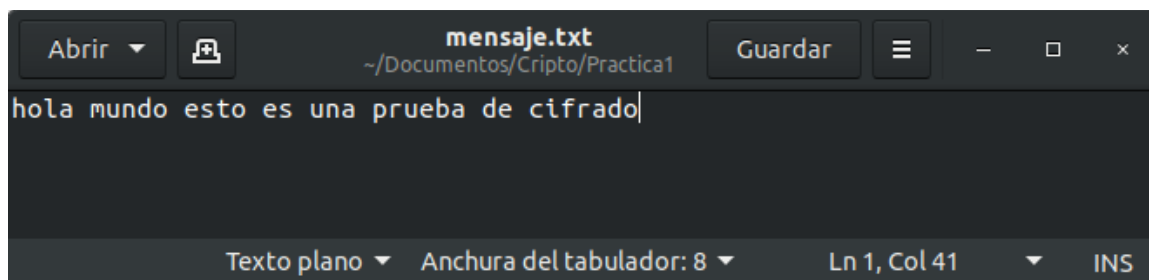
```

1. string cifrar(string mensaje, string llave){
2.     for (int i = 0; i < mensaje.length() ; i++) {
3.         mensaje[i]=(((mensaje[i]-32)+(llave[i%llave.size()]-32))%94)+32;
4.     }
5.     return mensaje;
6. }
7.
8. string decifrar(string mensaje, string llave){
9.     for (int i = 0; i < mensaje.length() ; i++) {
10.        int valor=((mensaje[i]-32)-(llave[i%llave.size()]-32));
11.        if (valor<0){
12.            valor=valor+94;
13.            mensaje[i]=((valor)%94)+32;
14.        }else {
15.            mensaje[i] = ((valor) % 94) + 32;
16.        }
17.    }
18.    return mensaje;
19.}

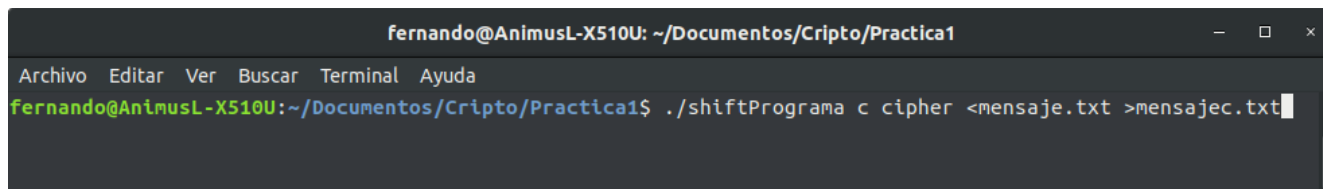
```

Ejemplo shift cipher

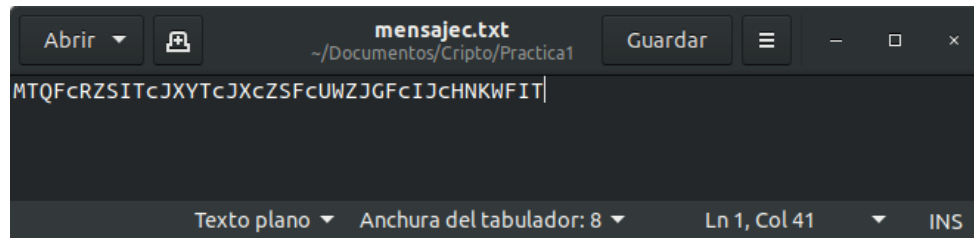
Mensaje en claro



Introducción de la llave y el mensaje a cifrar

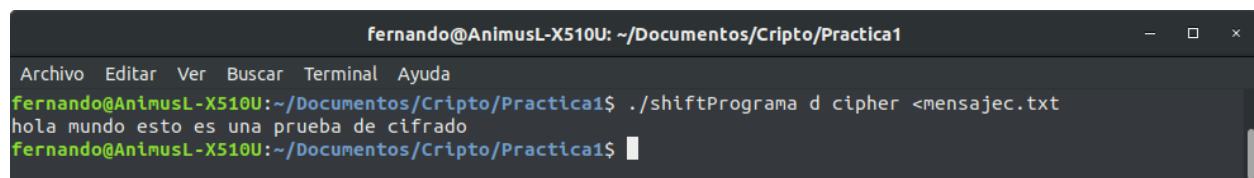


Mensaje cifrado



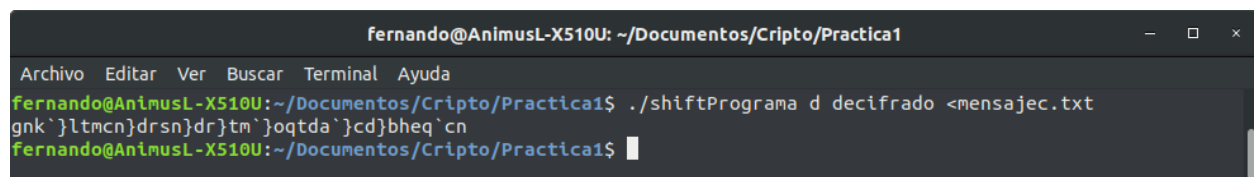
A screenshot of a text editor window titled 'mensajeec.txt' with the path '~/Documentos/Cripto/Practica1'. The editor contains the ciphertext 'MTQFcRZSITcJXYTcJXcZSfcUWZJGfcIJcHNKWFIT|'. The status bar at the bottom indicates 'Texto plano', 'Anchura del tabulador: 8', 'Ln 1, Col 41', and 'INS'.

Opción descifrar



A screenshot of a terminal window with the title 'fernando@AnimusL-X510U: ~/Documentos/Cripto/Practica1'. The terminal shows the command `./shiftPrograma d cipher <mensajeec.txt` being executed, resulting in the output 'hola mundo esto es una prueba de cifrado'.

Opción descifrar con contraseña errónea



A screenshot of a terminal window with the title 'fernando@AnimusL-X510U: ~/Documentos/Cripto/Practica1'. The terminal shows the command `./shiftPrograma d decifrado <mensajeec.txt` being executed, resulting in the output 'gnk`}}ltmcn}drsn}dr}tm`}}oqtda`}cd}bheq`cn'.

Afín Cipher

Para poder utilizar afín cipher con los caracteres imprimibles de ascii se sabe que va desde el 32 al 126 con lo cual para poder hacer el cambio la fórmula de cifrado queda como:

$$c = (((a * mi - 32) + b) \% 94) + 32$$

y para poder descifrar se usa

$$m = a^{-1} * (ci - 32 - b) \% 94 + 32 \text{ si } ci - 32 < 0 \text{ entonces } (ci - 32) + 94 \text{ siempre y cuando } a \text{ tenga inverso}$$

Funciones afín cipher

1. `int xGCD(int a, int b, int &x, int &y) { //Funcion teorema de Euclides extendido`
2. `if(b == 0) {`
3. `x = 1;`
4. `y = 0;`
5. `return a;`
6. `}`
- 7.
8. `int x1, y1, gcd = xGCD(b, a % b, x1, y1);`

```
9.    x = y1;
10.   y = x1 - (a / b) * y1;
11.   return gcd;
12. }
13.
14. string cifrarAfin(string mensaje, int a, int b,int x, int y){//función de cifrado
15.   int gcd=xGCD(94,a,x,y);
16.   if(gcd==1){
17.     for (int i = 0; i <mensaje.length() ; i++) {
18.       mensaje[i]=(((mensaje[i]-32)*a+(b))%94)+32;
19.     }
20.   }else{
21.     cout<<"El valor de a no es valido"<<endl;
22.   }
23.   return mensaje;
24. }
25. string decifrarAfin(string mensaje, int a, int b,int x, int y){//función de descifrado
26.   int gcd=xGCD(94,a,x,y);
27.   if(gcd==1) {
28.     for (int i = 0; i < mensaje.length(); i++) {
29.       int valor = ((mensaje[i] - 32) - (b));
30.       if (valor < 0) {
31.         valor = valor + 94;
32.         mensaje[i] = ((y*valor) % 94) + 32;
33.       } else {
34.         mensaje[i] = ((y*valor) % 94) + 32;
35.       }
36.     }
37.   }else{
38.     cout<<"Valor de a no valido";
39.   }
40.   return mensaje;
41. }
42.
```

Ejemplo cifrado afín

Mensaje en claro

```

mensaje.txt
~/Documentos/Cripto/Practica1
Guardar
hola esto es una prueba de cifrado afin
Texto plano Anchura del tabulador: 8 Ln 1, Col 40 INS

```

Introducción de las llaves y mensaje

```

fernando@AnimusL-X510U: ~/Documentos/Cripto/Practica1
Archivo Editar Ver Buscar Terminal Ayuda
fernando@AnimusL-X510U:~/Documentos/Cripto/Practica1$ ./afinPrograma c 5 7 <mensaje.txt >mensajec.afn
fernando@AnimusL-X510U:~/Documentos/Cripto/Practica1$

```

Texto cifrado

```

mensajec.afn
~/Documentos/Cripto/Practica1
Guardar
u:+R'fNS:'fN'X5R'?IXfWR'af'\zkIRa:'Rkz5
Texto plano Anchura del tabulador: 8 Ln 1, Col 1 INS

```

Descifrado del mensaje

```

fernando@AnimusL-X510U: ~/Documentos/Cripto/Practica1
Archivo Editar Ver Buscar Terminal Ayuda
fernando@AnimusL-X510U:~/Documentos/Cripto/Practica1$ ./afinPrograma d 5 7 <mensajec.afn
hola esto es una prueba de cifrado afin
fernando@AnimusL-X510U:~/Documentos/Cripto/Practica1$

```

Descifrado del mensaje con llaves no válidas.(llave sin inverso)

```

fernando@AnimusL-X510U: ~/Documentos/Cripto/Practica1
Archivo Editar Ver Buscar Terminal Ayuda
fernando@AnimusL-X510U:~/Documentos/Cripto/Practica1$ ./afinPrograma d 4 7 <mensajec.afn
Valor de a no validou:+R'fNS:'fN'X5R'?IXfWR'af'\zkIRa:'Rkz5
fernando@AnimusL-X510U:~/Documentos/Cripto/Practica1$

```

Descifrado del mensaje con llaves no válidas.(llave con inverso)

```

fernando@AnimusL-X510U: ~/Documentos/Cripto/Practica1
Archivo Editar Ver Buscar Terminal Ayuda
fernando@AnimusL-X510U:~/Documentos/Cripto/Practica1$ ./afinPrograma d 7 5 <mensajec.afn
|#dwV_i4#V_iV]XwVL@]_BwV6_VkG*@w6#Vw*GX
fernando@AnimusL-X510U:~/Documentos/Cripto/Practica1$

```

Conclusión

Santuario Parra Luis Fernando

En esta práctica se lograron desarrollar los dos sistemas de cifrado y descifrado, tanto el afín como el shifter empleando el lenguaje de programación C++ y cumpliendo con la características solicitadas en la hoja de la práctica, también se logró utilizar los caracteres imprimibles de ASCII así como lograr modificar las funciones de cifrado y descifrado de cada método para poder utilizar ese rango de valores.

Adicionalmente se pudo comprender de mejor manera este tipo de cifradores al poder implementarlos en un lenguaje como lo es C++.

César Alejandro Varela Cruz

Esta práctica, realizada en C++ nos permitió aprender más sobre cómo funcionan 2 de los cifrados básicos de la criptografía clásica, así como el cómo descifrarlos y la importancia de que los algoritmos de encriptación sean simétricos. En base a los requerimientos, desarrollamos 2 programas: 1 Afín cipher|decipher y un Shift cipher|decipher observando que aparte de poder manejar diferentes tipos de cifrado, también se puede variar el rango de caracteres con el que se cifra o descifra, en este caso uno funciona con el alfabeto y el otro cifrado con todas los caracteres imprimibles del ASCII.

Referencias

[1] *Egov.ufsc.br*, 2019. [Online]. Available:

http://www.egov.ufsc.br/portal/sites/default/files/la_criptografia_desde_la_antigua_grecia_hasta_la_maquina_enigma1.pdf. [Accessed: 12- Feb- 2019].

[2] "Historia de la Criptografía | Seguridad en Cómputo", *Blogs.acatlan.unam.mx*, 2019. [Online].

Available: <http://blogs.acatlan.unam.mx/lasc/2016/06/15/historia-de-la-criptografia/>. [Accessed: 12-Feb- 2019].