Memoria

Prácticas

Algoritmia Básica

Práctica 1

Autor:

Hugo Mateo Trejo, 816678

Paula Oliván Usieto, 771938

Toma de decisiones

A la hora de enfrentarnos a este problema teníamos varios puntos de guión que debían ser debatidos y elegir una posible solución para continuar con el desarrollo del código tratando de crear el algoritmo más eficiente posible.

El primer punto importante era cómo cifrar el mensaje ya que para esto se debía convertir cada carácter ASCII a codificación binaria, por lo tanto se manejaron dos opciones, la primera de ellas era convertir el mensaje a bits haciendo uso de la biblioteca estándar de C++ bitset, la otra opción existente era tratar el mensaje como una máscara. Esta segunda opción fue la que se decidió e implementó.

Se consideró la máscara como la mejor opción ya que nos ahorramos tener convertir el string en caracteres independientes que posteriormente son pasados a formato bitset<8>, además de debía volver a recorrer cada uno de estos bits para realizar el cifrado. Al usar una máscara sólo es necesario concatenar la clave pública un cierto número de veces por letras contenga el string y posteriormente aplicar la máscara, proceso que es mucho más eficiente ya que usa operaciones a nivel de bit que el procesador es capaz de realizar fácilmente.

En segundo lugar se debió decidir los formatos de mochila que eran admitidos por nuestro programa para realizar el cifrado del mensaje. Como sabemos un carácter char posee 8 bits que lo identifican, por tanto, si elegimos una mochila de un tamaño distinto a 8 se debe cifrar de manera que estos 8 bits sean procesados correctamente y no se pierda ninguno. En el algoritmo de cifrado utilizado cada bit de la letra en cuestión es multiplicado por un número de la clave pública, es decir, que si nuestra clave es de mayor o menor tamaño habrá números que pueden no utilizarse o carácteres que no sean cifrados, esto es peligroso, debido a que al realizar el descifrado al no saber qué parte no se ha utilizado los resultados obtenidos no son iguales a los inicialmente introducidos.

Por ello se tomó la decisión de permitir al usuario únicamente utilizar divisores de 8 como posible mochila. También se barajó la idea de permitir múltiplos de 8 también, esto debido a que entonces se debían cifrar juntas varias letras lo cual en el descifrado produce los mismos problemas redactados anteriormente, además también se necesitaría introducir un número de carácteres que al ser dividido por el múltiplo no diera carácteres sin bloque de cifrado. Sin embargo al usar números menores o iguales a 8 y que son sus divisores esto no se produce ya que los carácteres podrán ser divididos sin problema en las partes necesarias para que cada bit se corresponda a uno de los números de la clave, y posteriormente en el descifrado los bits producidos se concatenan con el tamaño necesario para volver a originar el char inicial.

Pruebas realizadas:

```
Probamos con una mochila de tamaño 2
El mensaje a cifrar es: Este mensaje no podrá ser descifrado
El número N escogido es: 85
El número w escogido es: 11
La mochila escogida como clave privada es: 15 20

Clave publica: 80 50
El mensaje cifrado es: 50 0 50 50 50 130 0 130 50 130 50 0 50 80 50 50 0 80 0 0 50 80 130 50 50 80 50 50 50 80 130 80 50 130 0 130 50 80 0 50 50 80 80 80 50 80 50 50 0 80 0 0 50
 80 130 80 50 80 130 130 0 80 0 0 50 130 0 0 50 80 130 130 50 80 50 0 50 130 0 80 130 0 0 130 80 80 0 50 0 80 0 0 50 130 0 130 50 80 50 50 50 130 0 80 0 80 0 0 50 80 50 0 50 80
50 50 50 130 0 130 50 80 0 130 50 80 80 50 50 80 50 80 50 130 0 80 50 80 0 50 50 80 50 0 50 80 130 130

El mensaje original es: Este mensaje no podrá ser descifrado
```

```
El mensaje a cifrar es: Buenos días Mario, ¿qué tal ayer la pescas?
El número N escogido es: 85
El número w escogido es: 11
La mochila escogida como clave privada es: 20 45

Clave publica: 50 70
El mensaje cifrado es: 70 0 0 50 70 120 70 70 70 50 70 70 70 50 120 50 70 50 120 120 70 120 0 120 0 50 0 0 70 50 70 0 120 0 0 120 50 50 120 70 70 50 0 70 70 120 0 120 0 50 0 0 7
0 0 120 70 70 50 0 70 70 120 0 50 70 50 50 70 70 50 120 120 0 50 120 0 0 50 0 0 120 0 0 50 50 120 120 120 70 120 0 70 70 120 70 70 120 0 0 120 50 50 50 70 0 50 0 0 70 120 70 0 7
0 50 0 70 70 50 120 0 0 50 0 0 70 50 0 70 70 120 50 70 70 50 70 70 70 120 0 50 0 50 0 0 70 50 120 0 70 50 0 70 0 50 0 0 70 120 0 0 70 50 70 70 70 120 0 120 70 50 0 120 70 50 0 7
0 70 120 0 120 0 120 120 120

El mensaje original es: Buenos días Mario, ¿qué tal ayer la pescas?
```

```
Ahora probamos con una mochila de tamaño 4
El mensaje a cifrar es: Continuamos haciendo pruebas aumentando la mochila
El número N escogido es: 85
El número w escogido es: 11
La mochila escogida como clave privada es: 1 15 20 45

Clave publica: 11 80 50 70
El mensaje cifrado es: 80 120 130 211 130 141 200 80 130 81 130 141 200 150 130 70 130 161 130 211 200 120 50 0 130 11 130 70 130 120 130 81 130 150 130 141 130 80 130 211 50 0
200 0 200 50 200 150 130 150 130 50 130 70 200 120 50 0 130 70 200 150 130 161 130 150 130 141 200 80 130 70 130 141 130 80 130 211 50 0 130 91 130 70 50 0 130 161 130 211 130 1
20 130 11 130 81 130 91 130 70

El mensaje original es: Continuamos haciendo pruebas aumentando la mochila
```

```
El mensaje a cifrar es: Parece que con 4 elementos la mochila sigue funcionando bien :)
El número N escogido es: 1500
El número w escogido es: 11
La mochila escogida como clave privada es: 15 20 45 85

Clave publica: 165 220 495 935
El mensaje cifrado es: 1155 0 715 935 1650 495 715 1155 715 1430 715 1155 495 0 1650 935 1650 1155 715 1155 495 0 715 1430 715 1815 715 880 495 0 1430 220 495 0 715 1155 715 385
 715 1155 715 1320 715 1155 715 880 1650 220 715 1815 1650 1430 495 0 715 385 715 935 495 0 715 1320 715 1815 715 1430 715 165 715 1100 715 385 715 935 495 0 1650 1430 715 1100
715 1650 1650 1155 715 1155 495 0 715 715 1650 1155 715 880 715 1430 715 1100 715 1815 715 880 715 935 715 880 715 220 715 1815 495 0 715 495 715 1100 715 1155 715 880 495 0 143
0 660 495 1100

El mensaje original es: Parece que con 4 elementos la mochila sigue funcionando bien :)
```

```
Ahora probamos con una mochila de tamaño 8
El mensaje a cifrar es: Empezamos las pruebas con el máximo tamaño de la mochila
El número N escogido es: 1500
El número w escogido es: 11
La mochila escogida como clave privada es: 1 15 20 45 85 170 340 700

Clave publica: 11 165 220 495 935 370 740 200
El mensaje cifrado es: 735 1890 880 955 2555 585 1890 2630 1820 220 1690 585 1820 220 880 1620 1450 955 1125 585 1820 220 1325 2630 2430 220 955 1690 220 1890 1116 431 1815 1520
 1890 2630 220 1250 585 1890 585 1116 926 2630 220 755 955 220 1690 585 220 1890 2630 1325 1320 1520 1690 585

El mensaje original es: Empezamos las pruebas con el máximo tamaño de la mochila
```

```
El mensaje a cifrar es: Esta es la última prueba del script, ¿irá todo bien?
El número N escogido es: 1500
El número w escogido es: 11
La mochila escogida como clave privada es: 1 15 20 45 85 170 340 700

Clave publica: 11 165 220 495 935 370 740 200
El mensaje cifrado es: 735 1820 1250 585 220 955 1820 220 1690 585 220 1116 2401 1690 1250 1520 1890 585 220 880 1620 1450 955 1125 585 220 755 955 1690 220 1820 1325 1620 1520
880 1250 1525 220 916 2971 1520 1620 1116 431 220 1250 2630 755 2630 220 1125 1520 955 2430 2960

El mensaje original es: Esta es la última prueba del script, ¿irá todo bien?
```

Análisis de los resultados:

Como podemos observar en las imágenes adjuntadas en la página anterior los mensajes obtenidos tras el descifrado son equivalentes a los introducidos como parámetro de la función inicialmente. Pasamos a analizar el rendimiento del programa.

Número de Prueba	Tiempo Cifrado (s)	Tiempo Descifrado (s)	Tiempo Total (s)
Prueba 1	0.0001653	0.0002156	0.0048821
Prueba 2 con tildes	0.0001053	0.0007942	0.0033572
Prueba 2 sin tildes	0.0001862	0.000153	0.0049726
Prueba 3	0.0001476	0.000578	0.0038001
Prueba 4	0.0001161	0.0005323	0.0059481
Prueba 5	0.0001264	0.0007334	0.0057732
Prueba 6	0.0001933	0.0007187	0.0054415

Vemos que al hacer uso de métodos sencillos pero eficientes el tiempo que se tarda en realizar tanto el cifrado como el descifrado del mensaje es bajo en comparación con el tiempo total de ejecución del fichero.

Esto no es preocupante ya que debido a la necesidad de comprobar que se cumplian todas las condiciones necesarias para realizar el algoritmo inicialmente se debían realizar varias funciones con bucles que podían contener bastantes iteraciones, como es recorrer toda la mochila para comprobar que N es un número superior o comprobar que w es un número primo. Además de los mensajes que se sacan por terminal para poder hacer un seguimiento del algoritmo con los cuales es necesario recorrer vectores completos.

Otro dato relevante es el crecimiento de los tiempos de cifrado y descifrado de los mensajes. El primero de los tiempos se mantiene más o menos constante parece en todos los casos independientemente del tamaño de la mochila tardar de media 150 microsegundos, en cambio, los resultados del tiempo de descifrado va aumentando conforme se añaden elementos a la clave privada del usuario. Esto se puede deber a que el algoritmo de cifrado utilizado como se ha nombrado anteriormente hace uso de operaciones de máscara de bits que el procesador es capaz de realizar en un único ciclo.

Por el contrario, el tiempo de descifrado aumenta conforme la mochila va aumentando de tamaño, esto se debe a que es un algoritmo lineal en el número de componentes ya que en el descifrado se deben recorrer la mayoría de números de la clave privada para comprobar si pueden o no ser incluidos en el número C que se está descifrando en la iteración en cuestión.

Un dato curiosos es la gran diferencia existente entre el descifrado de cadenas con tildes y sin tildes, ya que vemos que el tiempo es mucho mayor, esto seguramente se debe a que son carácteres en UTF-8 y no son básicos del sistema