Universidad Simón Bolívar
División de Ciencias Físicas y Matemáticas
Departamento de Computación y Tecnología de la Información
Caracas, Venezuela

Sartenejas, 08 de febrero del 2019

Tarea: descifrado

¡El imperio nos ataca! El Ejército Imperial Napoleónico ha tomado Castilla y, respaldado por el ilegalmente nombrado Consejo de Castilla, ha nombrado como rey a José Bonaparte, usurpando el poder Su Legítima Majestad Fernando VII.

Sin embargo, la real Junta de Gobierno permanece en funciones, y ha recibido información de que Napoleón se comunica con sus tropas utilizando mensajes encriptados con un sencillo cifrado de sustitución transmitidos por telégrafo óptico. El esquema de cifrado cambia periódicamente, por lo que debe desarrollarse un algoritmo que permita a los criptoanalistas patriotas no sólo descifrarlos, sino también identificar cuándo cambia, utilizando los mensajes que vayan llegando. La Junta de Gobierno contínuamente recibe el descifrado de varios mensajes gracias a el creciente número de desertores del Consejo de Castilla.

Varios de los operadores de telégrafo óptico se han sumado a la causa, y han aceptado transmitir mensajes de desinformación al Ejército Imperial Francés, pero deben llevárseles ya cifrados, por lo que también debe desarrollar un algoritmo de cifrado.

La Junta de Gobierno ha llamado al pueblo a tomar las armas contra los invasores franceses, pero la revolución sólo podrá tener éxito si se pueden interceptar y descifrar el mayor número de mensajes posibles. ¡En sus manos está que nuestra bandera ondee de nuevo sobre el Palacio de Gobierno!

Requerimientos del programa

Desarrolle un programa interactivo que permita:

- Registrar nuevos mensajes cifrados y sus descifrados
- Descifrar mensajes
- Cifrar mensajes
- Mostrar un esquema de cifrado
- Borrar un esquema de cifrado debido a un error

Las primeras tres opciones deben seguir recibiendo mensajes hasta que el usuario escriba un símbolo numeral (#).

Si un mensaje nuevo no coincide con el esquema de cifrado registrado, se debe indicar que el mismo ha cambiado. Debe mantenerse almacenado el cifrado anterior en caso de que se reciba un mensaje a descifrar con esa fecha. Si alguna letra no se puede cifrar o descifrar, se debe indicar con un signo numeral (#) dejando en manos del redactor escribir un mensaje que no utilice esa letra.

Así, si se recibe el siguiente mensaje:

Fecha: 26 de septiembre de 1807
Cifrado: ULEKNT!ZZL OFDAFQL QK BR!XPIW DHK G!JHMLSF K,R!VKY
Descifrado: JOVENCILLO ZAMPADO DE WHISKY, QUE FIGUROTA EXHIBE!

Se sabrá que el esquema de cifrado es

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	,	!
F	V	T	Q	K	G	J	R	!	U	P	Z	D	N	L	A	D	M	X	S	H	E	B	,	I	O	W	Y

En este ejemplo, “JOVENCILLO” queda cifrado como “ULEKNT!ZZL”. Según el esquema de cifrado, U se es el cifrado de J, L de O, etc. Para obtener el mensaje original utilizamos el mismo esquema, pero en dirección opuesta. Es decir, partiendo “ULEKNT!ZZL”, J es el descifrado de U, O de L y así sucesivamente. Claro, este ejemplo deliberadamente contiene todas las letras. Napoleón nunca enviará un mensaje así.

Cabe destacar que los franceses, como herencia de la revolución francesa, no respetan a la Real Academia de la Lengua, por lo que siguen denotando la Ñ como NN, omiten los acentos, y no usan los signos de interrogación ni exclamación de apertura (¡ ni ¿). Los espacios siempre serán espacios en el cifrado, ya que son introducidos por el transcriptor como interpretación de pausas en la transmisión. Los mensajes siempre se transmiten en mayúsculas por limitaciones del telégrafo óptico.

Si se desea enviar un mensaje falso como “ABORTEN”, se puede usar este esquema de cifrado para convertirlo a “FVLMSKN”.

Sin embargo, si se registra el siguiente mensaje,

Fecha: 1 de enero de 1808
Cifrado: QKYLD MEENO
Descifrado: FELIZ ANNO!

Se sabrá que el esquema cambió. Si el mensaje “ABORTEN” se desea enviar posterior al 1 de enero de 1808, el algoritmo debe cifrarlo como “M#N##KE”. Sin embargo, es posible que se deba cifrar o descifrar un mensaje anterior al 1 de enero para saber por dónde vienen los invasores.

Si se recibe el mensaje

> Fecha: 25 de diciembre de 1807
> Cifrado: QKYLD EMTLXMXO
> Descifrado: FELIZ NAVIDAD!

se puede ver que este cifrado es consistente con el del 1 de enero, por lo que se puede actualizar la fecha del cambio, y así procesar mensajes que contengan la letra O en su descifrado (presente en el mensaje del 1 de enero pero no el del 25 de diciembre) enviados entre las dos fechas. Así, sabiendo a partir de qué fecha tiene validez cada esquema de cifrado, puede saberse qué esquema usar dado una fecha.

Funcionamiento del programa

Debe almacenar cada esquema como dos tablas de hash (una para cifrar y una para descifrar), ya que no se sabe qué símbolos se usen en el cifrado (Napoleón regularmente prohíbe letras y símbolos al cambiar el cifrado). Debe guardar el conjunto de esquemas de cifrados como una lista enlazada ordenada por fecha. Si un mensaje (del cual se conoce el cifrado y el descifrado) tiene una fecha entre la de dos esquemas de cifrado, y no es consistente con ninguno de los dos, debe agregarse un nuevo elemento a la lista en esa posición. Si un mensaje es consistente con ambos, debe preguntársele al usuario, el cual será un criptógrafo experto leal al legítimo Rey Fernando VII si desea agregarlo al anterior, siguiente, o crear un esquema de cifrado nuevo en esa posición.

Requisitos de la entrega

El código debe estar bien comentado, ya que va a ser ejecutado a mano por lo criptógrafos expertos leales a Fernando VII.

El programa será probado en las computadoras del LDC.

Debe entregar antes del 22 de febrero a las 11:59 pm en el Moodle del curso. Solo deberá efectuar una entrega por grupo.

Debe tener Makefile.

Distribución de Puntos

- 1 punto por su lista enlazada y funciones de acceso relacionadas
    - 0,5 puntos por código
    - 0,5 puntos por poder probarlo al ejecutar
- 1 punto por su tabla de hash y funciones de acceso relacionadas
    - 0,5 puntos por código
    - 0,5 puntos por poder probarlo al ejecutar
- 1 punto por su programa principal
    - 0,5 puntos por código
    - 0,5 puntos por como corre
- 1 punto por uso de malloc y free
    - 0,5 puntos por usarlos correctamente
    - 0,5 puntos por permitir que el programa siga ejecutando al ocurrir estas llamadas
- 1 punto por su makefile