

**ESCUELA SUPERIOR POLITECNICA DEL LITORAL**

**Organización de computadoras**

**Proyecto 1 Parcial**

**Integrantes:**

*Erick Cordova Gavilanes*

*Daysi Maroto Lema*

**CIFRADO GREY CM**

Programa que permite encriptar un mensaje en base a la combinación de varios métodos de cifrado, de forma que solo pueden comprenderse si se dispone del mismo programa para interpretar y descifrarla.

Para lograrlo, se le pide al usuario el mensaje y un código, el cual será el que identifique los tipos de cifrados a usar y le permitirá tener la variabilidad de encriptación para su mensaje.

Se aplica un cifrado principal predeterminado independiente de código, y adicionalmente 2 cifrados secundarios los cuales son seleccionados por el usuario e identificados por el código.

Dando como resultado la combinación de varios métodos de encriptación para un solo mensaje y la capacidad de generar diferentes mensajes encriptados representando la misma información, pero con diferentes niveles de cifrado.

**Código**

El código es una palabra de 3 caracteres conformada por 2 vocales y una letra la cual puede ser también consonante, cada carácter identifica el tipo de cifrado que se va a aplicar al mensaje o si no se lo va a aplicar.

Las 3 primeras vocales corresponden a los 2 cifrados secundarios opcionales y la tercera letra es un parámetro para el cifrado principal.

Ejemplo de código valido: *aei,uic,eim*

Ejemplo de código invalido: *bae, aci,ae2*

**Cifrado principal**

El cifrado principal es invariable y su elección no depende del código, se aplica directamente al mensaje original, usando como parámetro el ultimo carácter del código.

Se toma el parámetro, como el numero de saltos hacia adelante en el alfabeto que hay que avanzar, para identificar la letra que reemplazará al caracter original, de forma que cada letra del mensaje sea diferente y mantenga la misma cantidad de caracteres.

Por ejemplo en el código *“aea”,” oib”,”euz”,*  parámetro es “a”,”b” y “z” los cual se interpreta como su posición en el alfabeto de esa letra, así “a” es 1 y,“b” es 2 y “z” es 27 los saltos o letras que avanzaremos.

**Cifrado secundario**

Cada cifrado secundario va a tener 5 diferentes variantes, uno por cada vocal, de forma que se pueda escoger solamente una variante por encriptación, también es posible indicar que no se quiere aplicar un cifrado secundario usando la variante u.

La última variante u de cualquiera cifrado secundario indica que no se va a aplicar la variante de cifrado y se continua al próximo cifrado secundario.

Cada vocal en el código, excepto el ultimo carácter se refiere a una variante cifrado que se va a aplicar, en el código “aeb”

La *“a”* indica que variante del primer cifrado secundario se aplica, la *“e”* indica que variante del segundo cifrado secundario se aplica, la “*b*” no se usa en el cifrado secundario, corresponde al parámetro del cifrado principal.

**Definición de los cifrados secundarios y sus variantes**

Para el presento proyecto se definió solamente un cifrado secundario, donde dependiendo de la variante del cifrado, se realiza un desplazamiento parcial a la palabra de la siguiente forma:

**Cifrado Secundario A**

Se invierte la palabra por completo, desde el primer al último carácter

“abcdefghi” = > “ihgfedcba”

**Cifrado Secundario E**

Se invierte la palabra solo hasta la primera mitad, si la palabra es par se invierte hasta el índice medio empezando por 1

“abcdefg” => “cbadefg”

**Cifrado Secundario I**

Se invierte la palabra solo desde la segunda mitad, si la palabra es par se invierte desde índice medio empezando por 1

“abcdefg” => “abcdgfe”

**Cifrado Secundario O**

Se invierte la palabra solo desde la segunda mitad, si la palabra es par se invierte desde índice medio empezando por 1

**Cifrado Secundario U**

La variante u de todo cifrado secundario, indica que no se le aplica ningún cambio a la palabra.

“abcdefg” => “abcdefg”

**Proceso interno de cifrado**

Por cada método que se aplica, se agrega al mensaje cifrado el carácter del código, de forma que aumenta en uno el tamaño del mensaje.

El carácter del código principal se aplica al inicio del mensaje cifrado

Los caracteres de los códigos secundarios se aplican al final del mensaje cifrado.

**Ejemplo de aplicación del algoritmo**

Si el mensaje es “Me gustan los gatos” y el codigo “ouf” el proceso interno seria

***Cifrado principal****:*

F tiene la 6 posición en el alfabeto, así que se toman las letras 6 posiciones adelante a las originales y luego se añade la letra f al mensaje encriptado al inicio.

*“Me gustan los gatos” ->* “*Rk mayzgs quy mgzuy”->* “**f***Rk mayzgs quy mgzuy”*

***Cifrado secundario:***

Se aplican la variante “o” del cifrado secundario 1 y se agrega la “o” al final del mensaje cifrado

“f*Rk mayzgs quy mgzuy”-> “*hTm ñcabiu swa ñibwa*”-> “*hTm ñcabiu swa ñibwa**o***”*

Se aplican la variante “u” del cifrado secundario 2 y se agrega la “u” al final del mensaje cifrado

Recordemos que la variante u de cualquier cifrado secundario es la ausencia de este

*“*hTm ñcabiu swa ñibwao*”-> “*hTm ñcabiu swa ñibwao*”-> “*hTm ñcabiu swa ñibwao**u***”*

**Mensaje completamente cifrado**

*“Me gustan los gatos”-> “*hTm ñcabiu swa ñibwao**u***”*

# Referencias

Patterson, D. A., & Hennessy, J. L. (2013). *Computer Organization and Design MIPS Edition: The Hardware/Software Interface*. Newnes.

Kane, G. (1987). *mips R2000 RISC Architecture* (pp. 2-1). Englewood Cliffs, NJ: Prentice Hall.

Vollmar, K., & Sanderson, P. (2006, March). MARS: an education-oriented MIPS assembly language simulator. In *ACM SIGCSE Bulletin* (Vol. 38, No. 1, pp. 239-243). ACM.

Britton, R. L. (2004). *MIPS assembly language programming*. Pearson/Prentice Hall.