

Facultad de Ingeniería

Al

goritmos y Programación (BPT

SP05

)

Trimestre 1415

-

2

**Proyecto 2 Unidad II – Individual**

**Algoritmos y Programación BPTSP05**

Funciones, Parámetros, Recursividad y Arreglos

Efectué el análisis correspondiente para resolver el problema del Sistema de Cifrado “Vigenère”.

# Problema (20 puntos)

Desarrollar un programa estructurado (funciones) en Lenguaje C, que mediante la utilización de parámetros por valor y referencia, así como de arreglos unidimensionales y bidimensionales, y al menos 1 rutina recursiva, permita cifrar y descifrar un mensaje mediante el sistema de cifrado de Vigenère.

**Descripción General:** El criptosistema de Vigenère, también llamado el sistema de cifrado de Vigenère (en honor al criptógrafo francés del mismo nombre), es un sistema polialfabético, es decir de sustitución múltiple. El principal elemento de este sistema es la llamada Tabla de Vigenère, la cual es una matriz cuadrada de caracteres (ver Ilustración 1 - Tabla Vigenère).

La clave del sistema de cifrado de Vigenère es una palabra escogida al azar y que generalmente suele tener sentido para que sea fácil de recordar. Cada una de las letras de la tabla corresponde con el alfabeto elegido de la tabla adjunta para cifrar el mensaje.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **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** |
| **A** | 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 |
| **B** | 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 | a |
| **C** | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b |
| **D** | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c |
| **E** | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d |
| **F** | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e |
| **G** | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f |
| **H** | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g |
| **I** | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h |
| **J** | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i |
| **K** | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j |
| **L** | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k |
| **M** | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l |
| **N** | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m |
| **O** | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n |
| **P** | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o |
| **Q** | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p |
| **R** | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q |
| **S** | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r |
| **T** | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s |
| **U** | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t |
| **V** | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u |
| **W** | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v |
| **X** | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w |
| **Y** | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x |
| **Z** | z | 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 |

**Ilustración 1 - Tabla Vigenère**

Febrero 2015 Pág 1

Preparado por Prof. Germán Biaggini



Facultad de Ingeniería

Al

goritmos y Programación (BPT

SP05

)

Trimestre 1415

-

2

Por ejemplo, si la clave es la palabra *sol*, se utilizaran los alfabetos de la tabla Vigenère correspondientes a los alfabetos S, O, y L de la tabla, es decir si el mensaje a ser cifrado fuera Paz y Amor, se buscaría la equivalencia de la letra “P” en la fila correspondiente a la primera letra de la clave dada la cual es para la “S” la letra “h”. La equivalencia de la segunda letra del mensaje (a), se buscaría en la fila correspondiente a la letra “O” (2da, letra de la clave), siendo el carácter la letra “o”. Para el resto de las letras del mensaje, se sigue el mismo procedimiento y cuando se llegue a la última letra de la palabra clave se vuelve a comenzar desde la primera. En definitiva el mensaje de Paz y Amor con clave SOL sería:

Clave=SOL

Mensaje= PazyAmor

Mensage Vigenère= hokqoxgf

El mensaje a cifrar o descifrar tendrá como máximo cuarenta (40) caracteres, sin separación entre palabras al momento de digitarlo, ni tampoco ningún otro carácter especial (ni ñ ni acentos). El carácter de fin de mensaje será el número cero (0), el cual no deberá ser tomado en cuenta bajo ninguna circunstancia en el mensaje.

El programa solicitará indicar si se quiere cifrar o descifrar, solicitará la clave a ser asignada, preguntará si se va a digitar el mensaje y en caso afirmativo y dependiendo si es cifrado o descifrado solicitará la secuencia de caracteres, para luego mostrar tanto el mensaje descifrado como el mensaje cifrado o viceversa. En caso de que se indique que no se desea digitar el mensaje, se deberá solitar la clave estando el mensaje pre-codificado en un arreglo unidimensional de 40 posiciones tipo char denominado para el caso de cifrado **men\_cif** o **men\_des** para el caso de descifrado. Ambos arreglos deberán estar presentes en el código e inicializados en blanco.

Febrero 2015 Pág 2

Preparado por Prof. Germán Biaggini