**Laboratorio de Sistemas Basados en Microprocesadores**

Práctica 4: Diseño de programas residentes.

## Cuadrado de Polibio

Inventado hacia 150 a. C. por el historiador Polibio, el cuadrado de Polibio se trata de un algoritmo trivial, donde cada letra del alfabeto es reemplazada por las coordenadas de su posición en un cuadrado. Es un caso particular de transposición mono-alfabética.

Polibio no concibió la tabla como un modo de escritura secreta sino como un medio de comunicarse a distancia por medio de antorchas, como una especie de telégrafo primitivo. En las prisiones de la Rusia zarista se utilizaba para comunicarse, mediante golpes en las paredes, una tabla similar a la de Polibio pero de seis números para poder contener el alfabeto cirílico.

La tabla de Polibio tiene tres características muy interesantes desde el punto de vista de la criptografía:

- En primer lugar sirve para transformar los caracteres alfabéticos en números lo que hace posible aplicar posteriormente transformaciones de tipo aritmético.
- En segundo lugar permite reducir el número de caracteres de 36 a 6 (originalmente de 25 a 5) lo que puede hacer más sencilla la transmisión del mensaje.
- Finalmente, a cada carácter le hace corresponder dos cifras que pueden ser manipuladas separadamente mediante técnicas de trasposición.

**Principio**

Tomamos una matriz cuadrada de Polibio relleno con un alfabeto:

| | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | A | B | C | D | E | F |
| 2 | G | H | I | J | K | L |
| 3 | M | N | O | P | Q | R |
| 4 | S | T | U | V | W | X |
| 5 | Y | Z | 0 | 1 | 2 | 3 |
| 6 | 4 | 5 | 6 | 7 | 8 | 9 |

Por ejemplo, la palabra Polibio se escribiría 34 33 26 23 12 23 33.
La matriz Polibio **deberá ser diferente para cada pareja**. P.e. para la pareja 1, la letra A deberá aparecer en la primera posición (11), para la pareja 2 en la segunda (12), etc

**Programa 1: p4a.asm (4 ptos)**

Diseñar un programa residente que instale un vector en la **INT 57h**, proporcionando servicios en **AH=10H**, para imprimir en pantalla la codificación de un string a código Polibio y **AH=11**, para imprimir en pantalla la decodificación de un string en código Polibio.
Las cadenas estarán en **DS:DX** y terminarán en **$.**

El programa a desarrollar sera de tipo .COM y deberá incluir lo siguiente:

- Implementar una rutina de servicio a la interrupción 57h, que ofrezca los servicios especificados anteriormente
- Cuando se ejecute sin parámetros, muestre el estado de instalación del driver, num de grupo (versión Polibio), nombres de la pareja y las instrucciones de uso.
- Cuando se ejecute con el parámetro /I, instale el driver caso que no lo esté ya
- Cuando se ejecute con el parámetro /D, desinstale el driver caso de estar instalado

**Programa 2: p4b.asm (3 ptos)**

Realizar un programa que muestre en pantalla la matriz Polibio utilizada y pruebe el funcionamiento del programa residente anterior mediante la codificación/decodificación de un mensaje predefinido.

## La interrupción periódica (1Ch)

El PC, con cierta electrónica de temporización, realiza una petición de interrupción al microprocesador a un ritmo aproximado de 18,2 veces por segundo. Esto permite al programador utilizar dicha interrupción cuando necesite realizar una tarea periódica. Esta interrupción es la interrupción hardware 08 cuya rutina de atención, además de ciertas tareas de control y mantenimiento, realiza una llamada a la interrupción software 1Ch.
Por defecto, el único contenido de la rutina de atención a esta interrupción es la instrucción IRET. Reinstalando los vectores de esta interrupción el programador puede realizar tareas periódicas sin más modificaciones.

**Programa 3 p4c.asm (3 ptos)**

Realizar un programa que, dada una cadena entrada desde el teclado, escriba en pantalla cada uno de los caracteres convertidos a código Polibio utilizando la interrupción definida en el apartado anterior, a un ritmo de un carácter por segundo, aproximadamente, **utilizando la interrupción 1Ch** para la temporización.
Se recomienda modificar el programa p4a.com para incluir la RSI del 1Ch.

Adicionalmente, **se solicita habilitar/deshabilitar las interrupciones** para instalar el driver, pero en lugar de usar CLI/STI, aplicar una inhibición/ desinhibición selectiva del **TIMER** modificando el bit 0 del registro de máscara (IMR) del controlador de interrupciones maestro. Para ello se recomienda usar **IN** para leer el registro con la ayuda de una máscara binaria para cambiar el bit de menos peso y un **OUT**para escribir el resultado.

Cuando se reciba la instrucción "**decod**", el programa deberá decodificar las cadenas siguientes, salvo que se reciba cod o quit.
Cuando se reciba la instrucción "**cod**", el programa deberá codificar las cadenas siguientes, salvo decod o quit.
Cuando se reciba la instrucción "**quit**" el programa deberá finalizar.

**ENTREGA DE LA PRÁCTICA: Fecha y contenido**

Un único miembro de la pareja deberá subir a Moodle un fichero zip incluyendo el número de pareja en el nombre (p. ej: 3_entregaP4.zip) y que contenga únicamente los ficheros fuente de los programas y el fichero makefile.
Los ficheros fuente deberán contener en los comentarios de cabecera los nombres de los autores y el identificador de la pareja.

El código generado deberá estar correctamente tabulado y comentado. La falta de comentarios o la baja calidad de éstos, será calificada negativamente.

**El límite de fecha de subida de los ficheros, para cada grupo es el siguiente:**

Grupos del Miércoles: 23 de Abril de 2019 a las 23:55h
Grupos del Viernes: 25 de Abril de 2019 a las 23:55h