

NOTA DE APLICACIÓN

PROYECTO CON dsPIC PARA LA ENCRIPCIÓN DE COMUNICACIONES

Autores:

*Jose M^a Angulo Usategui
Aritz Etxebarria Ruiz
Ignacio Angulo Martínez
Iván Trueba Parra*

Facultad de Ingeniería ESIDE de la Universidad de Deusto

CAPACITACIÓN EN EL DISEÑO CON dsPIC

Los dsPIC son microcontroladores avanzados PIC de 16 bits que integran los recursos de los DSP. Tienen un campo de aplicación muy extenso que cubre las tecnologías que precisan de las características específicas de los dsPIC.

El laboratorio PIC'School ha sido desarrollado por Ingeniería de Microsistemas Programados S.L. (www.microcontroladores.com) con el objetivo de facilitar el aprendizaje y el diseño de proyectos basados en cualquier tipo de microcontroladores PIC, desde los humildes enanos de 8 patitas hasta los modernos dsPIC. Para conseguirlo, además de la tarjeta PIC School existe una serie de módulos orientados a temas concretos. Así, el equipo base PIC School está dotado de un tutorial y un kit de componentes complementarios orientados al aprendizaje de los PIC16F87x y los PIC18FXXX. Otro módulo especial es el destinado a los dsPIC, que consta de los siguientes elementos:

- Libro “dsPIC. Diseño Práctico de Aplicaciones”, de la Editorial Mc Graw-Hill, 2006. En él se explica la arquitectura y programación de los dsPIC y se ofrece una extensa colección de programas y prácticas para la PIC School.*
- Dispositivo dsPIC30F4013 con zócalo para la PIC School.*
- Motor de cc, circuito integrado controlador de pantallas LCD SYM-20AA y material complementario para el montaje de los experimentos sobre el laboratorio PIC School*
- Tutorial de Prácticas con los programas fuente en Ensamblador y en C, software y documentación técnica.*



Figura 1.- Fotografía del sistema de desarrollo PIC School. Cortesía de Ingeniería de Microsistemas Programados S.L..

Los dsPIC de Microchip son microcontroladores avanzados que contienen un motor DSP que añade al repertorio de instrucciones habitual un conjunto de 19 instrucciones DSP capaces de resolver aplicaciones complejas en los campos de la imagen y el sonido, el tratamiento matemático, los filtros, etc..

Con el módulo dsPIC y la PIC School el usuario podrá dominar en poco tiempo todas las posibilidades de estos potentes dispositivos mediante la realización de una serie de proyectos didácticos y reales entre los que se encuentra el que se describe a continuación.

ENCRIPCIÓN DE DATOS CON dsPIC

Se propone comunicar un dsPIC30F4013 con un computador empleando el puerto serie del PC. Se utiliza el hardware de comunicaciones USART disponible en el dsPIC y que permite realizar este tipo de comunicación sin emplear recursos de la CPU. Los objetivos de esta experiencia son los siguientes:

- Configurar correctamente el dsPIC30F4013 para el envío y recepción de datos por el puerto serie
- Utilizar el motor DSP para realizar una encriptación de los datos en las comunicaciones.

Para visualizar los datos enviados desde el dsPIC en el PC se puede utilizar cualquier programa terminal de comunicaciones, como el software Hyperterminal que se encuentra en la carpeta Accesorios / Comunicaciones del sistema operativo Windows.

Aprovechando las posibilidades matemáticas de los dsPIC se pueden desarrollar mecanismos de encriptación de comunicaciones mucho más avanzados que con un microcontrolador MCU. Con un

microcontrolador, para codificar un dato rápidamente se le puede sumar o restar una cantidad fija, que solo sea conocida por el equipo con el que se establece comunicación.

Por ejemplo, si se quiere enviar el carácter ASCII “z”, correspondiente al código ASCII 122, se le puede sumar una cantidad de forma que al transmitir el dato no pueda ser reconocido. El equipo receptor deberá restar la misma cantidad al recibir el dato para descryptarlo y convertirlo en un carácter legible. Esto se aplicará a todos los datos transferidos. Sin embargo, un simple desplazamiento de datos a través de sumas y restas es una protección muy sencilla, que puede ser fácilmente descubierta por un programa que pruebe a restar y sumar cifras hasta localizar cadenas de información válidas.

Con un dsPIC es posible complicar mucho la encriptación ya que las operaciones matemáticas que se pueden ejecutar a gran velocidad son mucho más complejas que las sumas o restas de un microcontrolador MCU. Por ejemplo, podemos elevar al cuadrado un dato, dividirlo entre una cantidad y después enviar dos datos, el cociente y el resto de la división. Para poder descryptar esta información, habría que conocer que hay 2 datos en transmisión por cada dato enviado, que está previamente elevado al cuadrado y luego desglosado entre cociente y resto de una división, que en el caso de esta experiencia tendrá el divisor 100.

En la aplicación el dsPIC esperará la recepción de un carácter ASCII por el puerto serie. Una vez recibido el dato, lo reenviará hacia el PC a modo de ECO y hacia una pantalla LCD pero aplicando antes una codificación para encriptar los datos. Las comunicaciones se realizan a una velocidad de 9600 baudios, 8 bits de datos y con 1 bit de stop. Estos parámetros de la comunicación hay que tenerlos en cuenta a la hora de configurar el dsPIC, ya que la comunicación por el puerto serie es de tipo asíncrono y es necesario que los dos equipos conozcan previamente estos parámetros.

El programa se repite de forma indefinida en un bucle. Se espera a la recepción de un dato del ordenador. Cuando llegue el dato se aplica el algoritmo de encriptación que consiste en elevarlo al cuadrado y dividirlo entre 100. Tras realizar esta operación tenemos un cociente y un resto, ambos de 8 bits. Estos dos datos son reenviados hacia el PC y se mostrarán en la pantalla del ordenador.

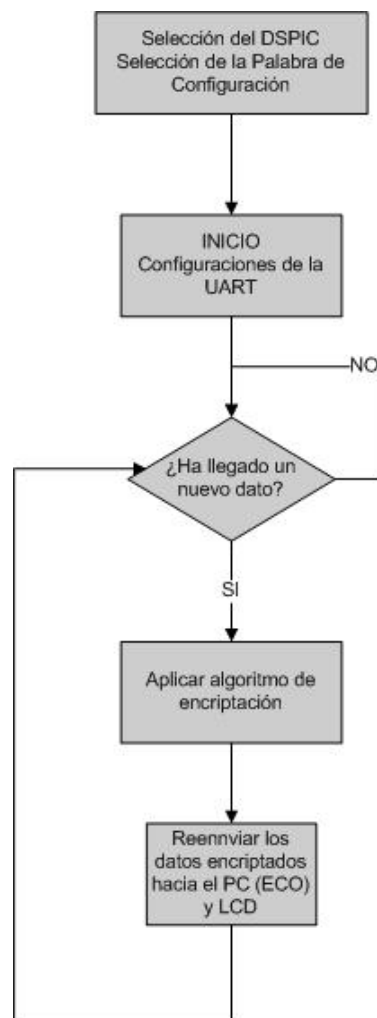


Figura 2. Organigrama de la práctica de transferencia de datos encriptados.

ESQUEMA ELECTRÓNICO

El hardware necesario para la implementación de esta aplicación se encuentra en la tarjeta PIC School, distribuida por Ingeniería de Microsistemas Programados S.L. (www.microcontroladores.com).

Para mostrar los mensajes en la pantalla LCD de la PIC School se utiliza un circuito conversor de serie a LCD. Este controlador serie SYM 20-AA requiere de las conexiones reflejadas en la Figura 3 entorno a la pantalla LCD.

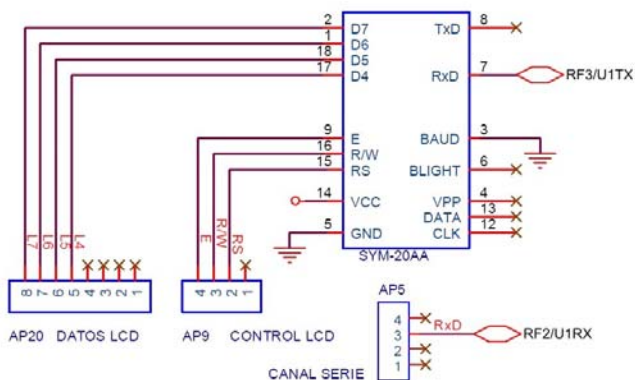


Figura 3. Esquema electrónico de la aplicación.

Las patitas 25 y 26 del dsPIC, en las que se encuentran las salidas hardware de la USART, serán las utilizadas en esta experiencia. Para probar las comunicaciones y poner en marcha la práctica hay que conectar la tarjeta PIC School al ordenador empleando un cable para el puerto serie que disponga de un terminal DB9 hembra en un extremo y un DB9 macho en el otro. Los conectores tipo DB9 son el estándar más extendido en las comunicaciones por el puerto serie. Es el mismo tipo de cable que se utiliza para programar los dsPIC a través del programa WinPIC800. Así, se usa el mismo cable de la siguiente manera: Primero se programa el microcontrolador y una vez programado, en segundo lugar, antes de pasar a modo "RUN" se cambia el cable de posición en la PIC School, conectándolo al interfaz RS-232 para poder observar el funcionamiento de dicho laboratorio.

CONSTRUCCIÓN DEL PROGRAMA

El programa comienza configurando el hardware de las comunicaciones y a las patitas R1X y T1X del dsPIC. La primera de ellas debe configurarse como entrada digital para poder recibir los datos y la segunda como salida. Es necesario acceder a los registros de control de la USART para activar la comunicación a la velocidad adecuada.

Una vez configurado el chip, el programa queda a la espera de recibir un nuevo carácter por el puerto serie, evento que es detectado por la USART. Cuando llegue el nuevo dato, se descarga y se aplica el algoritmo de cifrado para reenviarlo. Hay que destacar que la comunicación es full-duplex, de modo que si se recibe un nuevo dato mientras se está enviando la respuesta anterior también es almacenado en el buffer de recepción de la USART.

```
.include "p30f4013.inc"
.global __U1RXInterrupt

__U1RXInterrupt:
    BCLR    IFS0,#U1RXIF    ;Tratamiento de interrupción de recepción
    MOV     U1RXREG,W7      ;de dato. Primero se borra el flan de int.
    MPY    W7*W7,A          ;Se mueve a W7 el dato recibido
    MOV     ACCAL,W2        ;Se eleva al cuadrado dicho dato
    MOV     #0x0064,W3      ;Se mueve a W2
    REPEAT #17             ;Se divide entre 100
    DIV.U   W2,W3           ;Se transmite el resultado de la división
    CALL    TRANSMITE
    MOV     W1,W0           ;Se transmite el resto de la división
    CALL    TRANSMITE
    RETFIE

.global _main

_main:
    BSET    CORCON,#0x0    ;Trabajo con enteros
    CALL    INICIAUART     ;Inicialización modulo UART

bucle:
    CLRWDT    ;Se espera en un bucle infinito
    GOTO bucle ; a que se dé una interrupción por llegada
                ;de un carácter

INICIAUART:
    CLR     U1BRG          ;Se inicializa U1BREG para transmisión
    MOV     #0x0019,W0    ;a 9600 baudios con un reloj de 4Mhz
    MOV     W0,U1BRG
    MOV     #0x8000, W0    ;Se habilita la recepción de datos
    MOV     W0, U1MODE
    MOV     #0x0510, W0
    MOV     W0, U1STA
    MOV     #0x8020, W0    ;Se habilita el módulo
    MOV     W0, U1MODE
    MOV     #0x0200, W0    ;Se habilita interrupción por recepción
    MOV     W0, IEC0
    CLR     IEC1
    CLR     IEC2
    RETURN

TRANSMITE:
    BTSS    U1STA,#8      ;Rutina que envía un carácter
    BRA     TRANSMITE     ;Espera a estar disponible
    MOV     W0,U1TXREG    ;Envía el dato a través de U1TXREG

    RETURN
end
```

Figura 4. Código fuente del programa.

GRABACIÓN Y EJECUCIÓN

Una vez abierto el proyecto y tras compilar y grabar el programa en la memoria del dsPIC mediante el uso del laboratorio PIC School y el software WinPIC800, se deberá ejecutar un programa de comunicación en el PC para poder enviar datos por el puerto serie y recibir las respuestas del dsPIC.

Una vez que el programa entra en ejecución todo carácter escrito con el teclado es enviado por el puerto serie hacia la tarjeta PIC School. Cada vez que se reciba un carácter por el puerto es mostrado en la

pantalla. Se puede seleccionar en el menú de configuración del Hyperterminal la opción ECO de los caracteres escritos localmente, que sirve para que veamos en la pantalla los caracteres que estamos tecleando y están siendo enviados hacia el dsPIC. En la pantalla principal hay 2 iconos con los que iniciar y detener la comunicación, que tienen la forma de un teléfono colgado y un teléfono descolgado respectivamente.

Tras grabar el dsPIC, se pulsará el botón de Reset para comenzar la ejecución de la experiencia. Al teclear un carácter en el programa Hyperterminal de Windows se reciben dos caracteres en la pantalla del ordenador y en la pantalla LCD, que es un resultado ECO del carácter enviado pero encriptado. Se puede probar a realizar

manualmente la operación de descryptación y así comprobar que las operaciones son realizadas correctamente por el dsPIC. Todo carácter ASCII recibido tiene un valor asignado entre 0 y 255 que puede ser consultado en una tabla estándar de códigos ASCII o en el programa Mapa de Caracteres de las Herramientas del sistema operativo Windows.

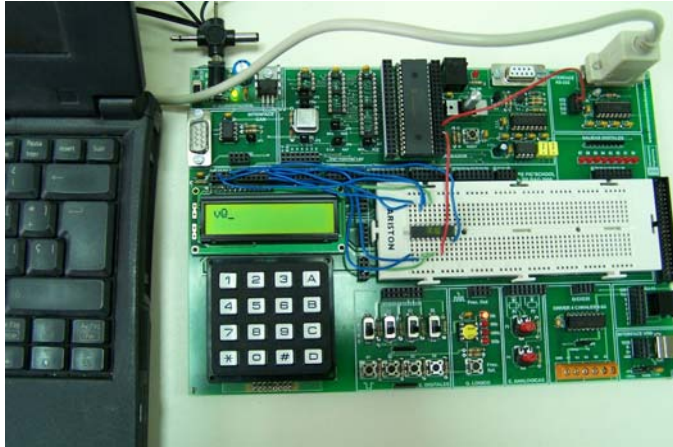


Figura 5. Sistema PIC School conectado al puerto serie de un ordenador y con la experiencia en ejecución.

Como ejemplo se ha tecleado en el ordenador la letra m que se corresponde con el código ASCII 109. El resultado de elevar 109 al cuadrado da 11881. Al dividir 11881 entre 100, el resultado es de 118 y resto 81, que se corresponden con los caracteres v y Q respectivamente, que aparecen sobre la pantalla LCD de la Figura 5.

CONCLUSIONES

Los actuales técnicos, profesionales y diseñadores de sistemas con microcontroladores PIC van a poder desarrollar con suma facilidad aplicaciones con dsPIC gracias al esfuerzo que ha dedicado su fabricante Microchip en simplificar y homogeneizar el hardware y el software que rodean a los nuevos dispositivos y a herramientas tan sencillas y asequibles como la PIC School y libros como los que se citan en la bibliografía.

BIBLIOGRAFÍA

“dsPIC: Diseño práctico de aplicaciones” Jose M^a Angulo Usategui, Aritza Etxebarria Ruiz, Ignacio Angulo Martínez e Iván Trueba Parra. Editorial Mc-Graw Hill 2006.

“Microcontroladores Avanzados dsPIC”, Angulo, JM, García, B. , Angulo, I. y Vicente, J.. Editorial Thomson, 2006.

“Comunicación encriptada con dsPIC”, Angulo J.M^a, Etxebarria, A., Angulo I. y Trueba, I., Revista Española

de Electrónica, Mayo/Junio 2006

DIRECCIONES DE INTERES

Microchip Technology Inc.

<http://www.microchip.com>

Ingeniería de Microsistemas Programados S.L:

<http://www.microcontroladores.com>