Embedded Systems Design

EECE 4038C, Embedded System Design

Ranga Vemuri

Laboratory Assignment – 5

Preparation:

1. Install MPLAB IDE. Read "A Basic Tutorial for MPLAB IDE" included with the software.
2. Read Chapters 1 and 2 in "44-Pin Demo Board User's Guide."
3. Keep "MPASM User Guide" handy. This is the user guide to the assembler.
4. Go through Lessons 1, 2 and 3 in Chapter 3 and execute the corresponding programs on the demo board with PIC 16F887.

Assignment:

Linear Feedback Shift Register (LFSRs) for Cryptography

LFSRs have numerous applications in pseudo-random number generation, cryptography, testing and other disciplines. An LFSR is a shift register whose input is a linear function of its previous state. This assignment asks you implement different LFSRs on your PIC demo board.

Read about LFSRs at https://en.wikipedia.org/wiki/Linear_feedback_shift_register. For the following designs, you may choose either the Fibonacci LFSR or the Galois LFSR.

1. Implement an 8-bit LFSR with suitable "taps". The 8-bit state of the LFSR should be presented on the 8 LEDs available on the board. State should change once every second.

   You should verify that your LFSR produces the entire cycle of 255 numbers before repeating. Verify this for a couple of initial states of the LFSR.

2. Implement the Alternating Step Generator (ASG) discussed at https://en.wikipedia.org/wiki/Alternating_step_generator. This requires that you implement three LFSRs (sizes 14, 15 and 16 bits respectively) and use one of them to control the other two.

   Present the output bit stream on the 8-LED panel as follows: Let b(t) be the output bit of the ASG at step t = 0, 1, 2 …. b(t) should be presented 8 bits at a time on the panel and the panel

should be updated at the rate of 1 Hz. That is, present b(7:0) for one second, then present b(15:8) over the next second, then present b(23:16) for the next second and so on.

You should verify that your ASG produces the correct output for the first 1024 bits of the output stream (ie. first 128 bytes on the LED panel) by comparing with the output of the C program given at the above site.

Submit a report with assembly program design and test information. Submit assembly programs.

In addition note that,

1. Your report must include a flow chart for your solution.
2. You must draw the circuit diagram and include a photograph of your circuit setup. You must describe the design decisions made during the circuit design process and any other alternative designs you have considered.
3. Your code must be well documented and must correspond to your flow chart.
4. You must use macros and subroutines wherever appropriate to improve modularity and maintainability of the code.
5. You must use a good template design for your program, following the coding practices you have noticed in your reading assignments.
6. You must discuss the algorithmic, circuit design and programming choices you have made while developing this solution.