

Name:

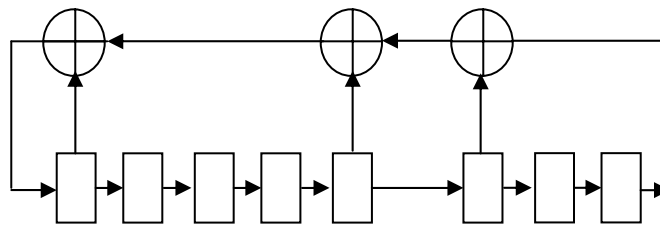
Id#

COE 205, Term 032

Computer Organization & Assembly Programming Programming Assignment# 3

Due date: Tuesday, May 4, 2004

You are required to write an 8086 assembly program to implement a pseudo random generator using Linear Feedback Shift Register (LFSR). An 8-bit LFSR is shown below:



The 8-bit LFSR shown above is guaranteed to generate a random sequence in the range from 1 to 255 before it repeats again. The register has to be initialized first by a seed, which can be any number other than 0. In your implementation use a seed of 10101010.

- (i) Write a subroutine, RAND8, that implements the pseudo random generator mentioned above. Every time RAND8 is called, it returns a new random number. The seed should be initialized outside the subroutine only once. The returned number should be stored on the stack.
- (ii) Write a subroutine that displays the content of an 8-bit register in decimal. The content of the register should be passed on the stack.
- (iii) Display in decimal using the subroutine in (i) the first 10 numbers generated by the above shown LFSR.
- (iv) Ask the user to enter a string of characters. Then, encrypt the string using RAND8 as follows. Each character is encrypted by XORing the least significant 4-bits of the ASCII code of the character with the least significant 4 bits of the generated random number. For example, assume the character to be encrypted is A=41H and the random number is AAH. Then, the encrypted character will have the ASCII code 4BH = K. As an example show the encryption of the string Hello COE-205!!. Then, rerun your program giving it the encrypted string and it should correctly decrypt it to Hello COE-205!!.

Make sure that your program is well documented. Provide a hard copy of the program and a soft copy of both the assembly code and the executable stored in a floppy disk.