Quiz 4

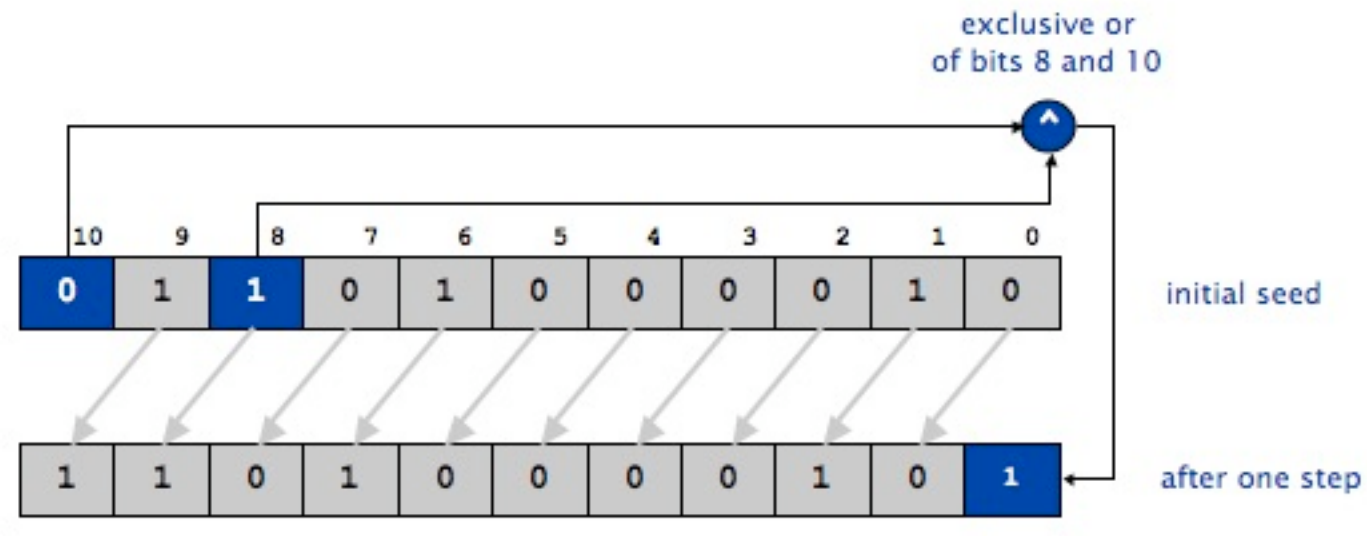
1 . Linear Feedback Shift Register (LFSR) Programming Assignment

Write a program that produces pseudo-random bits by simulating a linear feedback shift register, and then use it to implement a simple form of encryption for digital pictures.

LFSR review. A linear feedback shift register is a register of bits that performs discrete step operations that Shifts the bits one position to the left and

Replaces the vacated bit by the exclusive or of the bit shifted off and the bit previously at a given tap position in the register.

A LFSR has three parameters that characterize the sequence of bits it produces: the number of bits N, the initial seed (the sequence of bits that initializes the register), and the the tap position tap. As in the example in our lecture, the following illustrates one step of an 11-bit LFSR with initial seed 01101000010 and tap position 8.



One step of an 11-bit LFSR with initial seed 01101000010 and tap at position 8

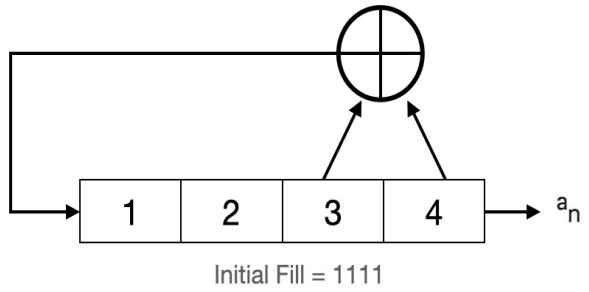
should output

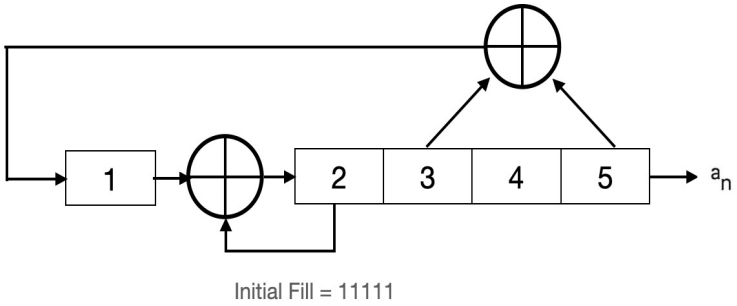
11010000101 1
10100001011 1
01000010110 0
10000101100 0
00001011001 1
00010110010 0
00101100100 0
01011001001 1
10110010010 0
01100100100 0

Extra credit takes as input the picture pipe.png and encrypted then recovery to plaintext

https://www.cs.princeton.edu/courses/archive/spr15/cos126/assignments/lfsr.html

2. Using the initial fills indicated, find and compare the output sequences for the following two shift register generators





3. Does the first shift register generator produce a maximal length linear recursive sequence?

4. What is the maximal length of a linear recursive sequence generated by a seven stage shift register generator?

5. Find the output sequences of the following shift-register generator using the following initial fills:

a. Initial fill 1000

b. Initial fill 1111

c. Initial fill 0110

Are any of these sequences maximal length?