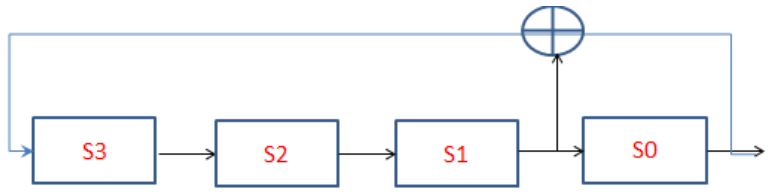
CSEC-462- Spring 2017

Homework 3 (Total 60 points)

Note: Include your explanations to the questions and show all the intermediate steps appropriately.

1. We will now analyze a pseudorandom number sequence generated by a LFSR characterized by (p2 = 1, p1 = 0, p0 = 1. This is the tap sequence).
   a. What is the sequence generated from the initialization vector (s2 = 1, s1 = 0, s0 = 0)? (6 points)
   b. What is the sequence generated from the initialization vector (s2 = 0, s1 = 1, s0 = 1)? (6 points)
2. Question: What is the polynomial representation of the LFSR of degree m = 4 and the feedback coefficients p3 = 1, p2=1, p1=1, p0=1? (5 points)
3. Based on the following figure, what are the values for ***m*** and the feedback coefficients p_i ? (5 points)



4. Draw the corresponding LFSR for each of the three polynomials. Determine the sequences generated by: (12 points; 4 + 4 + points)
   a. $x^4 + x + 1$
   b. $x^4 + x^2 + 1$
   c. $X^4 + x^3 + x^2 + x + 1$
5. If we take the linear congruential algorithm with an additive component of 0 (i.e. c = 0)
   $X_{n+1} = (aX_n) \mod m$
   Then it can be shown that if *m* is prime and if a given value of *a* produces a maximum period of *m*-1, then a^k will also produce the maximum period **provided that *k* is less than *m* and *k* and *m* -1 are relatively prime**. Show this statement is true by using $X_0 = 1$ and *m* = 5 and producing sequences for a^k = 3, 3^2, and 3^3 . (Total 9 points (3 + 3 + 3)
6. With linear congruential algorithm, some parameters that provide full period do not necessarily provide a good random sequence as we saw in class lecture. For example consider the following two generators: (Total 10 points; 5 + 5 points)
   a. $X_{n+1} = (6X_n) \mod 13$
   b. $X_{n+1} = (7X_n) \mod 13$
   Start with an initial seed of 1. Write out the two sequences to show that both are full period (that is upto *m*-1, where *m* = 13). Which appear more random to you? Why?
7. Using the Blum Blum Shub (BBS) pseudorandom number generator algorithm below, generate the binary digits.
   What is the maximum period of sequence before numbers starts repeating? (7 points)

Use the following values:

$p = 7$, $q = 11$

$n = p * q$

S is the seed, which is a random number relatively prime to n.

$S = 4$

$X_0 = S^2 \bmod n$

for i = 1 to 10

$X_i = (X_{i-1})^2 \bmod n$

$B_i = X_i \bmod 2$