HW # 2
Due: September 24, 2012

1. Determine the *linear complexities* of each of the following sequences:

   (a) `0101010101`

   (b) `011001100110`

   (c) `011011011011011`

   (d) `1011010010110`

2. We conduct a known plaintext attack on an LFSR-based stream cipher. We know that the plain text sent was (starting with the left-most bit):

   `1001 0010 0110 1101 1001 0010 0110`

   By tapping the channel we observe the following stream:

   `1011 1100 0011 0001 0010 1011 0001`

   (a) What is the degree m of the stream generator?

   (b) What is the initialization vector?

   (c) Determine the feedback coefficients of the LFSR.

   (d) Draw a circuit diagram and verify the output sequence of the LFSR.

3. In class we discussed stream ciphers and studied LFSRs as an early proposal for use as PRNGs. It turned out that LFSRs give extremely weak PRNGs. What happens if we use two separate maximal length LFSRs whose outputs are XOR-ed together to form the PRNG output? Does this approach significantly improve over using a single LFSR? If not prove your answer. For simplicity assume the lengths of the LFSRs are identical.

4. In this problem we consider advanced stream ciphers that are built by combining individual LFSRs. Such ciphers can be secure. We consider the alternating stop-and-go generator. The three LFSRs are specified by the following polynomials and combined in the typical stop-and-go generator configuration with initial vectors:

   LFSR-1 $x^2 + x + 1$; $(z_0 = 1; 0)$
   LFSR-2 $x^3 + x + 1$; $(z_0 = 1; 0; 0)$
   LFSR-3 $x^5 + x^2 + 1$; $(z_0 = 1; 0; 0; 0; 0)$

   (a) Draw the circuit diagram of the stream cipher.

   (b) Compute the first eight output bits.

(c) It generally holds for stream ciphers build from LFSRs that the sequence length is the product of the sequence lengths of the individual LFSRs if the individual lengths are all relative prime. Is this condition fulfilled for the generator above? What is the length of the sequence generated?

5. In class we discussed stream ciphers and studied LFSRs as an early proposal for use as PRNGs. It turned out that LFSRs give extremely weak PRNGs. What happens if we use two separate maximal length LFSRs whose outputs are XOR-ed together to form the PRNG output? Does this approach significantly improve over using a single LFSR? If not prove your answer. For simplicity assume the lengths of the LFSRs are identical.