MATH 587/CSCE 557: HOMEWORK 7, DUE MAR 29.

1. (a) In ASCII, the letters A,B,C,...,Z are represented by $65, 66, 67, ..., 90$ respectively. Convert the word TALK into a bit stream by turning each letter in turn into an integer, turning the integers into binary (strings of 7 bits), and then juxtaposing the binary strings.

(b) Give the first 8 bits produced by the LFSR with the rule $x_{i+3} = x_i + x_{i+2} (i = 0, 1, 2, ...)$ and with $x_0 = 1, x_1 = 0, x_2 = 1$. What is its period?

(c) Encipher TALK using this LFSR.

2. Suppose the bit stream 0000010111 was generated by an LFSR. Could that register have as few as 3 cells? 5 cells?

3. The following ciphertext was obtained by using an LFSR:
01100010101110011101010001000110001010111001110101

Suppose the plaintext is known to begin with 100100100100100. Decrypt the ciphertext.