HOMEWORK 5, DUE OCT 19.

Be sure to include brief explanations. You will not get full credit if you give only the final answer.

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 converting each letter in turn into an integer using ASCII, 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 $x_n = x_{n-1} + x_{n-3}$ and with $x_1 = 1, x_2 = 0, x_3 = 1$. What is its period?

(c) Encrypt TALK using this LFSR.

2. Suppose the bit stream 1100000101 was generated by an LFSR. Could that register have as few as 3 cells? 5 cells?

3. The following ciphertext was obtained by using a periodic stream cipher:
01100010101110011101010001000110001010111001110101

Suppose the plaintext is known to begin with 100100100100100. Assuming the key stream is generated by an LFSR with as few cells as possible, decrypt the ciphertext. (The answer will be a bit stream- it's not in ASCII.)