Cryptology
Assignment 1

Due Friday, March 3, 2000.

Note that this is an actual assignment which must be approved in order to take the exam in June. You may not work with others on the assignment. It must be turned in by 10:15 on Friday, March 3. If it is late, it will not be accepted.

1. Do problem 1.11 in the textbook. It is not necessary to actually try your algorithm on the given cryptotext.

2. Suppose that you are able to obtain the cyphertext "01101010101101", and you learn that the first eight bits of the plaintext are "10111011". You know that the encryption was done with the aid of a linear feedback shift register over the field GF(2), with length four. Determine the linear feedback shift register and the remainder of the message.

3. Suppose that a keystream is produced by a linear feedback shift register with m stages and that the period is r. Suppose the first m bits of the sequence are all ones. What value does bit r have, and why? (Hint: Consider separately the case where $r = 1$.)

4. Are there any linear feedback shift register sequences where within one period, the number of zeros and the number of ones differs by more than one? Prove your answer.

Problems

To be discussed Monday, February 28, 2000.

Do problems 2.3, 2.4, 2.7 and 2.8 in the textbook.