# Cryptology
# Assignment 1

Due Friday, March 2, 2001.

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 2. If it is late, it will not be accepted.

1. Explain why there is no point to multiple round Vigenere encryption, if all of the keys are of the same length. Multiple round ecnryption is encryption several times, using a different key for each encryption. (The ciphertext round $i$ is the plaintext input to round $i+1$.

2. Suppose that you are able to obtain the cyphertext "01101010101101", and you learn that the first eight bits of the plaintext are "11011001". 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 $S$ is produced by a linear feedback shift register with $n$ stages (by a linear recurrence relation of degree $n$). Suppose the period is $2^n - 1$. Consider any positive integer $i$ and the following pairs of positions in $S$: $(S_i, S_{i+1}), (S_{i+1}, S_{i+2}), ..., (S_{i+2^n-3}, S_{i+2^n-2})), (S_{i+2^n-2}, S_{i+2^n-1}))$. How many of these pairs are such that $(S_j, S_{j+1}) = (1, 1)$? (In other words, how many times within one period does the pattern 11 appear?)

Prove that your answer is correct.

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 Wednesday, February 21, 2001.

Do problems 2.3, 2.7 and 2.8 in the textbook.

Suppose a cryptosystem has $P = \{a, b, c\}$, $C = \{1, 2, 3, 4\}$ and $K = \{K_1, K_2, K_3\}$.

The encryption rules are as follows:

| | $a$ | $b$ | $c$ |
|---|---|---|---|
| $K_1$ | 1 | 2 | 3 |
| $K_2$ | 4 | 3 | 2 |
| $K_3$ | 3 | 4 | 1 |

Suppose $p_K(K_i) = 1/3$ for $1 \leq i \leq 3$, $p_P(a) = 1/2$, $p_P(b) = 1/3$, and $p_P(c) = 1/6$.

**a.** Compute the probabilities $p_C(y)$ for all $y \in \{1, 2, 3, 4\}$.

**b.** Does this cryptosystem achieve perfect secrecy? Explain your answer.