Homework 1
Introduction to Information Security
Due Date: Feb 26, 2007 (Monday)

Note: You can talk to your classmates, instructor, and TA about the problems. However, unless stated otherwise, problems should be written individually. University of Wisconsin rules for academic misconduct apply.
Consider this as a warm-up homework. If you attended the lectures, these problems should be very easy.
In the homework "the Stallings book" refers to [2] and "the Handbook" refers to [1] (I have linked the Handbook to the class homepage. You can download it for free.)
Question 1 (15 points): Problem 2.1 from the Stallings book.

Question 2 (15 points): problem 2.4 from the Stallings book.

Question 3 (20 points): Let a, b, c, d, e, f be integers mod 26. Consider the following combination of the Hill and affine ciphers: Represent a block of plaintext as a pair $(x, y) \bmod 26$. The corresponding ciphertext (u, v) is

$$(x, y) \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} + (e, f) \quad \equiv \quad (u, v) (\mathrm{mod}\ 26)$$

Describe how to carry out a chosen plaintext attack on this system (with the goal of finding the key a, b, c, d, e, f). You should state explicitly what plain-texts you choose and how to recover the keys.

Question 4 (linearity, 10 points): Let f be a function that takes as its input a n-bit vector and returns a m-bit vector (we write this formally as f has type $\{0, 1\}^n \to \{0, 1\}^m$).
Part A: Define what it means for f to be linear.
Part B: Give an example of a linear and a non-linear function.

Question 5 (LFSR-based Stream cipher, 40 points):
Part A: Assume that the 4-stage LFSR shown in Figure 1 starts in the initial state 0110. Generate a key stream of length 8. Show all the steps.

Part B: What is the relationship between the i-th key k_i ($i \geq 5$) and the previously generated keys of the LFSR? Is this relationship linear? Justify your answer.

Part C: Alice and Bob are communicating using a stream cipher where the key stream is generated by a 4-stage LFSR. Oscar wants to crack the stream cipher (remember Oscar is always the bad guy) using a known plaintext attack. How long a plaintext (and the corresponding ciphertext) does Oscar need? Justify your answer.

Part D: The known plaintext attack described in Part (C) depends on the linearity of LFSR. One solution for that is to use a non-linear generator for keys. Read the *alternating-step generator* from the Handbook (page 209). Describe it in your own words. Answer the following question:

Why is the alternating-step generator non linear?

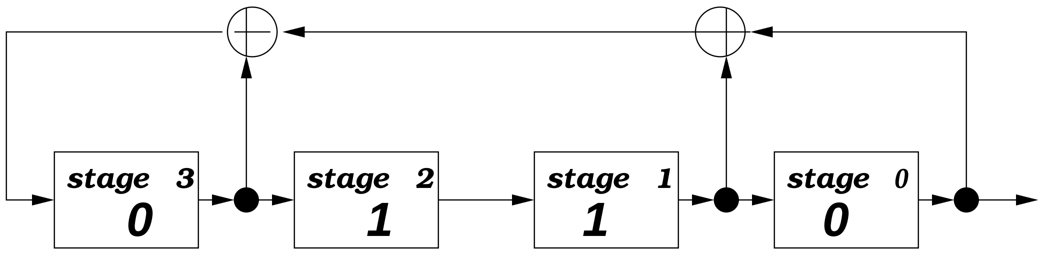

Figure 1: A 4-stage LFSR.

References

[1] A.J. Menezes, P.C. Van Oorschot, and S.A. Vanstone. *Handbook of Applied Cryptography*. CRC press, 1997.

[2] William Stallings. *Cryptography and Network Security: Principles and Practice*. Prentice Hall, 2006.