Homework 1
Introduction to Information Security
Due Date: Oct 4, 2010 (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.)
In the homework Boneh-Shoup refers to the draft I mentioned in class. I have been handing out chapters from this draft.
Question 1 (15 points): Read up on Hill Cipher form the Stallings book and then answer the following question. Eve captures Bob's Hill cipher machine, which uses a 2-by-2 matrix $M \mod 26$. She tries a chosen plaintext attack. She finds that the plaintext ba encrypts to HC and the plaintext zz encrypts to G. What is the matrix M?

Question 2 (15 points): Generalize the substitution cipher discussed in chapter 2 of Boneh-Shoup so that sequence of two letters is substituted (i.e., cd is replaced by xy). Does this cipher satisfy the perfect-secrecy criteria? Justify your answer.

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

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

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 n bits and outputs m bits (we write this formally as f has type $\{0,1\}^n \rightarrow \{0,1\}^m$).
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: Suppose Alice and Bob discard the first 5 outputs of the LFSR and use the rest as the key stream. How does this effect your answer to Part C?

Part E: Suppose we build an LFSR machine that works $\mod 3$ instead of $\mod 2$. It uses a recurrence of length 2 of the form

$$x_{n+2} \equiv c_0 x_n + c_1 x_{n+1} (\mod 3)$$

to generate the sequence $1, 1, 0, 2, 2, 0, 1, 1$. Setup and solve the matrix equation to find the coefficients c_0 and c_1.

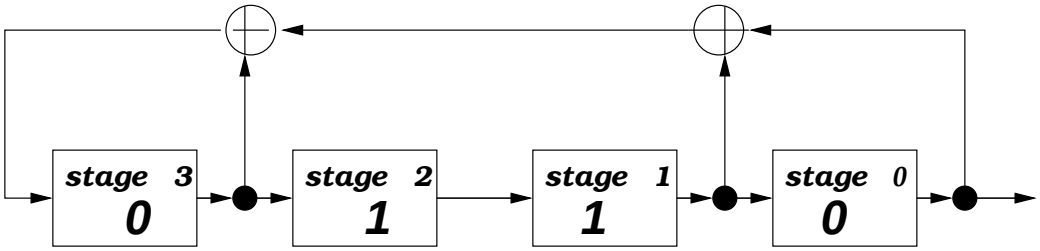

Figure 1: A 4-stage LFSR.

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.