Examination 1
Computer and Network Security
19 October, 1994

Instructions:

- Answer any five (5) questions below (graduate students may not answer question 1 and must answer the last two questions).
- Start the answer to a new question on a new piece of paper (that is, no more than one answer per page).
- Be sure to include your name on your answer sheets.
- This test is closed book, but you may use one 8.5 by 11 inch sheet of notes.
- You have 50 minutes to complete this examination.

1. Define and distinguish the following terms:
   (a) Exposure
   (b) Vulnerability
   (c) Threat
   (d) Attack
   (e) Control
   (f) Policy
2. (a) What is a permutation, mathematically speaking?
   (b) Describe two ways permutations are used in basic cryptography.
   (c) What is a one-to-one function (injection)?
   (d) What is an onto function (surjection)?
   (e) What do these properties of functions have to do with encryption?
3. (a) Contrast substitution ciphers and transposition ciphers.
   (b) Do substitution functions commute with each other? Do transpositions? Do transpositions and substitutions commute?
   (c) What is a one-time pad? Why is it considered a "perfect" cipher?
   (d) What is a Viginere Tableau and how is it used? What type of encipherment is this?
   (e) Describe the Vernam Cipher. What type of encryption is this?
4. (a) What are frequency of occurrance (FO) and index of coincidence (IC)? How are they related? How do they differ?
   (b) How would you use FO and IC to distinguish texts that had been enciphered using mono-alphabetic substitution, polyalphabetic substitution, and transposition?
   (c) What is Kasiski's Method, and how is it used?

5. (a) What principle(s) of encryption does substitution exemplify? How?
   (b) What principle(s) of encryption does transposition exemplify? How?
   (c) What are the Shannon Characteristics of a good cipher?
   (d) How does the violation of each of these characteristics lead to weaker ciphers?
   (e) Rate monoalphabetic substitution, transposition, and a combination of these with regard to the Shannon Characteristics.

6. (a) Distinguish block ciphers from stream ciphers.
   (b) What are the good point and bad points of block and stream ciphers?
   (c) Describe the ECB, CBC and CFB modes of DES.
   (d) What desirable properties do these various modes of DES have?

7. Let K_1 and K_2 be symmetric keys, M_1 and M_2 be plaintext messages, and let $C_1 = E(M_1, K_1)$.
   (a) Suppose we have K_2. How hard is it to find an M_2 such that $C_1 = E(M_2, K_2)$?
   (b) Suppose we have M_2. How hard is it to find an K_2 such that $C_1 = E(M_2, K_2)$?
   (c) Does this suggest a possible problem with the "oblivious transfer" (really, probabilistic transfer) protocol given in the text? (See attachment if your memory needs refreshment on this protocol) If so, how can you fix this protocol so that it no longer has this problem?
   (d) Why must Nancy send Peter K_N along with the message M if the message is a pre-arranged one?

8. (a) How are the "S-Puzzles" used in distributed contract signing?
   (b) How is oblivious transfer used? Why won't the probabilistic transfer called "oblivious transfer" described in the book work for this?
   (c) In the book, it says bits from only the first n keys are exchanged between the contract signers - why is this a problem?