Last Name, First Initial:

**Examination 2**

CEN 5540 Computer and Network Security

24 April 2001

Instructions:

- **Failure to follow instructions may result in loss of points.**
- Do not start the examination until instructed to do so.
- This test is closed book, but you may use one 8.5" by 11" sheet of notes you have prepared.
- **Answer two (2) questions below.**
- Start the answer to each question on a new page (i.e., do **not** put the answer to more than one question on the same page).
- Put the question number in the middle of the top of each answer page.
- Show your work.
- Assemble your answers in numerical order of the questions when you submit them.
- **Leave a 1" square in the upper left corner for a staple.**
- Be sure to include your name on your answer sheets.
- You have 50 minutes to complete this examination.
- **Read and sign the following statement.** You may write this on your exam and sign it there if you wish to take the exam questions home with you today. Do not discuss this exam with anyone in this course who has not yet taken this exam.

On my honor, I have neither given nor received unauthorized aid on this examination, and I will not discuss the contents of this examination with any student who has not yet taken this examination.

Signed:

1. (a) (4) How is steganography different from cryptography?

   (b) (4) Suppose that in some alphabet there are four (4) symbols, and that in the body of text (corpus) for a language using those symbols, the relative frequencies of these symbols are $\langle 1, 2, 3, 4 \rangle$. What is the Index of Coincidence (IOC) for this alphabet and corpus? What would the IOC be for a perfectly flat distribution? Show your work.

   (c) (4) For the same language as the preceding part, suppose that Alice decides to perform polyalphabetic substitution using the text of some commercially available book as a key stream for a Vernam cipher. How could a cryptanalyst attack this cryptosystem (assuming ciphertext only attacks)?

   (d) (3) Shannon stated that for a good cipher, the ciphertext should be the same size as the plaintext. Why is this? What kinds of cryptosystems typically violate this? Why?

2. (a) (3) How does the basic DES round achieve diffusion? Explain.

   (b) (6) Suggest a simple way to modify the basic DES round to increase diffusion. Describe how it does this compared to the standard DES round, and evaluate how much better it performs diffusion. Demonstrate that you can still decrypt (per round) with your modifications.

   (c) (6) In the PKC standards, PKCS #1 for RSA encryption states that the plaintext should be formatted before encryption so that the MSB is 0. Why is this? The second byte is non-zero; what kind of attack does this prevent? How? At least the next eight bytes are random bytes. Why? What restriction is there on the random bytes? Why?

3. (a) (5) Describe a method by which a one-way hash function can be used for stream encryption, and that allows encryption and decryption to be done very quickly for bursts of data. Indicate what the key for this system would be, and justify that your method fits the requirements given.

   (b) (5) Describe a method by which a one-way hash function can be used for block encryption with protection against cut-and-paste attacks. Indicate what the key for this system would be, and justify that your method fits the requirements given.

   (c) (5) Show how the DES can be used as a one-way hash function. What desirable properties do the standard secure hash functions have that this would not have? Explain, and explain why these properties are desirable.

4. (a) (3) What is the difference between an adjudicated and a non-adjudicated protocol? Give an example of each.

   (b) (5) Why are RSA signatures based on the hash of a message rather than the message itself? How does this lead to a vulnerability that otherwise would not be possible? Explain.

   (c) (3) Why is it that the Diffie-Hellman key exchange protocol does not provide authentication, even if the base (g) and the modulus (p) for a given principal are known correctly to all parties?

   (d) (4) In what way are hashes used for signatures using zero-knowledge proofs (ZKPs)? Compare this to use of ZKPs for authentication.