Examination 2
Computer and Network Security
8 December 1997

Instructions:

- 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 any three (3) questions below. Undergraduates need not answer the part marked (grad). Graduate students must answer the grad part.
- 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).
- 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) (5) What are the three classical types of attacks on cryptosystems (in generic terms, according to what information the attacker has available)? List them in order of increasing benefit to the attacker, describe them (include and example for each) and for the last two, give ways in which the additional information helps the attacker.

   (b) (4) In what ways can cryptography be used in controls to help meet the three basic goals of information security? Be specific with examples for each of the three goals.

   (c) (3) Describe a method by which a block cipher can be converted into a stream cipher. Include encryption and decryption of the stream cipher. Why might this be desirable?

   (d) (3) Describe a method by which most any cryptosystem can be modified to resist cut and paste attacks. Include encryption and decryption and how this resists these attacks.

   (e) (5) (Grad only) What type of attack can one use against a public key cryptosystem used for secrecy if the space of possible messages is small? Describe how the attack works. How can this type of attack be resisted with public key cryptosystems? Why is this attack not usually a problem with secret key cryptosystems?

2. (a) (3) What is the Index of Coincidence? How does it work? How is it used?

   (b) (4) What is the Kasksi method? When is it effective? Why? Describe how to extend it to encrypted source code files.

   (c) (4) What is digram analysis for columnar transpositions? Why does it work? What sources of noise exist for it?

   (d) (4) What is a product cipher and why are they used? Give three examples, one in which the product cipher increases security, one in which the level of security is unchanged, and one in which the security is decreased by its use, relative to the underlying ciphers.

   (e) (5) (Grad only) Explain how to use text from a novel and a Vigenere tableau to implement an polyalphabetic substitution cipher. Why is this encryption method insecure? Be specific in terms of what the cryptanalyst can work with.

3. (a) (10) Assume that in each DES S-box function, every input bit affects every output bit. Show that every input bit in the entire DES input affects every output bit. What is the minimum number of rounds that DES must have for this to be true? Suggest a method by which this number can be decreased and justify that claim.

   (b) (5) What are so-called weak DES keys, and why are they called weak? What are the semi-weak keys, and what distinguishes them from the weak keys and the rest of the keys?

   (c) (5) (Grad only) How does the DES processing of the right half of the input to a round (from expansion permutation to XOR with the left half) guarantee that each DES round implements a one-to-one function? Why is this important?

4. (a) (3) How does a message digest (MD) (a.k.a. cryptographic hash function) differ from standard error-detection codes? Why is this difference critical to security?

   (b) (4) How does a Message Integrity Check (MIC) differ from an MD? Why is this difference important in distributed security? How can it be used for standard computer security (give one example and explain why the MIC improves security over an MD).

   (c) (5) Describe a secret-key method for generating a MIC. Describe a public-key method for generating a MIC. What security property(ies) does the public-key method have that the secret-key method does not? Why? Why is this important?

   (d) (3) Compare MD-2 padding to MD-5 padding. What is the significance of their differences?

   (e) (5)(Grad only) Why is $MD4(K_{AB}.m)$ not secure as a MIC, while $MD2(K_{AB}.m)$ is? (Note that '.' represents concatenation here.) How can this problem be overcome if MD4 is used this way for a MIC?

5. Recall that the Mental Poker Protocol (MPP) involves distribution of randomly chosen, non-intersecting subsets S_i of a set S of values to each of k players, $i = 1, 2, ..., k$, with $|S_i| = n$ and $kn \leq |S|$. The example given in Pfleeger has $k = 2$ and $n = |S|/2$, with A initiating the distributed deal, B choosing and responding, then A completing the deal.

   (a) (7) Show how to modify the example MPP to allow $n < |S|/2$. Argue its correctness.

   (b) (8) Show how to modify the example MPP to allow for $k > 2$ players. Argue its correctness.

   (c) (5)(Grad only) What property must the encryption method used have in order for MPP to work? Be very precise! What cryptosystem(s), if any, have this property, and under what constraints? Do these systems have any other weaknesses when used in this way? Explain.