Print FAMILY name, first initial:__________________________

Examination 2

CEN 5540 Computer and Network Security
10 December 2002

Instructions Read all instructions. Failure to follow instructions will result in loss of points.

1. This is a closed-book examination.
2. You are permitted one 8.5 by 11 inch sheet of notes, both sides, that you have prepared.
3. You are permitted 50 minutes to complete this examination.
4. **Do not start** the exam until the proctor has told you to start.
5. **Answer any two (2) questions, and no more.** All questions are of equal value.
6. **Leave sufficient room in the upper lefthand corner for the staple** and staple your answer sheets in the room you have left.
7. 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).
8. Use exactly one page of paper (both sides is OK) to hold the answer to each question, and please write legibly.
9. Show your work.
10. Put the question number in the top center of each answer page and label each part of the question answer.
11. Include your last name and page number in the upper right hand corner of each answer page.
12. Assemble your answers in numerical order of the questions when you submit them.
13. Print your family name and first initial in the upper right hand corner of this page, and complete the honor statement affirmation below.

Read and sign the following statement. This page **MUST** be attached to your examination answers and **MUST** be completed to obtain credit for this examination.

On my honor, I have neither given nor received unauthorized aid on this examination.

Signed:

Printed Name:

SSN:

1. (a) (7) The purpose of the permutation at the end of a DES round is diffusion. How many rounds are required to diffuse the effects of a bit onto all output bits if the permutation is not performed at the end of each round? Give best case and worst case results.

   (b) (8) Consider DES-like encryption. What would happen if the output of an S-Box in the Feistel structure had collisions, i.e., two distinct, right-half inputs to the mangling function produced two identical outputs? Suppose that, after the initial permutation, two distinct inputs appear as L_0R_0 and L_0R_0', that is, the left halves of the inputs to the first round are identical, but the right halves are distinct. Further suppose that after the mangler function, the two right halves both produce the same output, S_0. Show what the outputs would be for two rounds, indicating where the intermediate values or outputs are distinct by using the prime symbol, and using the same label where they are the same (e.g., if the outputs after the second round are identical, then the outputs should be labeled L_2 and R_2 for both cases, while if left and right halves are both distinct, they should be labeled L_2 and R_2 for one case and L_2' and R_2' for the other). Using S_i and S_i' (as appropriate) for the mangler function output during the ith round. Will the encryption produce the same output for L_0R_0 as it will for L_0R_0'? If so, explain. If not, what will it produce and justify?

2. (a) (7) Public key cryptography solves the problem of a secure channel for key distribution for use of symmetric keys (the fundamental problem for them), but introduces its own problem. What is the fundamental problem for public key cryptography, and what are two distinct ways of solving it? What assumptions does each of the solutions make?

   (b) (4) The RSA algorithm can have the property that $E(m, f(k_1, k_2)) = F(E(m, k_1)E(m, k_2))$. Under what circumstances is this true (i.e., give the functions f and F, and state any other assumptions)? Show that it is true with the appropriate assumptions.

   (c) (4) The fact from the previous part suggests a mechanism for enforcing separation of duty (SoD) through multi-signature authorization. Suggest a mechanism that uses this property of RSA to allow an organization, X, to enforce SoD and an external entity, Alice, to verify that one or more authorized signers have signed a document for X without Alice knowing either the policies of the organization or the keys of its employees (i.e., she only knows the verification key of the organization).

3. (a) (4) Recall the simple nonce challenge authentication protocol is:

    - $M1.\ A \rightarrow B : N_a$
    - $M2.\ B \rightarrow A : \{N_a\}K_{ab}, N_b$
    - $M3.\ A \rightarrow B : \{N_b\}K_{ab}$

    and that it suffered from a reflection attack. One of the principles for prudent authentication protocol practice was that the messages contain information about what they were intended to be within to protocol. Show the reflection attack on the simple protocol, then show how an application of this principle can prevent the reflection attack on the simple nonce challenge authentication

    (b) (2) Another principle was that the message should state who it was from and who it was for. Again show how an application of this principle can prevent the reflection attack on the simple nonce challenge authentication.

    (c) (6) Apply BAN logic to the simple nonce challenge protocol, including developing the idealized protocol, writing down the initial assumptions, and deriving the resultant beliefs by application of the logic to the idealized protocol. Does the analysis show the vulnerability cited above?

    (d) (3) Would changing the responses to the nonce challenges to $\{N_x - 1\}K_{ab}$ fix the problem? Justify your answer.

4. (a) (5) What are the conflicting requirements on the audit log, and why do they conflict? Suggest a solution to this quandary and show that it solves the problem.

    (b) (6) What kinds of firewall are there (i.e., describe them functionally), and when could they be considered as more than just a patch to an already broken system? That is, if the systems they protected were secure by themselves, then would firewalls have any role to play at all?

    (c) (4) What are the limitations on firewalls — are they intrinsic limitations or not? Justify your answer(s).