**Print FAMILY name, first initial:**_____

# Examination 2

CEN 5540 Computer and Network Security
9 December 2005

**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 90 minutes to complete this examination.
4. **Do not start** the exam until the proctor has told you to start.
5. **Answer any three (3) 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. When possible, use exactly one page of paper (use of both sides is OK) to hold the answer to each question, and please write legibly.
9. Put the question number in the top center of each answer page and label each part of the question answer.
10. Show your work.
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. Staple this entire exam to the front of your answer sheets in their numerical order.
14. **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:

UF ID:

1. Consider 128-bit AES. For each of the modes below, rate this cryptosystem in the given mode for confusion and diffusion. Justify your claims.

   (a) (4) ECB mode.

   (b) (4) CBC mode.

   (c) (4) OFB mode.

   (d) (4) CFB mode.

   (e) (4) Counter mode.

   (f) (5) Answer this question for each of the modes given above. For which of these modes is an IV required, and what vulnerabilities (if any) exist if the IV is repeated with the same encryption key?

2. Consider the Mental Poker protocol.

   (a) (2) Alice is required to encrypt all the "cards" with the same key ($K_a$). Why?

   (b) (3) When Bob uses $K_b$ to encrypt all but 5 of these (thereby selecting Alice's "hand"), it must be the case that

   $$\{\{card_i\}K_a\}K_b = \{\{card_i\}K_b\}K_a$$

   i.e., encryption with Bob's key commutes with encryption with Alice's key. Why?

   (c) (7) One cryptosystem that can commute is the Vernam Cipher. What conditions are necessary and sufficient for two symbol-oriented Vernam Cipher encryptions to commute? Demonstrate two Vernam Cipher encryptions of the same type that do not satisfy one of the conditions and do not commute. Is a Vernam Cipher a good choice for Mental Poker? Justify your answer.

   (d) (8) Another (possibly) commutative cryptosystem is RSA. What conditions are necessary and sufficient for two RSA encryptions to commute, and why? Give a small counterexample to show that if the requirements are not met, then RSA encryption does not commute.

   (e) (5) If Alice's RSA public key is known to Bob, but not her private key, then Bob cannot decrypt the cards that Alice encrypts directly using $K_a^{-1}$. However, he may still be able to figure out which cards are which and give Alice a bad hand. How? How can the protocol be adjusted to prevent this, other than keeping Alice's "public key" a secret also? Explain why this works.

3. Consider the following protocol.

```
M1: A -> B: A, Na
M2: B -> S: B, {A, Na, Nb}Kbs
M3: S -> A: B, {B, Kab, Na, Nb}Kas, {A, Kab}Kbs
M4: A -> B: A, {A, Kab}Kbs, {Nb}Kab
```

   (a) (6) In BAN Logic, there are a number of assumptions about the underlying cryptosystems and the ways they are used, as well as some about the behavior of the principals. What are three of these assumptions, and why are they necessary for the logic to apply correctly? Give an example for each that shows how the logic would fail if the assumption were violated.

   (b) (4) Give the standard starting assumption and the standard goals for a trusted server, symmetric key based, key distribution and authentication protocol

   (c) (4) Give the idealized protocol corresponding to this actual protocol.

   (d) (9) Apply BAN Logic to derive new beliefs from the protocol messages. Can the standard goals be derived without adding non-standard assumption? If so, demonstrate this in sufficient detail; if not, where does (do) the problems lie, and what assumptions would be required?

   (e) (2) Can you make an improvement to the protocol? Provide it and explain how it would be an improvement, or justify that the protocol cannot be improved in any significant way.

4. (a) (6) What are the generic steps involved in anomaly detection? Explain what each step does and why it is needed.

   (b) (6) For each of the generic steps in anomaly detection, what are the main issues? Explain.

   (c) (6) Define and compare packet filtering and application level firewalls. What are their pros and cons?

   (d) (3) What are the advantages of having a separate machine as a dedicated firewall? Be as specific as possible.

   (e) (4) What are limitations of firewalls - explain and illustrate.