**CSC 290A – Network Security** **Name:**_____

**Midterm** **Hofstra University – Spring 2006**

Please answer all five questions.

1. Key distribution schemes using an access control center and/or a key distribution center have central points vulnerable to attack. Discuss the security implications of such centralization and how it could be improved. (10 pts)

2. Perform encryption and decryption using the RSA algorithm, as in Figure 3.9, for the following:

   *p = 5; q = 11, e = 3; M = 9*

   (10 pts)

3. The original three-way authentication procedure for X.509 illustrated in Figure 4.5c (p.111) contains a security flaw. The essence of the protocol is as follows (see p.106 for nomenclature):

   $A \rightarrow B$: $A\{t_A, r_A, ID_B\}$
   $B \rightarrow A$: $B\{t_B, r_B, ID_A, r_A\}$
   $A \rightarrow B$: $A\{r_B\}$

   The text of X.509 states that checking timestamps $t_A$ and $t_B$ is optional for three-way authentication. But consider the following example. Suppose A and B have used the preceding protocol on some previous occasion, and that opponent C has intercepted the preceding three messages. In addition, suppose that timestamps are not used and are all set to 0. Finally, suppose C wishes to impersonate A to B. C initially sends the first captured message to B:

   $C \rightarrow B$: $A\{0, r_A, ID_B\}$

   B responds, thinking it is talking to A but is actually talking to C:

   $B \rightarrow C$: $B\{0, r'_A, ID_A, r_A\}$

   C meanwhile causes A to initiate authentication with C, by some means. As a result, A sends C the following:

   $A \rightarrow C$: $A\{0, r'_A, ID_C\}$

   C responds to A, using the same nonce provided to C by B.

   $C \rightarrow A$: $C\{0, r'_B, ID_A, r'_A\}$

   A responds with

   $A \rightarrow C$: $A\{r'_B\}$

   This is exactly what C needs to convince B that it is talking to A, so C now repeats the incoming message back out to B.

   $C \rightarrow B$: $A\{r'_B\}$

   So B will believe it is talking to A whereas it is actually talking to C. Suggest a simple solution to this problem that does not involve the use of timestamps. (*Hint:* Make a slight change to the third message in the 3-way procedure) (10 pts)

4. Phil Zimmermann chose IDEA, three-key triple DES (also know as triple DEA), and CAST-128 as conventional encryption algorithms for PGP. Give reasons why each of the other conventional encryption algorithms described in this book is suitable or unsuitable for PGP: DES, Blowfish, and RC5. (10 pts)

5. End-to-end authentication and encryption are desired between two hosts. Draw figures similar to Figures 6.6 and 6.9 (pp. 181 & 185) that show
   a) Transport adjacency, with encryption applied before authentication
   b) A transport SA bundled inside a tunnel SA, with encryption applied before authentication
   c) A transport SA bundled inside a tunnel SA, with authentication applied before encryption

   (10 pts)

**NOTE: This is due next class April 10, 2006 – No late submissions!**