Name: _____

CIS 551 / TCOM 401 Midterm 2
Marcy 21, 2006

1	/10
2	/14
3	/25
4	/12
5	/15
6	/24
Total	/100

- Do not begin the exam until you are told to do so.
- You have 80 minutes to complete the exam.
- There are 8 pages in this exam.
- Make sure your name is on the top of this page.

1. True or False (10 points)

Circle the appropriate answer.

a. T F Most commonly used Internet protocols have been designed to be secure against malicious attacks.

b. T F The 802.3 (Ethernet) protocol does not guarantee that a host that wants to transmit a frame will eventually be able to do so.

c. T F A good password for human authentication should contain about 64 bits of random information, as provided by a typical mixed-case, alphanumeric, 8-character ASCII string.

d. T F Unlike Ethernet addresses, IP addresses are hierarchical.

e. T F Digital signatures require the property of *nonrepudiation*, which says that a principal should not be able to spoof another principal's signature.

f. T F Kerberos is an example of an arbitrated protocol.

g. T F The WEP protocol is insecure not because of poor protocol design, but because it is based on the easily breakable RC4 encryption scheme.

h. T F Good protocol design suggests that message formats be kept as uniform as possible to simplify the end hosts and reduce the trusted computing base.

i. T F It is infeasible in practice to arrange for users of a computer system to authenticate using one-time passwords.

j. T F For shared-key protocols that employ a trusted third party (like Needham–Schroeder and Kerberos), it is necessary to distribute $O(n^2)$ keys before any session keys may be generated. (Here, n is the number of principals.)

2. Cryptographic Protocols (14 points)

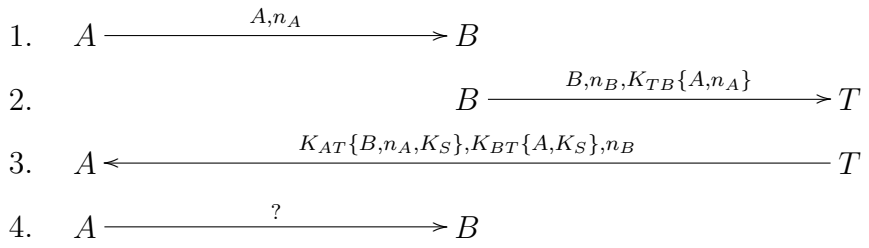
Suppose that A and B have previously established a secret shared key. At some later point they want to establish an encrypted channel between them, but they want to verify that they are both still in possession of the same secret key. Recalling that XOR with a one-time pad of bits constitutes a perfect cipher, A proposes the following solution: A generates a string of random bits of length equal to the key's length, XORs the random bits and her copy of the key and sends the result to B. B receives the message, XORs the result with his copy of the key and sends the result back to A who can verify whether the bits B sent her match her original random string—neither A nor B transmits the key in cleartext. If the bits match, A and B must have used the same key.

a. (6 points) Explain why this protocol is a bad idea.

b. (8 points) Suggest a different protocol to securely accomplish the same task and briefly explain how it works.

3. Cryptographic Protocols (25 points)

Consider the following protocol in which A and B use a trusted third party T to perform mutual authentication and establish a session key K_S. Assume that initially A and T share the symmetric key K_{AT} and B and T share the symmetric key K_{BT}. A and B generate nonces n_A and n_B, respectively. There are four messages in the protocol, the first three of which are shown below.



a. (8 points) What message should A send to B in step 4 to complete the protocol?

b. (6 points) Is the protocol still secure if the message in step 2 is changed to have the contents: $B, n_B, n_A, K_{TB}\{A\}$? Explain why or why not (the answer to this question does not depend on your solution for part a).

c. (6 points) Is the protocol still secure if the message in step 2 is changed to have the contents: $B, K_{TB}\{A, n_B, n_A\}$? Explain why or why not (the answer to this question does not depend on your solution for part a).

d. (5 points) Consider the following messages generated by a Dolev-Yao model attacker. For each message, indicate how many of the first three steps of the above protocol the attacker would need to see before it could generate the message. Write 0 if the attacker could generate the message without seeing any protocol message and ∞ if the Dolev-Yao attacker could never generate the message. Each answer should be one of $\{0, 1, 2, 3, \infty\}$.

i. _____ n_B
ii. _____ $K_{AT}\{n_A\}$
iii. _____ $K_X\{A\}$, where K_X is a fresh key
iv. _____ $n_A, n_B, K_{BT}\{A, K_S\}$.
v. _____ $K_S\{A\}$.

4. Diffie-Hellman Protocol (12 points)

Suppose Alice and Bart wish to use the Diffie-Hellman key exchange protocol to establish a shared secret. Alice suggests that they use the prime $p = 7$ with primitive root $g = 3$.

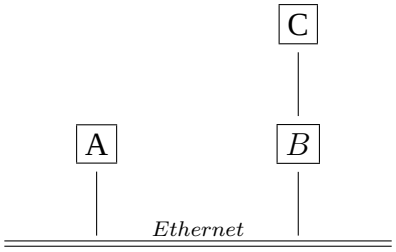
a. (6 points) What number does Alice send to Bart for her part in the protocol, assuming that she randomly chooses the number 2 for her contribution to the shared secret?

b. (6 points) What is the shared secret they calculate, assuming that Bart randomly chooses the number 3 for his contribution to the protocol.

5. Internet Protocol (15 points)

Consider the simple network shown below, in which hosts A and B are connected by an Ethernet LAN and host C is connected to B by a direct link. Suppose the Ethernet LAN has a class C IP network address of 192.5.51.

Give an assignment of IP addresses and Subnet Masks to all of the network adapters to properly configure this network. Assume that no additional network address is available. Note that B has two network adapters.



6. Short Answer (24 points)

a. (8 points) Suppose that A has a very short secret s (e.g. a single bit), and she wishes to send B a message m that will not reveal s but that can be later used verify that A did know s. Explain why sending the MD5 hash ($m = MD5(s)$) or encrypting s with A's public RSA key $m = K_A\{s\}$ would not be secure choices. Briefly, suggest a better way of creating m.

b. (8 points) Give an example of one problem faced by the 802.11 (wireless) transmission protocol that is not an issue for 802.3 (Ethernet). Briefly explain how the 802.11 MACA (Multiple Access Collision Avoidance) protocol addresses the problem.

c. (8 points) Recall that the five primary attacks against network protocols are: Replay, Interleaving, Reflection, Chosen Text, and Forced Delays. Pick *two* of these attacks, (briefly) describe them and give a typical countermeasure for each.

Attack 1:

Countermeasure 1:

Attack 2:

Countermeasure 2: