

Net ID:

**University of Illinois at Urbana-Champaign
Department of Computer Science**

Midterm 2

CS498SH – Information Assurance

Fall 2006

Wednesday, Oct. 27, 2006

Time Limit: 1 hour and 15 minutes

Instructions for the Student

Print your name and NetID in the space provided below; **print your NetID in the upper right hand corner of every page.**

Name: _____

NetID: _____

1. A single page of supplementary notes is allowed
2. Closed book
3. A calculator is allowed.
4. Students should show work on the exam. They can use supplementary sheets of paper if they run out of room.
5. Students can use scratch paper if desired.

Number of pages of the exam: 9

Number of questions on the exam: 15

Maximum grade on this exam is: 73 pts

Problem	Points	Score	Grader
1	2		
2	2		
3	2		
4	2		
5	2		
6	2		
7	2		
8	6		
9	9		
10	9		
11	10		
12	10		
13	8		
14	3		
15	4		

Information Assurance: Midterm 2

Multiple Choice – 2 points each

1. Which of the following cryptographic algorithms is self healing?
 - a. AES in Electronic Code Book (ECB) mode
 - b. DES in Cipher Feedback (CFB) mode
 - c. Vigenere Cipher
 - d. AES in Counter mode

2. What hard problem is the security of the Diffie-Hellman public key algorithm based on?
 - a. Factoring large primes
 - b. Computing discrete logarithms
 - c. Traveling salesman optimization
 - d. Bin packing

3. The Enigma cipher is an example of which of the following types of ciphers?
 - a. Substitution cipher
 - b. Transposition cipher
 - c. Proposition cipher
 - d. Product cipher

4. Which of the following encryption algorithms is an example of a Feistel network?
 - a. AES
 - b. DES
 - c. RSA
 - d. Enigma

5. Which of the following statements must be true for a RSA system? Where **e** is the public exponent, **d** is the private exponent, and **n** is the modulus.
 - a. **e** must be relatively prime to **d**
 - b. **n** and **d** must be kept private
 - c. **ed mod n = 1**
 - d. **ed mod $\Phi(n)$ = 1**

6. Which of the following is **not** traditionally an information source for proving an entity's identity?
 - a. Something you know
 - b. Something you have
 - c. Something you like
 - d. Something you are

Net ID:

7. Which of the following is **not** an operation performed by a standard firewall?
 - a. Deduce that incoming traffic on a random port is using the HTTP protocol and automatically apply HTTP analyzer.
 - b. Filter packets based on header data.
 - c. Verify that packets are well formed for specific protocols and no known protocol attacks are being launched.
 - d. Analyze packet stream and dynamically open access for protocol related streams.

Net ID:

10. (9 points total) A phoneme is a unit of sound which can be represented by a sequence of two or three characters. By using phonemes as the unit of password creation, you can create random but pronounceable passwords. According to the textbook there are 440 possible phonemes. Assume that an attacker can make 20,000 guesses per second. You are told that randomly chosen passwords must be secure with a probability of at least 75% at the end of a month.
- a. (4 points) Given a selection of 96 printable characters and assuming that all passwords are the same length, how long must randomly generated passwords be to meet the 75% unbroken requirement?

 - b. (4 points) Given a selection of 440 phonemes and assuming that all passwords are the same length, how long must the random passwords be to meet the 75% unbroken requirement? Give the length in terms of phonemes.

 - c. (1 point) Assume the average phoneme is 2.5 characters long. How long is the phoneme based password in terms of characters?

Net ID:

11. (10 points total) A basic key management protocol using public key certificates only requires a single message

Alice \rightarrow Bob $\{k\}_{e_{\text{Bob}}}$

This protocol has several points for Eve to attack. Identify two weaknesses and propose extensions to the protocol to fix these weaknesses. For your analysis assume that Alice and Bob have access to trustworthy certificate servers.

Net ID:

12. (10 points total) Alice and Bob use Diffie-Hellman to compute a shared secret. They select $p=67$ and $g=13$. Alice picks a k_{Alice} of 11 and Bob picks a k_{Bob} of 7.
- (4 points) Show the computations for K_{Alice} and K_{Bob} .
 - (4 points) Show how Alice and Bob use K_{Alice} and K_{Bob} to compute the shared secret
 - (2 points) Which values of p , g , k_{Alice} , k_{Bob} , K_{Alice} , and K_{Bob} can be made public without affecting the security of the key exchange?

