CSC 474/574 – Information Systems Security

Midterm Exam, Fall 2003

Time: 4:35pm – 5:35pm

Student Name:__________________________ Score: ______________________

You are allowed to use your textbook and notes; however, you are not allowed to exchange anything before you get permission from the instructor.

Questions 1 – 5. Multiple choices. (Total 25 points. 5 points/question.)

Choose appropriate answers and write it on the blank below the question.

1. If a bit error occurs in the transmission of a ciphertext character in 10-bit CFB mode with DES, how far does the error propagate? That is, how many more blocks does the error affect in addition to itself?

(A) 6
(B) 7
(C) 8
(D) 6 or 7
(E) 7 or 8

Answer: ________________

2. Which of the following was developed to defeat Trojan horses?

(A) DAC
(B) MAC
(C) Both DAC and MAC
(D) Access control matrix
(E) ACL and Capabilities

Answer: ________________

3. Meet-in-the-middle attack against double DES is

(A) Cipher-text only crypto analysis
(B) Known plaintext crypto analysis
(C) Chosen cipher text crypto analysis
(D) Chosen plaintext crypto analysis
(E) None of the above

Answer: ________________

4. Password salt is NOT effective to deter which of the following dictionary attacks?

(A) Guessing all users' passwords off-line with a dictionary of passwords and a password file.
(B) Guessing all users' passwords off-line with a dictionary of password hashes and a password file.
(C) Guessing Joe's password off-line with a dictionary of passwords and Joe's entry in a password file.
(D) None of the above.

Answer: ________________

5. Pick the strongest mechanism for user authentication from the list below.

(A) Password
(B) Retina scan
(C) Finger print
(D) Smart card
(E) All of the above together.

Answer: ________________

Questions 6 – 10. Simple calculation. (Total 25 points. 5 points/question.) Show your steps (or reasons).

6. 1234^{37} mod 19

7. 5^4 mod 10

8. 2^{-1} mod 17

9. gcd (45, 150)

10. $\log_{2,7}$ (4) (i.e., the index of 4 for the base 2 mod 7)

11. (20 points) A and B want to establish a secure communication channel between them. They do not care about the confidentiality of the messages being transmitted, but they do want to ensure the integrity and authenticity of the messages. Answer the following questions by drawing diagrams that show the procedures of sending and receiving messages. Assume A and B share a common key K.

(a) (5 points) How can they achieve their goal only with secret key cryptography?

(b) (5 points) How can they achieve their goal only with hash function (e.g., MD5)?

(c) (5 points) Can they get non-repudiation? (2 points) If yes, how? If no, why? (3 points)

(d) (5 points) Describe a way A and B can get non-repudiation. Explain your assumption and draw a diagram to show the procedure.

12 (10 points) Consider DSA signing process as shown below.

$$r = (g^{k} \bmod p) \bmod q$$

$$s = [k^{-1}(\mathrm{H(M)}+xr)] \bmod q$$

It is well known that the random number k should not be reused. Otherwise, an attacker will be able to recover the private key x. Due to this reason, Alice decides to change the value of k each time she signs on a message. Specifically, Alice adds a constant c to k each time when she uses k.

(a) (2 points) Is Alice's approach secure?

(b) (8 points) Give your reason to justify your answer to (a). If you answered Yes, you should prove why it is secure. If you answered No, describe a way to derive the private key x.

13. (10 points) Assume there is a Certificate Authority (CA) with a well-known public key. Further assume every user is issued a certificate for his/her public key. For convenience, we use PK_u and SK_u to represent user u's public key and private key, respectively. Draw diagrams to answer the following questions.

(a) (3 points) Suppose Alice wants to send a large secret message M to Bob. Describe how Alice should send M in an authenticated way.

(b) (3 points) Assume Bob receives the message sent by Alice. Describe how Bob should process the message.

(c) (4 points) Suppose Alice needs to send a number of large secret messages to Bob. Alice would like to avoid signing digital signatures for all these messages. Develop a protocol for Alice and Bob so that all the messages can be sent in a confidential and authenticated way. Briefly describe the intuition of your protocol first and then draw a diagram.

14. (10 points) A protocol named TESLA has been developed for broadcast authentication. In its simplified form, TESLA randomly generates a key K_n and computes $K_i = H(K_{i+1})$ for $i = n - 1, n - 2, \ldots, 0$, where H is a hash function. In addition, TESLA partitions a period of operation time into n time intervals, denoted as $I_1, I_2, \ldots, I_n$. Each key K_i is associated with the time interval I_i, and used to generate MACs for all the messages the sender broadcasts during I_i. However, the sender doesn't disclose K_i until T time units after I_i. Let's denote the beginning time of I_i is T_i. Then the sender doesn't disclose K_i until $T_{i+1} + T$. Each receiver buffers the messages received during I_i. It can authenticate the messages broadcasted during I_i after it receives K_i disclosed by the sender.

Assume all the receivers know the sender's public key *PKs*.

(a) (5 points) Develop a way so that each receiver can authenticate each K_i disclosed by the sender.

(b) (5 points) When a receiver receives a broadcast message authenticated with K_i at time t, how can it determine if the message wasn't forged by an attacker that just learned the K_i disclosed by the sender? In other words, develop *a security condition*, by checking which a receiver can determine if the message was sent before K_i is disclosed. Assume the maximum clock discrepancy between the sender and the receiver is Δ, and the time required for message transmission is negligible.