CSC 774 – Network Security

Mid-Term Exam #2
4:10pm – 5:00pm, March 26, 2004

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. Note that none of the questions need long answers. Please be brief. DO NOT write anything irrelevant to the questions.

Questions 1 – 4. Multiple choices. (Total 40 points. 10 points/question.)

Choose one appropriate answer for each question and write it on the blank below the question.

1. Consider the following statements about fair exchange.
   (1) An exchange is fair if either both parties get what they want, or no party gets anything;
   (2) All items being exchanged in a fair exchange protocol must be forwarded to the TTP first, so that the TTP can oversee the exchange and ensure the fairness;
   (3) A protocol that achieves strong fairness needs an external resolution system;
   (4) Strong fairness is possible when at least one item to be exchanged is revocable or generatable;
   (5) Fair exchange requires both parties be honest. That is, both of them have to follow the protocol in order to ensure the fairness of the exchange.

   Which of the following include the set of all correct statements?

   (A) All of them;
   (B) 1, 4;
   (C) 1, 4, 5;
   (D) 1, 2, 4;
   (E) 1, 5.

Answer: _____

2. Consider the following statements about intrusion alert correlation.

   (1) If the current IDS can detect all attacks, it is not necessary to correlate the IDS alerts;
   (2) One limitation of the alert correlation method using known attack scenarios is that it cannot correlate alerts correctly if the corresponding attack scenario is not known;
   (3) The alert correlation method based on prerequisites and consequences of attacks is the best method among all the existing ones;
   (4) The alert correlation method based on prerequisites and consequences of attacks can only handle known attack scenarios;
   (5) The correlation method based on similarity between alert attribute values is essentially an alert clustering method. That is, it simply puts alerts into different groups.

Which of the following include the set of all correct statements?

(A) 2, 5;
(B) 1, 2, 5;
(C) 2, 3, 5;
(D) 1, 2, 3, 5;
(E) None of the above.

Answer: _____

3. Consider the following statements about broadcast authentication:
(1) It is not possible to achieve broadcast authentication with symmetric cryptography;
(2) It is not possible to achieve broadcast authentication with digital signature;
(3) In TESLA scheme III, the sender delays the disclosure of each authentication key by d intervals. If d is not chosen correctly, TESLA cannot guarantee the security of broadcast authentication even if the security condition is always satisfied at each receiver;
(4) EMSS amortizes the signature cost by generating one signature for several data packets rather than having a signature for each packet.

Which of the following include the set of all correct statements?
(A) 1, 3, 4;
(B) 4;
(C) 3, 4;
(D) 3;
(E) None of them.

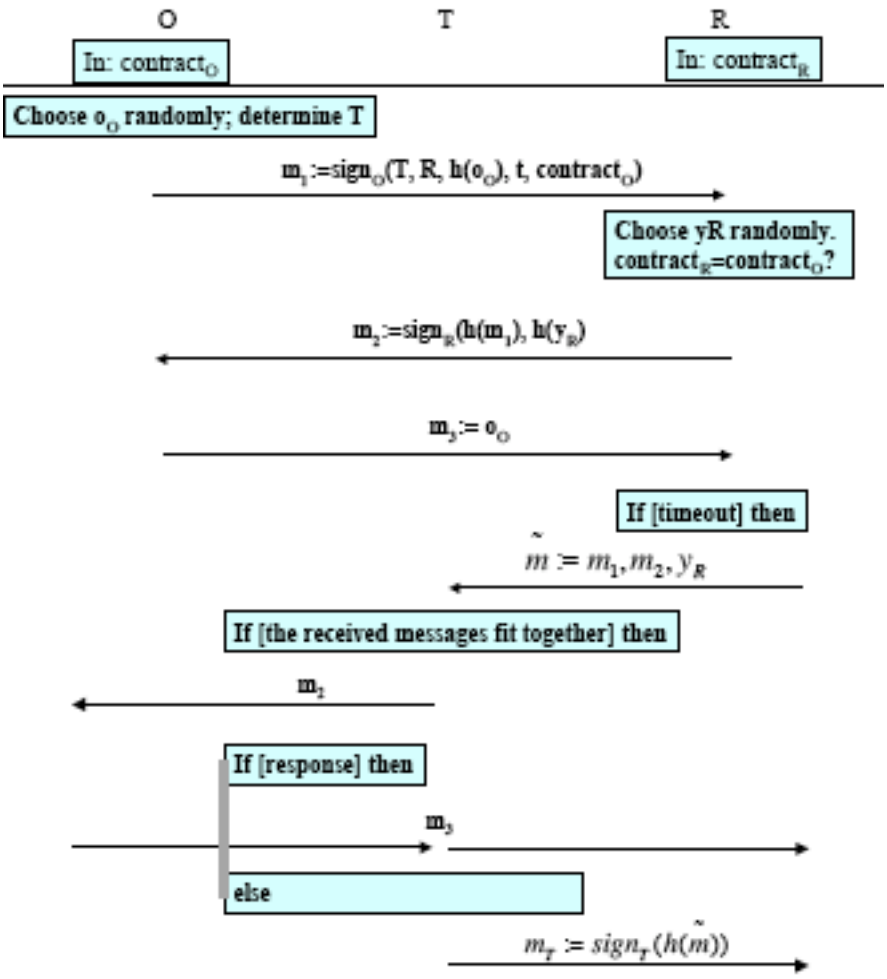
Answer: _____

4. Which of the following is a correct statement about group key management:

(A) Group key agreement protocols are more scalable than group key distribution protocols, and thus are more suitable for large groups;
(B) In group key agreement protocols, a group manager receives one item from each group member, computes the group key, and then distributes the group key to all the group members;
(C) Group key distribution protocols are usually more scalable than group key agreement protocols. Thus, we should only use group key distribution in practice;
(D) The "1-affect-n" problem only means that whenever a member leaves, all the remaining group members must change the group key;
(E) None of them.

Answer: _____

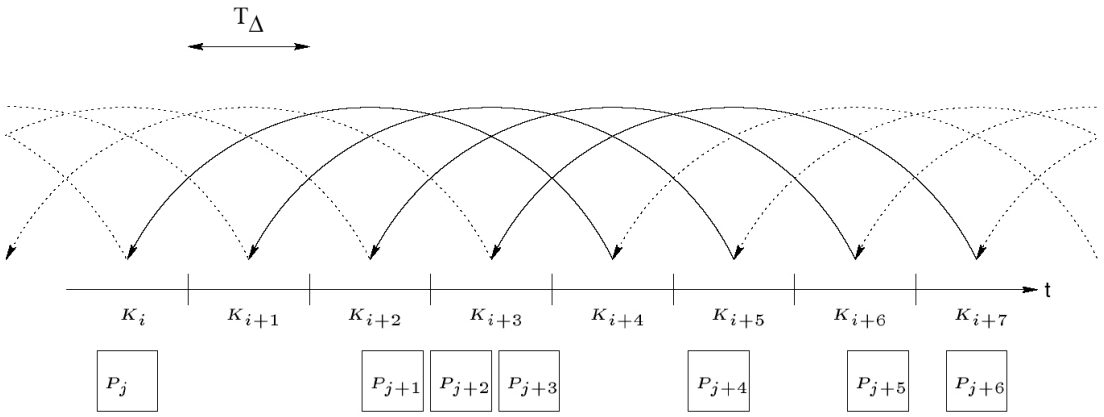
5. (20 points) Consider the following optimistic contract signing protocl.



(a) What is the valid signature of R on the contract for O? (2 point) Why can it prove that R has signed the contract? (8 points)

(b) What is the valid signature of O on the contract for R? (2 points) Why can it prove that O has signed the contract? (8 points)

6. (10 points) Consider the following figure illustrating TESLA Scheme IV, where each K_i is disclosed in time interval i+4.



(a) (5 points) This figure shows what keys are used to authenticate each packet. Explain in which time interval each packet can be authenticated. Write "U" if you can't determine. (You will lose 1 point for each mistake.)

P_j	P_{j+1}	P_{j+2}	P_{j+3}	P_{j+4}	P_{j+5}	P_{j+6}

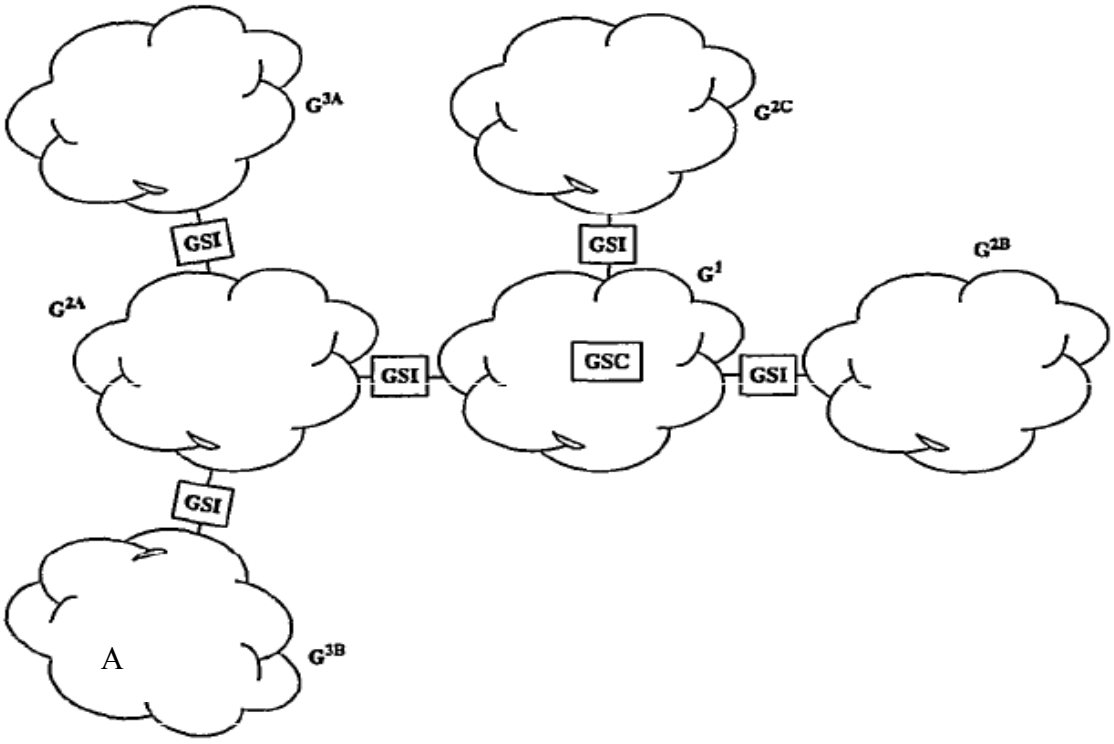
(b) (5 points) Is it possible to reduce the delay before authentication? (2 points) If yes, how? If no, why? (3 points)

7. (10 points) Consider EMSS scheme. Assume packet P_i includes $H(P_{i-1})$ and $H(P_{i-2})$ for i = 1, 2, …, where H is a hash function, P_{-1} and P_0 are empty packets. Further assume there is a signature packet S_j for every 5 packets, where S_j include $H(P_{5*j-1})$ and $H(P_{5*j})$ for j = 1, 2, ….

(a) (5 points) Suppose a receiver correctly receives packets P1, P2, P4, P5, P6, P8, P10, and S2. What packets can be authenticated by the receiver?

(b) (5 points) Assume that the above receiver finds P8 is corrupted. What packets can be authenticated by the receiver?

8. (4 points) Consider the following network configuration, in which Iolus is used.



Assume the GSC is distributing a new group key to the group members using Iolus. How many times will this new key be encrypted and decrypted before A learns the value of the new key? (You lose 2 points for each mistake you make.)

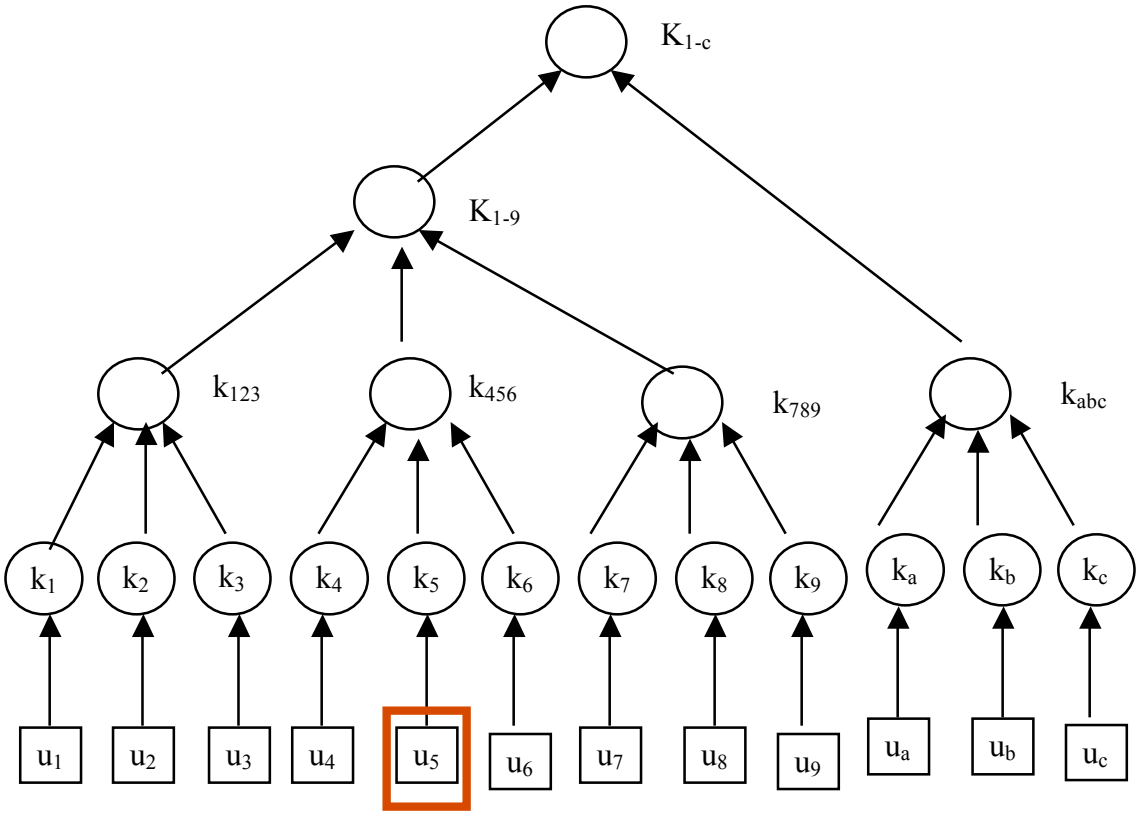
encryptions: _____; # decryptions: _____

9. (6 points) Consider GDH.2. Denote the members as Mi, and the secret of Mi as Ni. Assume there are totally 7 members in a group.

(a) (3 points) What is the set of messages M5 receives in the upflow stage?

(b) (3 points) What is the message sent in the downflow stage? (2 points) What is needed by M5 in this message? (1 point)

10. (10 points) Consider the following key tree.



(a) (3 points) If u5 is removed from the group, what keys should be changed?

(b) (7 points) Assume the key oriented rekey is used. Describe the messages the group manager needs to send to the group members. Use the following convention to describe each message:

GM → {set of users}: {Kx}Ky, {Kz}Kw, …;

You will lose 2 points for each mistake.