

## ISA662 Section 1

### Homework 3 (Due April-11)

(Note: Please keep your answers short. It is strongly recommended that you use a text editor, such as Notepad or Word, for the homework. If you submit homework through emails, make sure you get a receipt message from me the following day.)

1. Following the notations introduced in class, translate those messages into English:

(a)  $A \rightarrow B: \{m \parallel r_1\}_{k_{AB}} \parallel h(m \parallel r_1)$

(b)  $A \rightarrow B: \{m_1\}_{k_{AB}} \parallel \{m_2\}_{k_{AB}} \parallel h(m_1 \parallel m_2)$

(c)  $A \rightarrow B: \{m \parallel r_1\}_{e_B} \parallel \{m \parallel r_1\}_{d_A}$

(d)  $A \rightarrow B: \{m \parallel r_1\}_{k_{AB}} \parallel \{h(m \parallel r_1)\}_{d_A}$

(e)  $A \rightarrow B: \{m \parallel r_1 \parallel \{h(m \parallel r_1)\}_{d_A}\}_{k_s} \parallel \{k_s \parallel r_2\}_{e_B}$

2. Describe in English what the recipient will do, after he/she receives the above messages 1(a) through 1(e). (Your answer will be something like 'B decrypts with  $d_B$  to get  $m$ , computes  $h(m)$  from  $m$  and check if the result matches the transmitted  $h(m)$ '.)

(a)

(b)

(c)

(d)

(e)

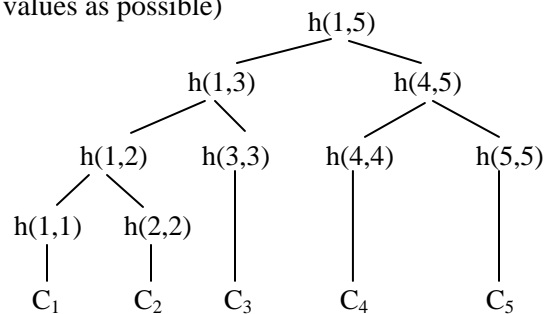
3. Consider each of the above messages 1(a) through 1(e) as a protocol (with a single step), then which of those protocols are vulnerable to replay attack?

4. Consider the following Merkle hash tree. Suppose Alice possesses a signature on  $h(1,5)$  that has been created by a trusted certificate authority.

(a) Suppose Alice has only the certificate  $C_1$ . Which of the hash values should be given to her, so she can verify  $C_1$  against that signature? (Your should include as few hash values as possible)

(b) Following the answer to (a), describe how Alice should do the verification.

(c) If Alice has both  $C_1$  and  $C_4$ . Then which of the hash values should be given to her, so she can verify both certificates? (Your should include as few hash values as possible)



5. Consider an SSL handshake (RSA one-way, as discussed in class).

(a) Suppose an attacker has intercepted all messages sent by the client during a former SSL handshake. The attacker now replays the messages to the server (and ignore whatever the server sends back). Describe when and why the server will detect this attack.

(b) Now the attacker changes his strategy. He/she ONLY replays the messages in the first three rounds (that is, up to 'client key exchange'), but he/she repeats this replay for many times. What is the attacker's intention? (Hint: consider what the server would do)

6. Alice talks to Bob using IPsec AH protocol in transport mode via two security gateways OSF1 and OSF2. Suppose OSF1 and OSF2 are using IPsec ESP protocol in tunnel mode. Draw a diagram to show the structure of a packet between OSF1 and OSF2.

