COMP90043: Cryptography and security

Week 8: Workshop-8

Preparation: We may not cover all parts of Part A, please come prepared to class by reading on MAC, Hash and Signatures. Please attempt Q1. Q2,Q7,Q8 of Part A below before coming to the class. Also come prepared with the basic key distribution protocol discussed in the class.

Part A: MAC, Hash Continued:

1. What is a message authentication code?
2. What types of attacks are addressed by message authentication?
3. What is the main difference between hash functions and Message Authentication codes?
4. In what ways a hash value can be secured so as to provide message authentication?
5. Discuss two scenarios for using MACs for implementing authentication and confidentiality discussed in lectures?

   Refer to Fig 12.4 attached.
6. List two disputes that can arise in the context of message authentication.
7. What are the properties a digital signature should have?
8. What are some threats associated with a direct digital signature scheme?
9. List ways in which secret keys can be distributed to two communicating parties.
10. What is the difference between a session key and a master key?
11. What is a nonce?

12. Explain the problems with key management and how it affects symmetric cryptography?

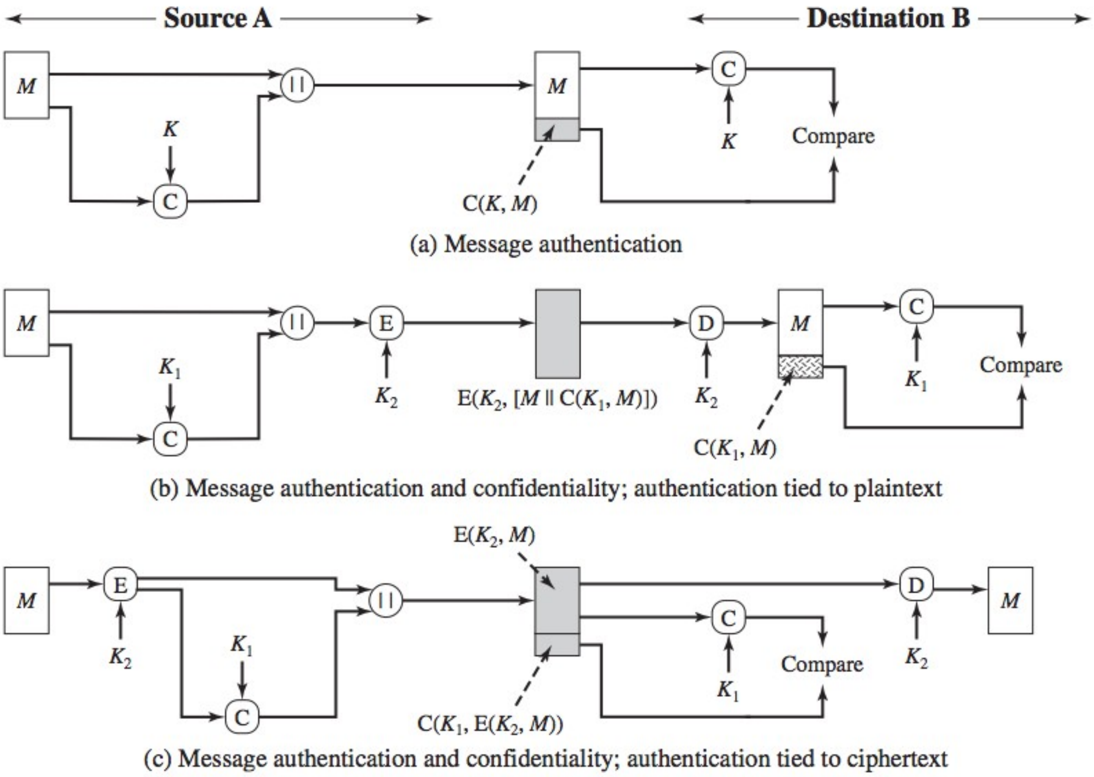

Figure 12.4 Basic Uses of Message Authentication code (MAC)

Part B: Symmetric Key Distribution protocol:

Q1 This is a variation of the protocol discussed in the class symmetric key description involving n users and a KDC. Here every user decides to generate random number themselves for the communication they seek to start.

The steps are as follows:

1. A generates a random number R and sends to the KDC his name A, destination B, and E(Ka, R).

2. KDC responds by sending E(Kb, R) to A.

3. A sends E(R, M) together with E(Kb, R) to B.

4. B knows Kb, thus decrypts E(Kb, R), to get R and will subsequently use R to decrypt

E(R, M) to get M.

Is this secure?

PS: Assume all other assumptions made in the protocol. All users share a master key with KDC, all communications can be observed by the users.

Q2. Consider the following protocol, designed to let A and B decide on a fresh, shared session key K=AB. We assume that they already share a long-term key K_{AB}.

1. A $\rightarrow$ B: A, N_A.

2. B $\rightarrow$ A:E(K_{AB}, [N_A, K'_{AB}])

3. A $\rightarrow$ B:E(K'_{AB}, N_A)

a. We first try to understand the protocol designer's reasoning:

— Why would A and B believe after the protocol ran that they share K'_{AB} with the

other party?

—Why would they believe that this shared key K'_{AB} is fresh?

In both cases, you should explain both the reasons of both A and B, so your answer should complete the sentences

A believes that she shares K'_{AB} with B since…

B believes that he shares K'_{AB} with A since…

A believes that K'_{AB} is fresh since…

B believes that K'_{AB} is fresh since…

b. Assume now that A starts a run of this protocol with B. However, the connection is intercepted by the adversary C. Show how C can start a new run of the protocol using reflection, causing A to believe that she has agreed on a fresh key with B (in spite of the fact that she has only been communicating with C). Thus, in particular, the belief in (a) is false.

c. Propose a modification of the protocol that prevents this attack.