COMP90043: Cryptography and security

Week 7 Workshop Activity

1. What is a message authentication code?

It is an authenticator that is a cryptographic function of both the data to be authenticated and a secret key.

2. What types of attacks are addressed by message authentication?

Masquerade: Insertion of messages into the network from a fraudulent source. This includes the creation of messages by an opponent that are purported to come from an authorized entity. Also included are fraudulent acknowledgments of message receipt or non-receipt by someone other than the message recipient.

Content modification: Changes to the contents of a message, including insertion, deletion, transposition, and modification.
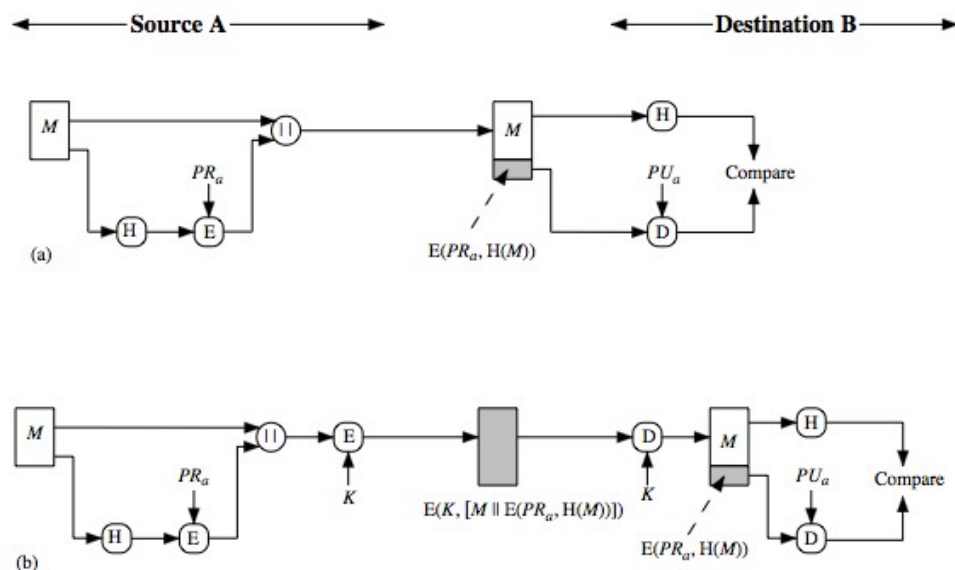
Sequence modification: Any modification to a sequence of messages between parties, including insertion, deletion, and reordering.

Timing modification: Delay or replay of messages. In a connection-oriented application, an entire session or sequence of messages could be a replay of some previous valid session, or individual messages in the sequence could be delayed or replayed. In a connectionless application, an individual message (e.g., datagram) could be delayed or replayed.

3. What is the main difference between hash functions and Message Authentication codes?

A hash function, by itself, does not provide message authentication. A secret key must be used in some fashion with the hash function to produce authentication. A MAC, by definition, uses a secret key to calculate a code used for authentication.

4. In what ways a hash value can be secured so as to provide message authentication?
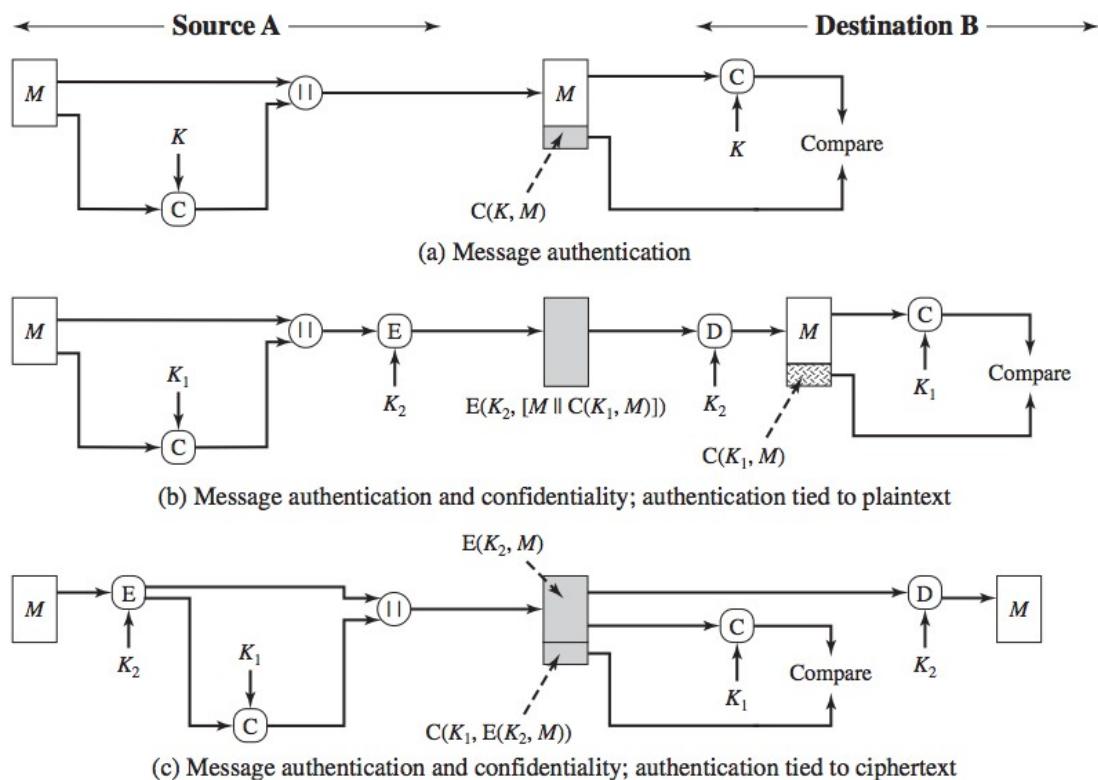
Source A ←→ **Destination B**

$C(K, M)$

(a) Message authentication

$E(K_2, [M \| C(K_1, M)])$

$C(K_1, M)$

(b) Message authentication and confidentiality; authentication tied to plaintext

$E(K_2, M)$

$C(K_1, E(K_2, M))$

(c) Message authentication and confidentiality; authentication tied to ciphertext

Figure 12.4 Basic Uses of Message Authentication code (MAC)

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.

Suppose that John sends an authenticated message to Mary. The following disputes that could arise:

- Mary may forge a different message and claim that it came from John. Mary would simply have to create a message and append an authentication code using the key that John and Mary share.

- John can deny sending the message. Because it is possible for Mary to forge a message, there is no way to prove that John did in fact send the message.

7. What are the properties a digital signature should have?

- It must be able to verify the author and the date and time of the signature.
- It must be able to authenticate the contents at the time of the signature
- The signature must be verifiable by third parties, to resolve disputes.

8. What are some threats associated with a direct digital signature scheme?

- The validity of the scheme depends on the security of the sender's private key. If a sender later wishes to deny sending a particular message, the sender can claim that the private key was lost or stolen and that someone else forged his or her signature.

- Another threat is that some private key might actually be stolen from X at time T. The opponent can then send a message signed with X's signature and stamped with a time before or equal to T.