COMP90043 Cryptography and Security
Semester 2, 2020, Workshop Week 8

Preparation: We may not have time to cover all questions. Please come prepared by at least reading on MAC, Hash and Signatures. Please start with Q1, Q2, Q4, Q8 and then attempt all other questions.

Exercises:

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. Discuss the following scenarios for using MACs for implementing authentication and confidentiality discussed in lectures.

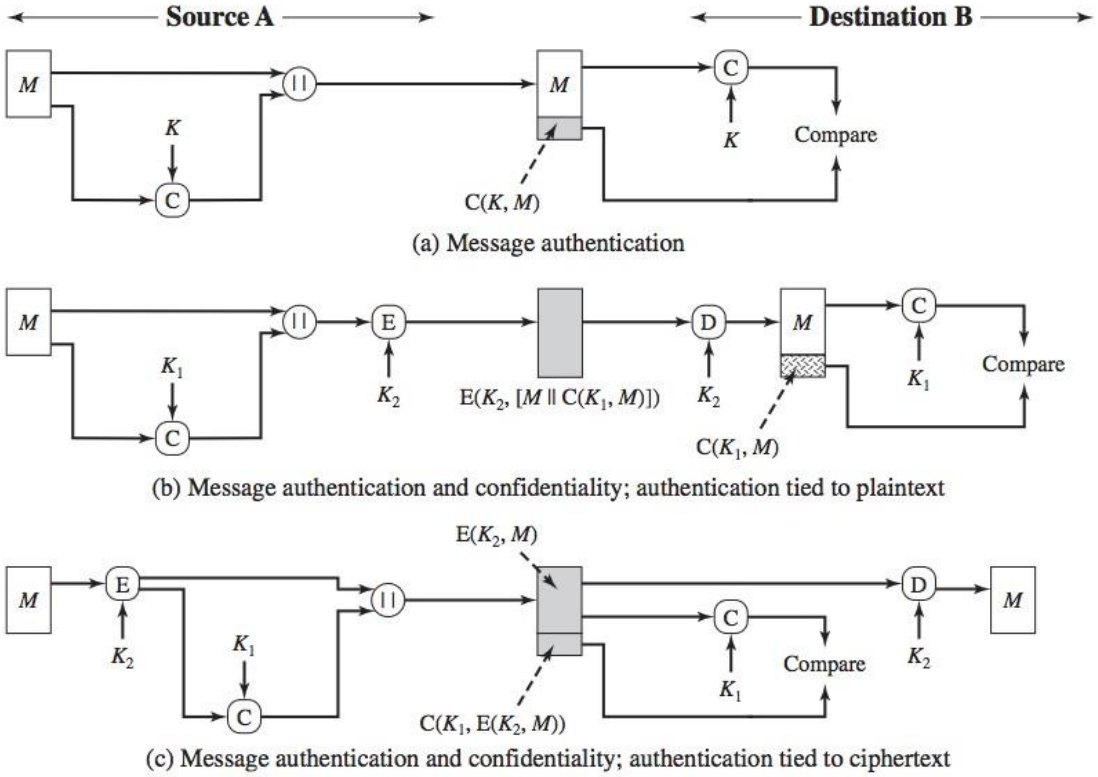

Figure 12.4 Basic Uses of Message Authentication code (MAC)

5. List two disputes that can arise in the context of message authentication.
6. What are the properties a digital signature should have?
7. What are some threats associated with a direct digital signature scheme?
8. List ways in which secret keys can be distributed to two communicating parties.
9. What is the difference between a session key and a master key?
10. What is a nonce?
11. Explain the problems with key management and how it affects symmetric cryptography?