COMP90043 Cryptography and Security

Semester 2, 2021, Workshop Week 7

Questions

1. What are the advantages of using Hash functions in digital signatures?
2. What characteristics are needed in a secure hash function?
3. What is the difference between weak and strong collision resistance?
4. Is it possible to use a hash function to construct a DES-like block cipher?
5. Explain the birthday paradox. What is the main implication of this for hash function?
6. Discuss the following scenarios for using MACs for implementing authentication and confidentiality discussed in lectures.

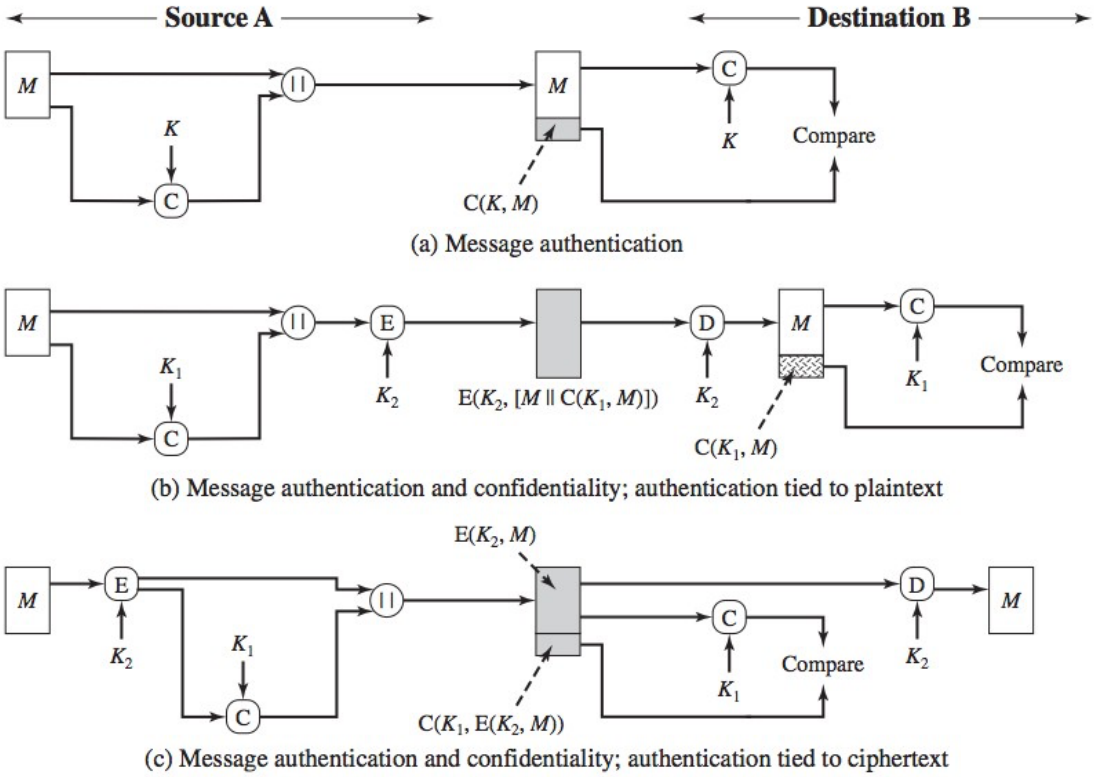

Figure 12.4 Basic Uses of Message Authentication code (MAC)

7. List two disputes that can arise in the context of message authentication.
8. What are some threats associated with a direct digital signature scheme?
9. What is the main difference between hash functions and Message Authentication codes?

Homework questions:

1. Explain how you can use RSA encryption function to construct a digital signature scheme.
2. Name three important hash functions used in practice.
3. Discuss how the security of the hash functions depends on the length of the hash.
4. Why CRC checksum cannot be used as a secure hash function?
5. What is a message authentication code?
6. What is Timing Attack? How can Timing Attacks be prevented?
7. What types of attacks are addressed by message authentication?
8. What are the properties a digital signature should have?