COMP90043: Cryptography and security

Workshop-7

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?