COMP90043 Cryptography and Security

Semester 2, 2020, Workshop Week 7

Questions

1. What are the advantages of using Hash functions in digital signatures?

2. Explain how you can use RSA encryption function to construct a digital signature scheme.

3. What characteristics are needed in a secure hash function?

4. What is the difference between weak and strong collision resistance?

5. Is it possible to use a hash function to construct a DES-like block cipher?

6. Explain the birthday paradox. What is the main implication of this for hash function?

7. Name three important hash functions used in practice.

8. Discuss how the security of the hash functions depends on the length of the hash.

9. Why CRC checksum cannot be used as a secure hash function?

10. What is Timing Attack? How can Timing Attacks be prevented?