Royal Holloway, University of London

IY2760/DC3760 Introduction to information security

Practice Exam Paper 2024-25

Time Allowed: **Two hours**

Note:

- You are not required to write *essays*.
- Write short sentences.
- Try to make your handwriting as clear as possible so there is no misunderstanding of your answer.
- I will accept bullet points too, as long as they are coherent and correct.
- No marks will be deducted for stylistic atrocities.
- No marks will be deducted for grammatical errors as long as the meaning is clear.
- But no marks will be given for the display of irrelevant knowledge! Indeed marks may be withheld if irrelevant knowledge contradicts nearly correct answers.

SLN
2024-25

1. *Security concepts, elements of cryptography.*

   (a) Information security is often defined in terms of 'CIA'. Explain what these three letters stand for, and briefly define each term.

   [9]

   (b) We say that a simple substitution cipher is not computationally secure against a ciphertext-only attack, given enough ciphertext.

      i. Explain what is meant by "computationally secure".

      ii. Why is "given enough ciphertext" in the above statement important?

      (Only brief answers are required. Do not write more than two or three lines.)

   [10]

   (c) What is Kerckhoffs' Principle?

   [6]

2. *Symmetric key cryptography, integrity mechanisms*

   (a) Discuss the speed of encryption and the error propagation properties of stream ciphers. [8]

   (b) i. Describe 2-key triple DES, 2TDES. [2]

      ii. What are the key length and block size of DES? [2]

      iii. What are the key length and block size of 2TDES? [2]

   (c) Suppose you store a file on a hard drive. You do not expect anyone to tamper with the file.

      What can you do to ensure that when you retrieve the file it is uncorrupted? [4]

   (d) What security services can a message authentication code (MAC) provide for a transmitted message? Name one widely used MAC algorithm. [7]

3. *Public key cryptography, entity authentication, digital signature, key establishment.*

   (a) What are two main characteristics of asymmetric cryptosystems in relation to the use of cryptographic keys?

   [4]

   (b) In authentication protocols, time-stamps can be used to provide "freshness checking" for protocol messages. Provide an advantage and a disadvantage for this mechanism.

   [8]

   (c) Describe how RSA can be used to construct a digital signature scheme with appendix (without message recovery). Make sure you describe what must be made public and what must be kept secret. [9]

   (d) Give one reason why two parties who already share a long-term key would want to establish session keys for communication.

   [4]

4. *Computer and network security.*

   (a) An access control matrix has rows indexed by subjects and columns indexed by objects. How does the reference monitor decide whether to grant a request if a subject s requests access to object r with access rights a?

   Give a brief explanation why access control matrices are not suitable for direct implementation.

   [8]

   (b) Describe briefly one role of firewalls in an organisation's network.

   [4]

   (c) Describe briefly one factor that contributes to software vulnerability.

   [5]

   (d) Explain what signature-based and anomaly-based intrusion detection systems are. [8]