Monash University

Semester One Examination Period 20XX

Faculty of Information Technology
Sample Exam Paper

EXAM CODES:	**FIT3031**
TITLE OF PAPER:	**Information & Network Security**
EXAM DURATION:	2 hours writing time
READING TIME:	10 minutes

THIS PAPER IS FOR STUDENTS STUDYING AT:(tick where applicable)

□ Berwick
☼ Caulfield
□ Pharmacy
☒Clayton
□ Gippsland
□ Other (specify)
□ Malaysia
□ Peninsula
□ Off Campus Learning
□ Enhancement Studies
□ Open Learning
☼ Sth Africa

During an exam, you must not have in your possession, a book, notes, paper, electronic device/s, calculator, pencil case, mobile phone or other material/item which has not been authorised for the exam or specifically permitted as noted below. Any material or item on your desk, chair or person will be deemed to be in your possession. You are reminded that possession of unauthorised materials in an exam is a discipline offence under Monash Statute 4.1.

No examination papers are to be removed from the room.

AUTHORISED MATERIALS

CALCULATORS	□ **YES**	☼ **NO**
OPEN BOOK	□ **YES**	☼ **NO**
SPECIFICALLY PERMITTED ITEMS	□ **YES**	☼ **NO**

INSTRUCTIONS

1. Please answer **ALL** of them.
2. Start the answer to each question on a new page.
3. Write on one side of the paper only.
4. Total marks - 100. This exam contributes 60% to your result for this unit.

Important Disclaimer: Preparing for Your EXAM

*It is advisable to complete your required preparation(s) as quickly as possible and be prepared at least 1 weeks before your exam. The sample exam and coverage can provide **ONLY** sample preparation materials to help you prepare for the exam. The Sample exam Questions above **ARE NOT** designed to provide you with all exam coverage for final exam assessment of your current skill levels, but to orient you to the style of question used in the actual final exam assessment. **DO NOT** treat the sample questions as the **ONLY** scope for your practice exam, or as the actual exam. The final Questions will vary considerably in their content, coverage and the level of difficulty.*

Full Marks: 80 marks

There are TWO sections. ANSWER ALL QUESTIONS in both sections in your answer book.

Section A. Multiple Choice. (30 marks) Choose only one answer that best completes the statement. 2 mark for each question.

1. Which of the following algorithm is a symmetric encryption algorithm?
   A. RSA
   B. Diffie-Hellman
   C. SHA-256
   D. DES

2. Which of the following attack(s) is/are active attack?
   (i) Replay
   (ii) Modification of Message
   (iii) Denial-of-Service
   A. (i) only
   B. (i) and (iii)
   C. (ii) and (iii)
   D. All of the above

3. Which of the following statement(s) regarding symmetric encryption is/are not true?
   A. The encryption key is the same as decryption key
   B. Symmetric key encryption is slower than asymmetric key encryption
   C. AES can be speed up using hardware module
   D. All of the above statements are not true

4. Asymmetric encryption can solve the___________problem(s) of symmetric encryption.
   A. key distribution
   B. integrity
   C. efficiency
   D. all of the above

5. Which of the following statement(s) regarding a hash function is/are true?
   (i) The output length of a hash function depends on the input message.
   (ii) It is collision-resistant.
   (iii) It is one-way.
   A. (i) only
   B. (ii) only
   C. (ii) and (iii)
   D. None of the above

6. In IPSec,__________encrypts the whole IP packet.
   A. tunnel mode
   B. transport mode
   C. host-to-host mode
   D. every mode

7. Which of the following issue(s) is/are related to WEP?
   A. No mutual authentication
   B. Directly uses master key
   C. IV value is too small
   D. All of the above

8. __________is used to secure email.
   A. SMTP
   B. S/MIME
   C. Telnet
   D. Kerberos

9. Trapdoors are left during the software___________phase.
   A. authentication
   B. certification
   C. development
   D. execution

10. The security of Diffie-Hellman Algorithm relies on the__________problem.
    A. factorization
    B. subset sum
    C. discrete logarithm (DL)
    D. learning with errors (LWE)

11. IPSec is used to secure the___________layer.
    A. application
    B. TCP
    C. IP
    D. physical

12. X.509 is a standard of___________.
    A. digital signature
    B. email security
    C. wireless-LAN security
    D. digital certificate

13. Which of the following activities are examples of Intrusion?
   (i) Cracking password
   (ii) Distributing pirated software

   (iii) Using e-banking service from a web browser in a library public computer during opening hours

   A. (i) and (ii)
   B. (ii) and (iii)
   C. (i) and (iii)
   D. All of the above

14. Which of the following statement(s) describe(s) correctly the difference(s) between a virus and a worm?
   A. A virus cannot be spread without a human action, but a worm has the capacity to travel without any human action.
   B. A virus does not have the dormant phase, but a worm does have.
   C. In the propagation phase, a virus searches for other systems but a worm only searchers for other programs running within the same system.
   D. All of the above are correct

15. Which of the following is/are the limitation(s) of a firewall?
   A. Cannot protect from attacks bypassing it
   B. Cannot protect against internal threat
   C. All of the above are limitations of a firewall
   D. There is no limitation of a firewall

In addition, please go through all the weekly Quizzes we have in the Moodle!

Important Disclaimer: Preparing for Your EXAM

*It is advisable to complete your required preparation(s) as quickly as possible and be prepared at least 1 weeks before your exam. The sample exam and coverage can provide **ONLY** sample preparation materials to help you prepare for the exam. The Sample exam Questions above **ARE NOT** designed to provide you with all exam coverage for final exam assessment of your current skill levels, but to orient you to the style of question used in the actual final exam assessment. **DO NOT** treat the sample questions as the **ONLY** scope for your practice exam, or as the actual exam. The final Questions will vary considerably in their content, coverage and the level of difficulty.*

Section B: Questions & Answers. (70 marks)

1. (a) Briefly explain the following security services:
   (i) Confidentiality
   (ii) Access Control
   (iii) Integrity
   (iv) Availability

   (b) Which of the above security services (i) – (iv) can a signcryption provide? Explain your answer.

2. (a) Which of the following (n,e) pair is a correct RSA public key?
   (i) n = 35, e = 3
   (ii) n = 85, e = 3

   Explain your answer. (3 marks)

   (b) For the correct RSA public key in part (a), what is the corresponding private key d? Show your steps. (3 marks)

   (c) Use the correct RSA public key in part (a) to encrypt a plaintext m=5. Show your steps.

3. Which Cipher Block Modes of Operations, ECB or CBC, is more commonly used? Give one advantage of using CBC over ECB and one disadvantage of using CBC over ECB. (3 marks)

4. Give any FOUR security services that IPSec can provide.

5. Give THREE possible attacks that involve password capture.

6.
   (a) What are the two default policies of packet filtering firewall?
   (b) Give TWO advantages and THREE disadvantages of using packet filtering firewall over application level gateway firewall.

7.
   a) What is Domain Keys Identified Mail (DKIM)?
   b) How is the DKIM e-mail authentication service different when compared to S/MIME or PGP? Give TWO differences.

8. Answer the following questions:
   a) Explain any two examples of security violations that can be experienced in the transmission of information over the network. For each example given, name the type of security service that applies to such violations.
   b) There are two major concerns with regards to where to implement the security mechanisms designed to combat security violations. Briefly explain these two concerns.
   c) Explain briefly polymorphic virus and metamorphic virus?
   d) List the six main security services defined by the X800 OSI security architecture?

9.

a) Suppose Bob chooses n=35 as his RSA modulus and chooses e=7 as his public key exponent so that his public key (n, e) = (7, 35). Calculate his private key exponent d.
b) In asymmetric encryption, a sender can deny his public key and a hacker can create a false key to impersonate someone. Explain how it can be ensured that the public key belongs to the entity that it claims it belongs to?

10.

a) What hash function is used in PGP and what is the length of the message digest? What is the use of detached signature supported by PGP?
b) Why does PGP generate a signature before applying compression?

11.

a) In relation to IPSec, answer the following:
   i. Explain how IPSec can prevent a replay attack.
   ii. Explain the difference between transport and tunnel mode operation of IPSec? When is it suitable to use each of the above modes of operation?

12.

a) What security areas are addressed by IEEE 802.11i? Briefly describe the four IEEE 802.11i phases of operation.
b) What is the difference between an SSL connection and an SSL session?
c) Describe services that are provided by the SSL Record Protocol.

13.

a) List and briefly define three classes of intruders.
b) Having an Intrusion Detection System (IDS) in a network is crucial for ensuring security. What are the benefits that can be provided by an intrusion detection system?
c) What are the characteristics of stealth and polymorphic viruses that make them difficult to detect? Name two advanced antivirus techniques.

14. Firewalls are a viewed as a means to protect internal networks from external networks. In relation to this, explain the following:

a) List three design goals for a firewall.
b) What is a DMZ network and what types of systems would you expect to find on such networks.
c) What is the difference between an external and internal firewall?

In addition, please go through all the tutorials solutions we have in the Moodle!

Important Disclaimer: Preparing for Your EXAM

*It is advisable to complete your required preparation(s) as quickly as possible and be prepared at least 1 weeks before your exam. The sample exam and coverage can provide **ONLY** sample preparation materials to help you prepare for the exam. The Sample exam Questions above **ARE NOT** designed to provide you with all exam coverage for final exam assessment of your current skill levels, but to orient you to the style of question used in the actual final exam assessment. **DO NOT** treat the sample questions as the **ONLY** scope for your practice exam, or as the actual exam. The final Questions will vary considerably in their content, coverage and the level of difficulty.*