Office Use Only

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: 3 hours writing time

READING TIME: 10 minutes

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

☐ Berwick	☐ Clayton	☑ Malaysia	☐ Off Campus Learning	☐ Open Learning
☑ Caulfield	☐ Gippsland	☐ Peninsula	☐ Enhancement Studies	☑ Sth Africa
☐ Pharmacy	☐ Other (specify)			

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. PART-B-There are **SEVEN** questions, please answer **ALL** of them.
2. PART-A MCQ T/F & SHORT-WORD ANSWERS
3. Write on one side of the paper only.
4. Total marks - 100. This exam contributes 60% to your result for this unit.

Answer the following questions:

1.

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.

(8+5=13 marks)

2.

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.

c. Explain why sending **m + MD5 (m),** which denotes message **m** concatenated with its digest, does not guarantee message integrity for **m**. What can you do make it secure?

(7+7+6=20 marks)

3.

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?

(6+6 = 12 marks)

4.

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?

b.

i. Explain SSL protocol?

ii. Explain what is HTTPS? & iii. Explain SSH protocol?

(4+(5+3)+2+4=18 marks)

5.

a. What security areas are addressed by IEEE 802.11i? Briefly describe the four IEEE 802.11i phases of operation.

b. WAP end-to-end security has a security gap in between. Describe 2 possible solutions to solving this problem?

c. What is the difference between an SSL connection and an SSL session?

.

d. Describe services that are provided by the SSL Record Protocol.

((2+4)+4+4+4=18 marks)

6.

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.

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

(i) List three design goals for a firewall.

(ii) What is a DMZ network and what types of systems would you expect to find on such networks?

(iii) What is the difference between an external and internal firewall?

(3+3+(4+1)+3+3+2=19 marks)