CONFIDENTIAL

Infrastructure University
Kuala Lumpur

FINAL EXAMINATION
MARCH SEMESTER 2016

BACHELOR OF INFORMATION TECHNOLOGY (HONS) IN NETWORK TECHNOLOGY
BACHELOR OF INFORMATION TECHNOLOGY (HONS) IN SOFTWARE ENGINEERING
BACHELOR OF COMPUTER SCIENCE (HONS)

NETWORK AND DATA SECURITY
(BTN 303)

(TIME : 3 HOURS)

MATRIC NO. : □□□□□□□□□

IC. / PASSPORT NO. : □□□□□□□□□□□□□□

LECTURER : **WONG FUI FUI**

GENERAL INSTRUCTIONS

1. This question booklet consists of 7 printed pages including this page.
2. Answer **ALL** questions from **Section A** and **C** in the **Answer Booklet**.
3. Answer ANY **FOUR (4)** questions from **Section B** in the **Answer Booklet**.

CONFIDENTIAL

INSTRUCTIONS: **TIME:** ***3 HOURS***

SECTION A (40 MARKS)

There are TWELVE (12) questions in this section. Answer ALL Questions in the Answer Booklet.

1. For each of the following assets, assign a low, moderate, or high impact level for the loss of confidentiality, availability, and integrity, respectively. Justify your answers.

   a) An automated teller machine (ATM) in which users provide a personal identification number (PIN) and a card for account access.

   (2 marks)

   b) A telephone switching system that routes calls through a switching network based on the telephone number requested by the caller.

   (2 marks)

   c) A desktop publishing system used to produce documents for various organizations.

   (2 marks)

   d) A hospital patient's allergy information stored in a database.

   (2 marks)

2. List **THREE (3)** major security threats on the Internet, and give a short description of each.

   (6 marks)

3. Why is deriving a security policy difficult?

   (2 marks)

4. List and describe the **FOUR (4)** basic security techniques.

   (4 marks)

5. What is a digital certificate?

   (2 marks)

6. What are the **TWO (2)** goals of a VPN system?

   (4 marks)

7. What is the difference between an internal and an external firewall?

(2 marks)

8. What is a message authentication code (MAC)?

(2 marks)

9. What is a nonce?

(2 marks)

10. For what applications is SSH useful?

(2 marks)

11. How does PGP use the concept of trust?

(2 marks)

12. Give **TWO (2)** examples of applications of IPsec.

(4 marks)

SECTION B (40 MARKS)

There are SIX (6) questions in this section. Answer ANY FOUR (4) questions in the Answer Booklet.

1.

a) A Feistel cipher is used in the DES algorithm. Draw a diagram to illustrate the structure proposed by Feistel

(6 marks)

b) Why is the middle portion of 3DES a decryption rather than an encryption?

(4 marks)

2.

a) What are the **FOUR (4)** key factors contributing to the higher security risk of wireless network compared to wired network.

(8 marks)

b) Explain how a man-in-the-middle attack on a Wi-Fi network can be defeated.

(2 marks)

3.

a) Compare and contrast any **FOUR (4)** block cipher modes of operation.

(8 marks)

b) List the **TWO (2)** modes that make it possible to convert a block cipher into a stream cipher.

(2 marks)

4.

a) Briefly describe any **THREE (3)** requirements must a public-key cryptosystems fulfill to be a secure algorithm.

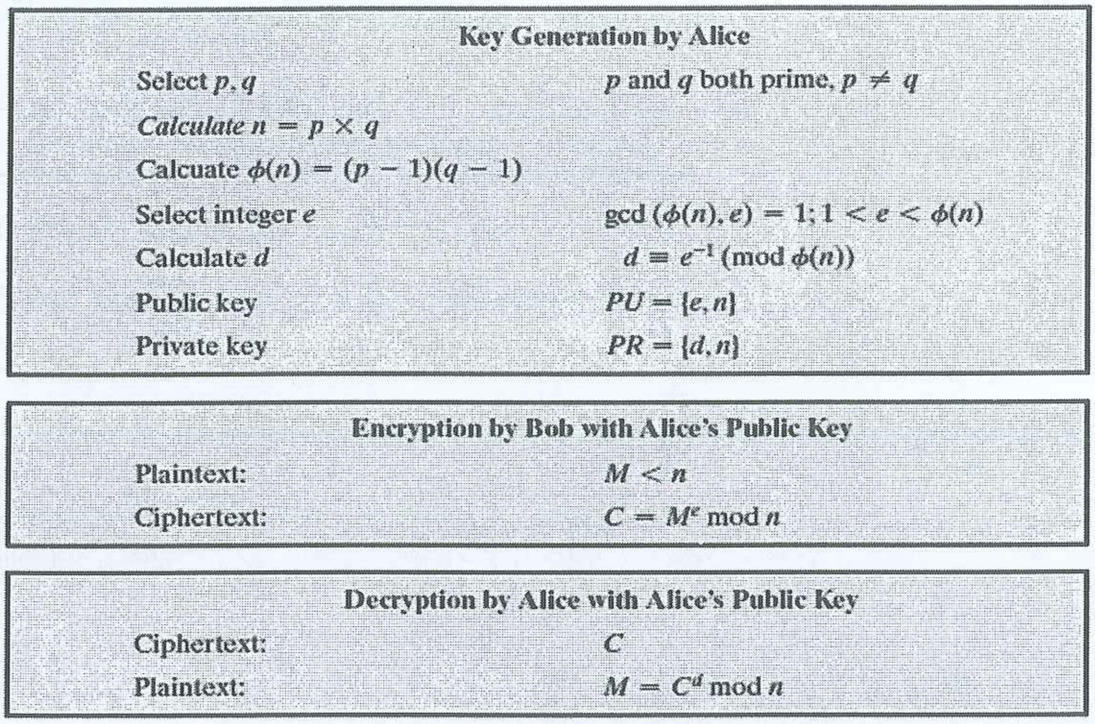
(6 marks)

b) List and describe the **TWO (2)** possible approaches to attacking the RSA algorithm.

(4 marks)

5. Perform encryption and decryption using the RSA algorithm, as in Figure 1, for the following:

$p = 17; q = 11, e = 7$; plaintext $M = 88$;



Key Generation by Alice	
Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calcuate $\phi(n) = (p - 1)(q - 1)$	
Select integer e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} (\mathrm{mod}\ \phi(n))$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

Encryption by Bob with Alice's Public Key	
Plaintext:	$M < n$
Ciphertext:	$C = M^e \bmod n$

Decryption by Alice with Alice's Public Key	
Ciphertext:	C
Plaintext:	$M = C^d \bmod n$

Figure 1: The RSA Algorithm

a) In a public-key system using RSA, Bob sent a plaintext M = 88 to Alice using her public key. What is the generated ciphertext C?

(4 marks)

b) Alice decrypts using her private key. Show the complete working process how to find the plaintext M?

(6 marks)

6.

a) Message Authentication does not protect the two parties against each other. For example, suppose that John sends an authenticated message to Mary. What are the **TWO (2)** possible forms of disputes between the two parties?

(4 marks)

b) What are the **THREE (3)** properties a digital signature should have?

(6 marks)

SECTION C **(20 MARKS)**

There is ONE (1) question in this section. Answer this Question in the Answer Booklet.

1. SMTP (Simple Mail Transfer Protocol) is the standard protocol for transferring mail between hosts over TCP. A TCP connection is set up between a user agent and a server program. The server listens on TCP port 25 for incoming connection requests. The user end of the connection is on a TCP port number above 1023. Suppose you wish to build a packet filter rule set allowing inbound and outbound SMTP traffic. You generate the following ruleset:

Rule	Direction	Src Addr	Dest Addr	Protocol	Dest Port	Action
A	In	External	Internal	TCP	25	Permit
B	Out	Internal	External	TCP	>1023	Permit
C	Out	Internal	External	TCP	25	Permit
D	In	External	Internal	TCP	>1023	Permit
E	Either	Any	Any	Any	Any	Deny

a) Describe the effect of each rule.

(10 marks)

b) Your host in this example has IP address 172.16.1.1. Someone tries to send e-mail from a remote host with IP address 192.168.3.4. If successful, this generates an SMTP dialogue between the remote user and the SMTP server on your host consisting of SMTP commands and mail. Additionally, assume that a user on your host tries to send e-mail to the SMTP server on the remote system. Four typical packets for this scenario are as shown:

Packet	Direction	Src Addr	Dest Addr	Protocol	Dest Port	Action
1	In	192.168.3.4	172.16.1.1	TCP	25	?
2	Out	172.16.1.1	192.168.3.4	TCP	1234	?
3	Out	172.16.1.1	192.168.3.4	TCP	25	?
4	In	192.168.3.4	172.16.1.1	TCP	1357	?

Indicate which packets are permitted or denied and which rule is used in each case.

(8 marks)

c) Someone from the outside world (10.1.2.3) attempts to open a connection from port 5150 on a remote host to the Web proxy server on port 8080 on one of your local hosts (172.16.3.4), in order to carry out an attack. Typical packets are as follows:

Packet	Direction	Src Addr	Dest Addr	Protocol	Dest Port	Action
5	In	10.1.2.3	172.16.3.4	TCP	8080	?
6	Out	172.16.3.4	10.1.2.3	TCP	5150	?

Will the attack succeed? Give details.

(2 marks)

*** END OF QUESTIONS ***