CONFIDENTIAL

Infrastructure University
Kuala Lumpur

FINAL EXAMINATION
SEPTEMBER / OCTOBER SEMESTER 2015

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 8 printed pages including this page.
2. In Section A, answer **ALL questions** in the **ANSWER BOOKLET.**
3. In Section B, answer **ALL questions** in the **ANSWER BOOKLET.**
4. In Section C, answer **ANY ONE (1) question** in the **ANSWER BOOKLET.**
5. The total marks is 100.

CONFIDENTIAL

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

SECTION A **(40 MARKS)**

There are SEVEN (7) 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 organization managing public information on its Web server.

   b) A law enforcement organization managing extremely sensitive investigative information.

   c) A financial organization managing routine administrative information (not privacy-related information).

   d) An information system used for large acquisitions in a contracting organization contains both sensitive, pre-solicitation phase contract information and routine administrative information. Assess the impact for the two data sets separately and the information system as a whole.

   e) A power plant contains a SCADA (supervisory control and data acquisition) system controlling the distribution of electric power for a large military installation. The SCADA system contains both real-time sensor data and routine administrative information. Assess the impact for the two data sets separately and the information system as a whole.

(10 marks)

2. What is the difference between a block cipher and a stream cipher?

(4 marks)

3. What is a meet-in-the-middle attack?

(2 marks)

4. What are the roles of the public and private key?

(4 marks)

5. Describe **FOUR (4)** main cloud-specific security threats.

(8 marks)

6. List and describe **THREE (3)** design goals for a firewall.

(6 marks)

7. Give **THREE (3)** examples of applications of IPsec

(6 marks)

SECTION B (40 MARKS)

There are THREE (3) questions in this section. Answer ALL Questions in the Answer Booklet.

1.

a) Explain how the security of DES may be increased by the use of 3DES. By how much does 3DES improve the strength of DES?

(2 marks)

b) Compare AES to DES. For each of the following elements of DES, indicate the comparable element in AES or explain why it is not needed in AES.

i. XOR of subkey material with the input to the f function

ii. XOR of the f function output with the left half of the block

iii. f function

iv. permutation P

v. swapping of halves of the block

(10 marks)

2.

a) What is a key distribution center?

(2 marks)

b) One local area network vendor provides a key distribution facility, as illustrated in Figure 1. Describe the scheme.

(10 marks)

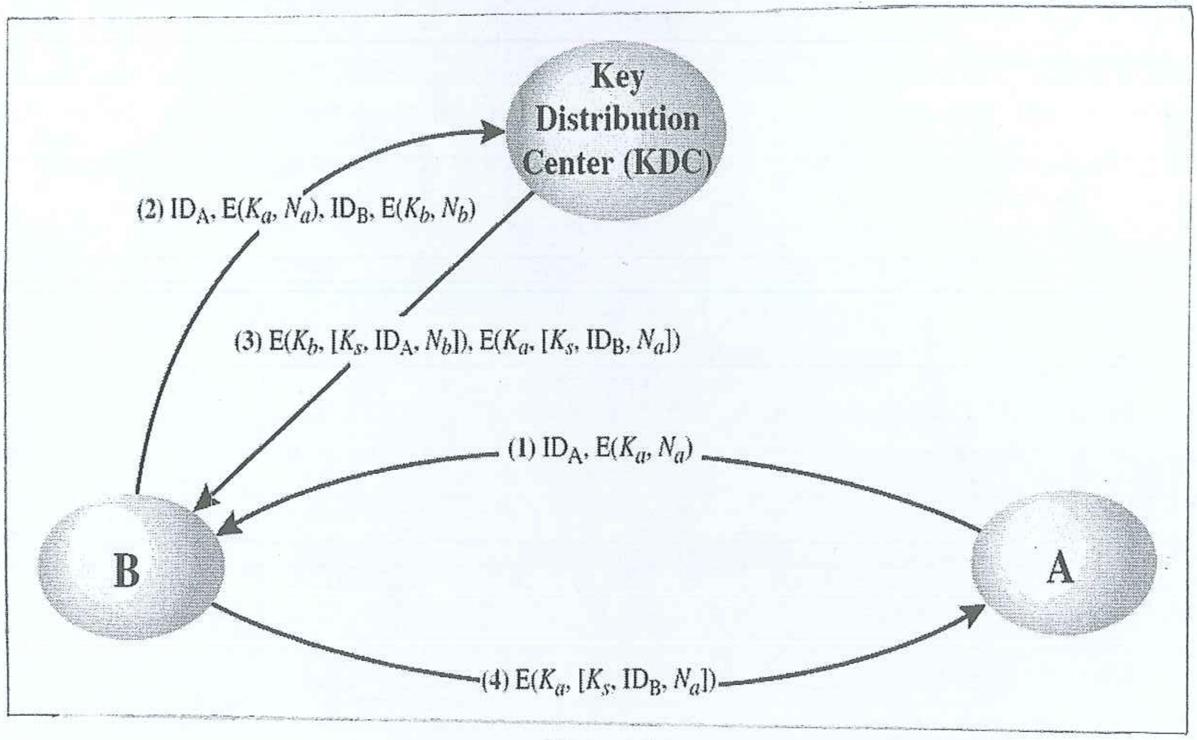

Key Distribution Center (KDC)
(2) ID_A, $E(K_a, N_a)$, ID_B, $E(K_b, N_b)$
(3) $E(K_b, [K_s, \mathrm{ID}_A, N_b])$, $E(K_a, [K_s, \mathrm{ID}_B, N_a])$
(1) ID_A, $E(K_a, N_a)$
B
A
(4) $E(K_a, [K_s, \mathrm{ID}_B, N_a])$

Figure 1

3.

a) Explain how public key cryptography may be used for identification.

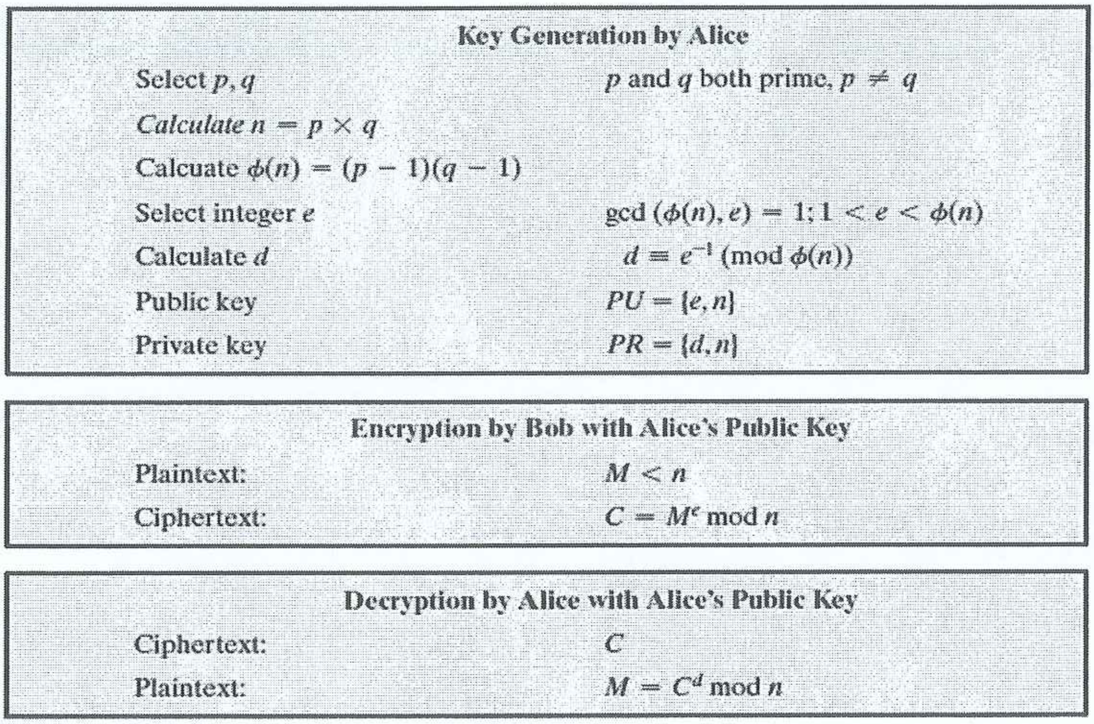
(2 marks)

b) Alice and Bob participate in a public-key infrastructure that enables them to exchange legally binding digital signatures. Name two reasons why, for some purposes, Alice might prefer to use a digital signature, instead of a message authentication code, to protect the integrity and authenticity of her messages to Bob.

(4 marks)

c) Perform encryption and decryption using the RSA algorithm, as in Figure 2, for the following:

p = 73; q = 151, e = 11; plaintext M = 3314;



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	$d \equiv e^{-1} \pmod{\phi(n)}$
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 2: The RSA Algorithm

i. In a public-key system using RSA, Bob sent a plaintext M = 3314 to Alice using her public key. What is the generated ciphertext C?

(4 marks)

ii. A hacker intercept the ciphertext C from Bob sent to Alice. Show the complete working process how to find the plaintext M?

(6 marks)

SECTION C (20 MARKS)

There are TWO (2) question in this section. Answer ANY ONE (1) question in the Answer Booklet.

1.

Secure Your Home Wireless Network

Home wireless networks are becoming more common every day. These networks provide the ability to have multiple computers set up all over your house or apartment without a mess of wires running through your home. With a wireless network and a laptop, you can surf the web from your couch, your kitchen table or even your bed.

However, with this increased convenience comes increased dangers. Hackers and identity thieves are targeting home wireless networks more than ever, looking for people that have simply plugged in their wireless router and taken no steps to protect their network. Being that careless is the same as moving into your home, but then leaving every door and window unlocked, simply hoping that no one will come in and steal your belongings. Only instead of walking off with your TV, wireless hackers are looking to steal your passwords, your credit card numbers and your bank account information over your own wireless network. Also, people may illegally download movies, music and other copyright protected material over your network without your knowledge. If that occurs, you can still be blamed for the illegal downloads.

While it will take a little effort to secure your home network, it is essential to do so. You can lock down your wireless network so you and your family can fully enjoy it, but intruders cannot get in.

a) Identify **FOUR (4)** type of wireless network threats

(8 marks)

b) Identify **THREE (3)** steps for securing your home wireless network

(12 marks)

2.

Secure Your Mobile Network

Mobile devices have become an essential element for organizations as part of the overall network infrastructure. Mobile devices such as smartphones, tablets, and memory sticks provide increased convenience for individuals as well as the potential for increased productivity in the workplace. Every day, more users are using mobile devices to access corporate services, view corporate data, and conduct business. Because of their widespread use and unique characteristics, security for mobile devices is a pressing and complex issue. Moreover, many of these devices are not controlled by the administrator, meaning that sensitive enterprise data is not subject to the enterprise's existing compliance, security, and Data Loss Prevention policies.

In essence, an organization needs to implement a security policy through a combination of security features built into the mobile devices and additional security controls provided by network components that regulate the use of the mobile devices.

Mobile devices need additional, specialized protection measures beyond those implemented for other client devices, such as desktop and laptop devices that are used only within the organization's facilities and on the organization's networks.

a) Identify **FOUR (4)** type of mobile network threats.

(8 marks)

b) Identify **THREE (3)** principal elements of a mobile device security strategy.

(12 marks)

***** END OF QUESTIONS *****