CONFIDENTIAL

Infrastructure University Kuala Lumpur

SUNWAY INT'L BUSINESS SCHOOL

FINAL EXAMINATION
JUNE SEMESTER 2018

NETWORK AND DATA SECURITY
(CSC 2730)

(TIME : 3 HOURS)

MATRIC NO. : | | | | | | | | | |

IC. / PASSPORT NO. : | | | | | | | | | | | | | | |

LECTURER : BHAS RAJ PATHAK

GENERAL INSTRUCTIONS

1. This question booklet consists of 5 printed pages including this page.
2. Answer **ALL questions** from **SECTION A** 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 SEVEN (7) questions in this section. Answer ALL Questions in the Answer Booklet.

1. Briefly discuss the following terms

   a) Eavesdropping (1 mark)

   b) Message Integrity (1 mark)

   c) Internet Fraud (1 mark)

   d) Denial-of-service attack (1 mark)

   (CLO1:PLO1:C2)

2. Interpret the activities of an ethical hacker. (4 marks)

   (CLO3:PLO4:C3)

3. Explain the following security attacks.

   a) Interruption (2 marks)

   b) Interception (2 marks)

   c) Modification (2 marks)

   d) Fabrication (2 marks)

   (CLO1:PLO1:C2)

4. Briefly explain each of the following three objectives of computer security

a) Confidentiality

(2 marks)

b) Integrity

(2 marks)

c) Availability

(2 marks)

(CLO1:PLO1:C2)

5. Differentiate between passive and active security attacks.

(4 marks)

(CLO1:PLO1:C2)

6. Illustrate with aid of a fully labelled diagram a model for internet security

(8 marks)

(CLO2:PLO3:C3)

7. Explain the following terms in relation to network security

a) Cryptography

(2 marks)

b) Cryptanalysis

(2 marks)

c) Brute force attack

(2 marks)

(CLO1:PLO1:C2)

SECTION B **(60 MARKS)**

There are FIVE (5) questions in this section. Answer ANY FOUR (4) questions in the Answer Booklet.

1. Discus at least THREE (3) approaches to message authentication.

(15 marks)

(CLO2:PLO3:C3)

2. With reference to the following questions,

   a) Illustrate with a fully labelled diagram a simplified model of conventional encryption.

(7 marks)

   b) In a public key system using RSA you intercept a cypher text C=10 sent to a user whose public key is e=5, n=35. What is the plaintext M?

Key Generation	
Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p - 1)(q - 1)$	
Select integer e	$\gcd(\phi(n),e) = 1$: $1<e<\phi(n)$
Calculate d	$de \bmod \phi(n) = 1$
Public Key	$KU = \{e,n\}$
Private Key	$KR = \{d,n\}$
Encryption	
Plaintext:	$M<n$
Ciphertext:	$C = M^e \pmod n$
Decryption	
Ciphertext:	C
Plaintext:	$M = C^d \pmod n$

(8 marks)

(CLO3:PLO4:C4)

3. With reference to the Kerberos key distribution and user authentication service,

a) Illustrate with a fully labeled diagram the Kerberos key distribution and user authentication system.

(5 marks)

b) Explain in detail the stages involved in Kerberos message exchanges between the client, Kerberos and host.

(8 marks)

c) Differentiate between Kerberos version 4 and version 5.

(2 marks)

(CLO3:PLO4:C2)

4. Pretty good privacy provides FIVE (5) services that can be used for electronic mail and file storage applications.

a) Name the FIVE (5) services

(5 marks)

b) Explain the FIVE (5) services

(10 marks)

(CLO3:PLO4:C2)

5. Answer the following questions.

a) Explain the following fundamental security design principles

i. Economy of mechanism

(3 marks)

ii. Separation of privilege

(3 marks)

iii. Psychological acceptability

(3 marks)

b) Name THREE (3) public key cryptographic algorithms and briefly describe each.

(6 marks)

(CLO3:PLO4:C2)

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