CONFIDENTIAL

Infrastructure University Kuala Lumpur

SUNWAY INT'L BUSINESS SCHOOL

FINAL EXAMINATION
SEPTEMBER/OCTOBER SEMESTER 2019

NETWORK AND DATA SECURITY
(CSC 2730)

(TIME: 3 HOURS)

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

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

LECTURER : MANOJ GAUTAM

GENERAL INSTRUCTIONS

1. This question booklet consists of 4 printed pages including this page.
2. Answer **ALL questions** in the **ANSWER BOOKLET.**
3. **PLEASE DO NOT TURN THIS PAGE AND START THE EXAM UNTIL YOU ARE TOLD TO DO SO.**

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) Threat

   (1 mark)

   b) Risk

   (1 mark)

   c) Denial of service attack

   (1 mark)

   d) Network Security

   (1 mark)
   (CLO1:PLO1:C2)

2. Interpret the activities of a Grey Hat Hackers.

   (4 marks)
   (CLO3:PLO4:C3)

3. Explain the following security attacks:

   a) Interruption

   (2 marks)

   b) Interception

   (2 marks)

   c) Security service definition according to RFC2828.

   (2 marks)

   d) Security service definition according to x.800

   (2 marks)
   (CLO1:PLO1:C2)

4. Briefly explain each of the following three Categories of Security Services mentioned in X.800.

   a) Access Control

   (2 marks)

   b) Integrity

   (2 marks)

   c) Non repudiation

   (2 marks)
   (CLO1:PLO1:C2)

5. Using Public key cryptographic algorithm RSA find the cipher text for the given plain text number.

   a) Plain Text (6), Public key (5), P * Q (119), C=?

   (4 marks)

   b) Plain Text (3), Public key (5), P*Q (119), C=?

   (4 marks)
   (CLO1:PLO1:C2)

6. Write a difference between digital signature and digital certificate.

   (4 marks)
   (CLO1:PLO1:C2)

7. Write three differences between MD5 and SHAHashing algorithm.

   (6 marks)
   (CLO1:PLO1:C2)

SECTION B **(60 MARKS)**

There are FIVE (5) questions in this section. Answer ALL Questions in the Answer Booklet.

1. Draw a General Scheme diagram of DES cipher and label it.

(8 marks)
(CLO2:PLO3:C3)

2. Explain PKI infrastructure with a labeled diagram.

(15 marks)
(CLO2:PLO3:C3)

3. With reference to the following questions,

   a) Implement a Caesar cipher encryption and decryption algorithm for a given function.

(7 marks)

   i. encrypt(message="CRYPTOCURRENCY", key=3):
   Pass

   ii. decrypt(cipher=encrypt("CRYPTOCURRENCY", key=3), key=3):
   Pass

   b) Find the cipher text of a message "NOIRA" if a message is encrypted using Play fair cipher using a keyword "MONARCHY".

(15 marks)
(CLO2:PLO3:C3)

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

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

(5 marks)

   b) Write a program to implement OneTimePad encryption algorithm for the given function using XOR operation.

   defone_time_pad_encrypt(message=15, key=9):
   pass

(8 marks)
(CLO3:PLO4:C2)

5. List two common types of firewalls.

(2 marks)
(CLO3:PLO4:C2)

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