Infrastructure University Kuala Lumpur

SUNWAY INT'L BUSINESS SCHOOL

INTERNAL EXAMINATION SEPTEMBER/OCTOBER SEMESTER 2020

BACHELOR OF COMPUTER SCIENCE (HONS.) (IN COLLABORATION WITH IUKL)

NETWORK AND DATA SECURITY (CSC2735)

(TIME: 1 HOUR)

MATRIC NO. : □□□□□□□□□

IC. / PASSPORT NO. : □□□□□□□□□□□□□□

LECTURER : **MANOJ GAUTAM**

GENERAL INSTRUCTIONS

1. This question booklet consists of 2 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.**

INSTRUCTIONS: **TIME:** ***1 HOUR***

(30 MARKS)

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

1. Perform encryption and decryption using RSA algorithm as shown below for the following.
   P = 17, Q = 11, E= 7; Plain Text M = 88

   a. In a public key system using RSA, Bob sent a plain text M=88 to Alice using her public key. What is the generated Cipher text C?

   (6 marks)

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

   (10 marks)

2. Robert runs a large website that allows users to log in and share images. When a new user sets up their account, the website hashes their password with **SHA256** and stores the hash in a database. When a user logs in, the website hashes the supplied password with **SHA265** and compares it to the stored hash. Robert figures that with this scheme, if anyone hacks into his database, they will only see hashes and won't learn the user's passwords. Out of curiosity, Robert does a Google search on several hashes in the database and is alarmed to find that, for a few of them, the google search results reveal the corresponding password.

   a. What is the risk that it introduces and how many of Robert's users could be affected?

   (2 marks)

   b. How should Robert store passwords?

   (2 marks)

3. One time pad ciphers are devised by Gilbert Vernam for AT&T. Encrypt the plaintext below using the Vernam cipher technique and given random number. Write your calculation

   Plaintext: **BLANK**
   Random Number: **34, 21 83, 55, 92**
   Numeric equivalent of letters A-z is **0 to 25.**

   (10 marks)

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