CONFIDENTIAL

Infrastructure University Kuala Lumpur

FINAL EXAMINATION
JUNE 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 (BTN303)

(TIME : 3 HOURS)

MATRIC NO.	: □□□□□□□□□
IC. / PASSPORT NO.	: □□□□□□□□□□□□□□
LECTURER	: FIZA ABDUL RAHIM

GENERAL INSTRUCTIONS

1. This question booklet consists of 6 printed pages including this page.
2. There are TWO (2) sections in this question booklet:
   Section A: Answer **ALL questions** in the **Answer Booklet**.
   Each question carries 10 marks.
   Section B: Answer **ALL questions** in the **Answer Booklet**.
   Each question carries 10 marks.
3. The total mark is 100.

CONFIDENTIAL

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

SECTION A **(40 MARKS)**

There are FOUR (4) questions in this section. Answer ALL Questions in the Answer Booklet. Each question carries 10 marks.

1. Cryptography is the practice and study of securing information in the presence of third parties.

   a) What are the common techniques used in cryptography? Briefly explain.
   (4 marks)

   b) Plaintext is one of the important elements of cryptography. List another FOUR (4) important elements of cryptography.
   (4 marks)

   c) Symmetric encryption involves one single key used for encryption and decryption. What is the major disadvantage of symmetric encryption? Explain.
   (2 marks)

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

Plaintext:	BLANK
Random Number:	34, 21, 83, 55, 92
Numeric Equivalent:	A – Z = 0 – 25

(10 marks)

3. Computers have replaced many face-to-face interactions with electronic ones. With no attentive neighbor to recognize that something is twisted, people need other mechanisms to separate authorized from unauthorized parties. For this reason, the basis of computer security is access control: *someone* is authorized to take *some action* on *something*. But for access control to work, we need to be sure who the "*someone*" is.

   a) In determining who a person really is consists of two separate steps. Briefly explain the TWO (2) steps.

   (4 marks)

   b) One of the authentication mechanisms is password. In a situation If you forget your password for a website and you click [Forgot my password], sometimes the company sends you a new password by email but sometimes it sends you your old password by email. Compare these two cases in terms of vulnerability of the website owner.

   (6 marks)

4. Attackers go after a browser to obtain sensitive information, such as account numbers or authentication passwords; to trap the user, for example, using pop-up ads; or to install malware.

   a) Differentiate between man-in-the-browser attack and page-in-the-middle attack.

   (4 marks)

   b) Discuss THREE (3) countermeasures for attacks against identification and authentication.

   (6 marks)

SECTION B (60 MARKS)

There are SIX (6) questions in this section. Answer ALL Questions in the Answer Booklet. Each question carries 10 marks.

1. Mary and John have each generated a public and private key pair. However, they do not know each other's' keys yet. Now they want to exchange a message, M over a network.

   a) What is the procedure to exchange the message confidentiality, if only passive attacks need to be considered?

   (4 marks)

   b) What is the main risk if active attacks are possible over a network?

   (2 marks)

   c) Discuss TWO (2) ways on how to ensure the authenticity of public keys in an attempt to mitigate the risk if active attacks are possible.

   (4 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 SHA256 and compares it to the stored hash. Robert figures that with this scheme, if anyone hacks into your database they will only see hashes and won't learn your users' 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?

   (4 marks)

   b) How should Robert store passwords?

   (6 marks)

3. A CAPTCHA (an acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart") is a program that protects websites against bots by generating and grading tests that humans can pass but current computer programs cannot.

   a) Identify accessibility issue with the use of CAPTCHAs. Suggest another method to solve the issue.

   (2 marks)

   b) Suppose a site implements a CAPTCHA by presenting users with four images and asking them to identify the one that shows a flower. Evaluate FOUR (4) weaknesses with this particular approach.

   (8 marks)

4. Wireless traffic uses a section of the radio spectrum, so the signals are available to anyone with an effective antenna within range. Because wireless computing is so exposed, it requires measures to protect communications between a computer and a wireless base station or access point.

   a) Suppose you have a wireless network access point in your home. List and explain TWO (2) reasons you might want to prevent an outsider's obtaining free network access by intruding into your wireless network.

   (4 marks)

   b) Wireless network is subject to threats to confidentiality, integrity and availability just like other computer applications and technologies. Describe ONE (1) example of vulnerability in wireless network for each confidentiality, integrity and availability.

   (6 marks)

5. Charles works as a system programmer for a large software company. He writes and tests programs such as compilers. His company operates two computing shifts. During the day, program development and online applications are run. At night, batch production jobs are completed. Charles has access to workload data and learns that the evening batch runs are complementary to daytime programming tasks; that is, adding programming work during the night shift would not adversely affect performance of the computer to other users. Charles comes back after normal hours to develop a program to manage his own online business. He uses very few expendable supplies, such as paper.

   a) Evaluate and discuss THREE (3) ethical implications involved in this situation.
   (6 marks)

   b) Would it affect the ethics of the situation if the following actions or characteristics were considered?

      i. Charles's employer knew of other employees doing similar things and approved by not seeking to stop them.
      (2 marks)

      ii. Charles's salary was below average for his background, implying that Charles was due the computer use as a benefit.
      (2 marks)

6. A security plan identifies and organizes the security activities for a computing system. The plan is both a description of the current situation and a map for improvement.

   a) Describe THREE (3) issues that must be addressed in security plan.
   (6 marks)

   b) Explain TWO (2) important factors that contribute to the successful of a security plan.
   (4 marks)

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