UTHM

Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2014/2015

COURSE NAME	:	SPECIAL TOPICS IN INFORMATION SECURITY
COURSE CODE	:	BIS 33403
PROGRAMME	:	3 BIS
EXAMINATION DATE	:	JUNE 2015 / JULY 2015
DURATION	:	3 HOURS
INSTRUCTION	:	ANSWER **ALL** QUESTIONS

THIS QUESTION PAPER CONSISTS OF **FOUR (4)** PAGES

Q1 Referring to the given paper:

(a) In the **ABSTRACT** section, identify a sentence that indicates the research problem.

(4 marks)

(b) In the **INTRODUCTION** section, which paragraph further describe this research problem?

(3 marks)

(c) From the **RELATED WORK** section, list **FIVE (5)** works by other that have been discussed as the foundation knowledge to the proposed solution.

(5 marks)

(d) Extract the main ideas from the **METHODOLOGY** section to discuss proposed solution in your own words.

(5 marks)

(e) Write a suitable summary for the **CONCLUSION** section?

(8 marks)

Q2 (a) How Cryptography and Steganography differs in providing data protection.

(5 marks)

(b) Consider the following scenario:

```
Bob and Alice want to communicate to each other. The short
message is very important and should not be exposed to
others. They asked your advice on how to secure
communication channel.
```

Based on the case study above, answer the questions below.

(i) Propose a suitable type of cipher that they should use to communicate.

(2 marks)

(ii) Justify your chosen cipher in Q2(b)(i).

(4 marks)

(iii) Propose a function that they should consider to ensure the integrity of the received message.

(2 marks)

(iv) Demonstrate how integrity of the message can be achieved using the proposed function in Q2(b)(iii).

(4 marks)

(c) Differentiate between:

(i) Symmetric cipher vs Asymmetric cipher

(4 marks)

(ii) Block cipher vs Stream cipher

(4 marks)

Q3 (a) Illustrate with a diagram the phishing activities through an email.

(10 marks)

(b) Propose FIVE (5) phishing email detection techniques.

(6 marks)

(c) Compare between origin based filtering and content based filtering.

(9 marks)

Q4 (a) Differentiate between Computer Security and Computer Forensics.

(4 marks)

(b) Discuss steps in Digital Forensics.

(10 marks)

(c) Consider the following scenario:

An investigation on the murder case has collected several evidences including the murdered weapon, a hand phone, a desktop with internet connection, a shirt soak in blood, few srings of hair and a glass with a bloody fingerprint.

Based on the case study above, answer the questions below.

(i) Categorize type of evidences found on the crime scene into e-evidence and trace evidence.

(6 marks)

(ii) Outline steps for gathering e-evidence from the desktop from the collection process until the analysis. (Note: Assume that no automatic tool available except a hex editor such as HxD)

(5 marks)

-END OF QUESTION-