35

MALAYSIAN INSTITUTE OF INFORMATION TECHNOLOGY

FINAL EXAMINATION

JANUARY 2016 SEMESTER

SUBJECT CODE	:	IBB42203
SUBJECT TITLE	:	CRYPTOGRAPHY
LEVEL	:	BACHELOR
TIME / DURATION	:	02:00 pm – 4:30 pm (2 ½ HOURS)
DATE	:	25 MAY 2016

INSTRUCTIONS TO CANDIDATES

1. Please read the instructions given in the question paper CAREFULLY.
2. This question paper is printed on both sides of the paper.
3. This question paper consists of ONE (1) section only.
4. Answer FOUR (4) questions only.
5. Please write your answers on the answer booklet provided.

THERE ARE 2 PAGES OF QUESTIONS, EXCLUDING THIS PAGE.

SECTION A (Total: 100 marks)

INSTRUCTION: Answer ONLY FOUR (4) questions.

Please use the answer booklet provided.

Question 1

a. What are the historic ciphers that were badly broken. Explain by examples.

(10 marks)

b. How the following cipher works

(15 marks)

i. Caeser Cipher

ii. Vigener Cipher

iii. Rator Machine

[Total 25 Marks]

Question 2

a. Formally define discrete probability and why it is used in cryptography?

(5 marks)

b. Write short notes on the following:

i. Events

(5 marks)

ii. Random Variable

(5 marks)

iii. Uniform Random Variable

(5 marks)

iv. Randomized algorithm

(5 marks)

[Total 25 Marks]

Question 3

a. Formally define Symmetric Ciphers

(5 marks)

b. What is correctness property of Symmetric Ciphers

(5 marks)

c. Prove that one time pad satisfies correctness property

(5 marks)

d. What is Shannon theory? Define formally

(5 marks)

e. Prove that one time pad has perfect secrecy according to shannon's theory.

(5 marks)

[Total 25 Marks]

Question 4

a. Explain the components of Trusted Platform Module.

(5 marks)

b. Describe the following different cryptographic primitives used in TPM

(20 marks)

i. Endorsement Key

ii. Sealing

iii. Binding

iv. Storage Root Key

[Total 25 Marks]

Question 5

a. Explain process of Remote Attestation

(10 marks)

b. How Static and Dynamic remote attestation techniques are applied during remote attestation. Give examples of both techniques.

(15 marks)

[Total 25 Marks]

END OF EXAMINATION PAPER