UTHM
Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
(ONLINE)
SEMESTER II
SESSION 2019 / 2020

COURSE NAME	:	INTRODUCTION TO INFORMATION SECURITY
COURSE CODE	:	BIS 10103
PROGRAMME CODE	:	BIS
EXAMINATION DATE	:	JULY 2020
DURATION	:	2 HOURS 30 MINUTES
INSTRUCTION	:	1. ANSWER ALL QUESTIONS. 2. THE STUDENTS SHOULD UPLOAD THE ANSWER BOOKLET (PDF/ WORD FORMAT) WITHIN 30 MINUTES AFTER EXAMINATION PERIOD.

THIS QUESTION PAPER CONSISTS OF **THREE (3)** PAGES

Q1 (a) Explain **FIVE (5)** steps in constructing public key and private key cryptosystem for Rivest Shamir Adleman (RSA) Cryptosystem.

(10 marks)

(b) Given Alice's public and private keys are `(33, 3)` and `(33, 7)` respectively. Bob wants to send the message `M = 13` to Alice.

Using Alice's public and private keys, describe the processes and calculations of the ciphertext, `C` and the value for `M` when Alice recovers the message.

(10 marks)

Q2 Common web security concept are:

`"Confidentiality, Integrity, Availability, Non-repudiation, Privacy, Authentication, Authorization"`

Map **ONE (1)** web security concept for each of following:

(i) Haziq received One Time Password message in his phone when transferring money via online banking to his father.

(ii) University are required to keep a student's personal information private unless consent to release the information is provided by the student.

(iii) The ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

(iv) The concept to ensure users can access information resources in timely manner.

(v) Maisarah hacked the student information system and changed her mathematic grade from B to B+.

(10 marks)

Q3 (a) Describe **TWO (2)** mobile malware delivery methods commonly used to infect smartphone users.

(4 marks)

(b) Explain why smartphone user should not download applications from unofficial application market.

(2 marks)

Q4 (a) Encrypt the message MEET ME AT HAMMERSMITH BRIDGE TONIGHT using a Playfair Cipher with keyword charles. Show all steps of the encryption process.

(10 marks)

(b) Decrypt the ciphertext `TEETNWRT RAHNWSEE OEBATUSH RISHBSKO NOMCIEAD VLPDYRHR CEBU` which was encrypted using 2-Row Rail Fence Cipher

(4 marks)

(c) Encrypt the message `TO BE OR NOT TO BE THAT IS THE QUESTION` using a `Vigenere Tableu` with keyword `RELATIONS`. Show your works.

(6 marks)

Q5 (a) Suppose the following groups are defined to shorten a system's ACLs:

```
Group1: Alice, Bob, Cynthia, David, Eve
Group2: Alice, Bob, Cynthia
Group3: Bob, Cynthia
```

While the ACLs of `File1` is:

```
File1: Group1, R; Group 2, RW
```

Does Alice will be allowed to write to `File1` if:

(i) The first relevant entry policy is applied. Give your reason.

(ii) The any permission in list policy is applied. Give your reason.

(4 marks)

- END OF QUESTIONS -