UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2018/2019

COURSE NAME	:	MULTIMEDIA SECURITY TECHNOLOGY
COURSE CODE	:	BIM 33403
PROGRAMME CODE	:	BIM
EXAMINATION DATE	:	JUNE / JULY 2019
DURATION	:	3 HOURS
INSTRUCTION	:	ANSWER **ALL** QUESTIONS

THIS QUESTION PAPER CONSISTS OF **FIVE (5)** PAGES

Q1 Questions **Q1(a) – Q1(e)** are based on the following scenario:

iTechnology Enterprise decided to develop a secure file transfer system between staff within the organization. It involves all branches located within Malaysia, using Internet. First, to use the in-house file transfer system, the staff must log in via a predetermined authentication method. Then, to secure the message between two staff, cryptography algorithm will be implemented for each session. iTechnology Enterprise has 2 branches, each with 2 staff.

(a) Based on 'what you know' and 'what you have' authentication approaches, propose **ONE (1)** method for each approach that can be used as the login mechanism for the system. For each method, provide **ONE (1)** suitable data type.

(6 marks)

(b) Suggest the most suitable cryptography type. Provide **ONE (1)** justification of why choosing it.

(4 marks)

(c) Based on the answer in **Q1(b)**, calculate the number of keys required.

(4 marks)

(d) List **TWO (2)** possible different attacks to the system. For each attack, provide **ONE (1)** possible source.

(6 marks)

(e) With an aid of a diagram, illustrate the inter-related security levels that will be implemented in the system.

(5 marks)

Q2 (a) Given the following scenario:

iBanking Berhad is planning to provide online banking for their customers that enables viewing accounts and performs online transaction. The security plan must be balanced between usability and security.

Develop **ONE (1)** security plan that describes authentication and corresponding authorization that enables different activities such as viewing accounts, online payment and money transfer. The plan should consider suitable authentication for each activity.

(10 marks)

(b) Given the text message below:

```
For things to change, I must change first.
```

Suggest **TWO (2)** strategies to encrypt the text. For each strategy, provide **ONE (1)** example of the encrypted message.

(6 marks)

(c) Given the following scenario:

```
iMovie Enterprise is a video streaming company. They
decided to use the scheme that can encrypt, decrypt and
compress some parts of the video between the server and the
authorized device. The encryption and compression processes
should be light-weighted.
```

Propose **TWO (2)** suitable tools or applications to perform the encryption or compression.

(4 marks)

(d) Given the following scenario:

```
iToones is a mobile application to upload and download
images. It uses a graphical authentication scheme that
enforces the user to select 3 images. Each image must be
selected from 8 given images. The 3 images must be selected
in the right order.
```

Justify the strength of the scheme using complexity analysis.

(5 marks)

Q3 Questions **Q3(a) – Q3(d)** are based on the following scenario.

```
Maestro Berhad is planning to develop a content delivery system
that includes digital right management (DRM): a publisher, a
server (streaming or Web), a client device (i.e., decoder box and
smart card), and a financial clearing house. The communication
between the server and the client is assumed to be unicast, i.e.,
point-to-point. Digital Right Management (DRM) refers to the
protection, distribution, modification, and enforcement of the
rights associated with the use of digital content. The types of
content include video and radio. The customers subscribe to the
content delivery system and make payment on monthly basis.
```

(a) Assume Maestro Berhad decided to encrypt the content during delivery so no one can view the content before it reaches the decoder box. The main criteria for the encryption is that all parts of the video should only be available to authorized clients. Justify the suitable encryption scheme and discuss your answer.

(5 marks)

(b) Develop **ONE (1)** recovery plan in case the main server is corrupted. The plan should include what to be recovered, how to recover, when to be recovered and by whom.

(8 marks)

(c) Draw **ONE (1)** diagram to illustrate how 'what you are' approach can be integrated as the authentication and transaction access control (payment) mechanism for the content delivery system.

(6 marks)

(d) Draw **ONE (1)** diagram to illustrate the typical DRM's activities to suit the content delivery system.

(6 marks)

Q4 (a) Given the following scenario:

```
Assume a collection of image and video content is kept in a
secure application called safety box. The safety box
consists of three characters. Each key used a number from 0
to 9. The box will be opened if the right combination of
the three keys is achieved.
```

Suggest **THREE (3)** Brute Force strategies to break the password.

(6 marks)

(b) Given the following **Figures Q4(b)(i)** and **Q4(b)(ii)**.

Figure Q4(b)(i)

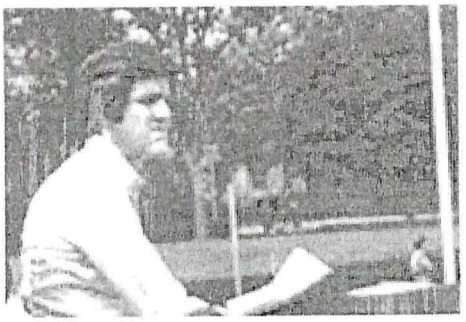

Figure Q4(b)(i)

Assume the image in **Figure Q4(b)(ii)** has been forged. Justify **ONE (1)** possible tampering method used to forge the image. Then, discuss **ONE (1)** method to detect it.

(4 marks)

(c) Given the following **Figure Q4(c)**.

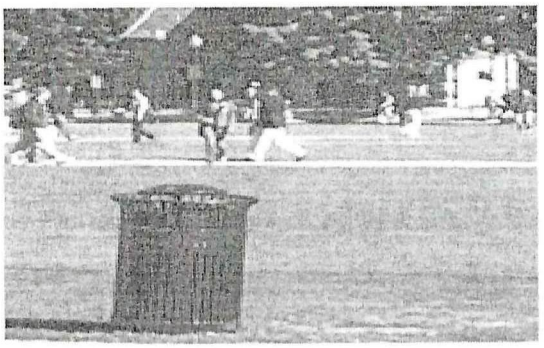

Figure Q4(c)

Draw the watermarked image if the visible watermarking technique is applied.

(4 marks)

(d) Describe **TWO (2)** applications where watermarking can be used.

(6 marks)

(e) List **THREE (3)** attributes of the pyramid of an effective enforcement for Digital Right Management (DRM).

(3 marks)

(f) State the standard number for International Standards Organization (ISO) for Information Security Management System.

(2 marks)

- END OF QUESTION -