Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2017/2018

COURSE NAME	:	MULTIMEDIA SECURITY TECHNOLOGY
COURSE CODE	:	BIM 33403
PROGRAMME CODE	:	BIM
EXAMINATION DATE	:	JUNE / JULY 2018
DURATION	:	3 HOURS
INSTRUCTION	:	ANSWER **ALL** QUESTIONS

THIS QUESTION PAPER CONSISTS OF **SIX (6)** PAGES

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

Robust Technology Sdn. Bhd. decided to develop a secure messaging system between staff within the organization. It involves all branches located throughout Malaysia, using Internet. First, to use the in-house secure messaging 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. Robust Technology Sdn. Bhd. has 5 branches, each with 20 staff.

(a) Based on 'what you know' authentication approach, propose **TWO (2)** methods 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) Propose the number of security levels that will be implemented in the system.

(5 marks)

Q2 (a) Given the following scenario:

Astrong Bhd. is planning to develop a movie delivery network that includes digital right management (DRM): a publisher, a repository, a client device (i.e., decoder box and smart card), and a financial clearing house. The communication between the repository and the client is assumed to be unicast, i.e., point-to-point. The types of movie include video (e.g., film, drama, documentary, and cartoon). The authentication approach that will be used in this system is smartcard number and password.

Develop **ONE (1)** guideline to ensure the password being used is strong enough. The guideline should include what is required to make a strong password.

(8 marks)

(b) Given the text message below:

I love what I do, I do what I love.

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

(8 marks)

(c) Given the following scenario:

Astrong Movie is a song streaming company. They decided to use the scheme that quickly can encrypt and decrypt some part of the audio between the server and the authorized device. The main criteria for the encryption is that it must be lightweight.

Justify the suitable encryption scheme and discuss your answer.

(4 marks)

(d) Given the following scenario:

A graphical authentication scheme enforces the user to select 4 images. Each image must be selected from 10 given images. The 4 images must be selected in the right order.

Justify the strength of the scheme using the password complexity calculation.

(5 marks)

Q3 (a) Justify why video code stream (e.g., MPEG-4 FGS) is not entirely scalable compared to image code stream (e.g., JPEG 2000).

(5 marks)

(b) Given the following scenario:

```
Person A sends an attachment using an email to Person B.
```

Draw **ONE (1)** diagram to illustrate end-to-end media security architecture that enables secure transmission of the attachment via Internet from Person A's email account to Person B's email account.

(6 marks)

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

(6 marks)

(d) Given the text message below:

```
we love what we do, we do what we love, we do what we do,
we love what we love
```

Suggest **TWO (2)** ways to combine encryption and compression processes during message streaming. For each way, provide **ONE (1)** example of the final output.

(8 marks)

Q4 (a) Given the following scenario:

```
Adam used a cloud-based e-Locker to keep files containing
copyright digital properties. The password of the e-
Locker consists of 4 characters. Each character must be
selected from alphabet between A to J.
```

Suggest **TWO (2)** Brute Force strategies to break the password.

(6 marks)

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

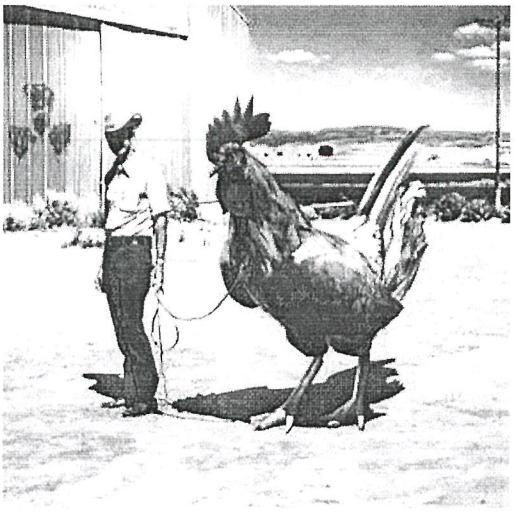

Figure Q4(b)

Assume the image in **Figure Q4(b)** 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)**.

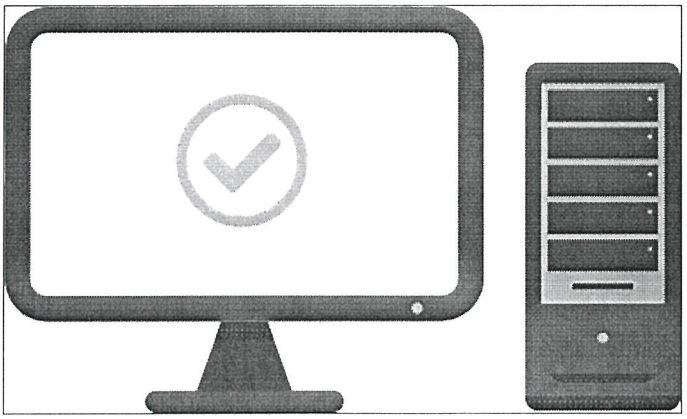

Figure Q4(c)

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

(4 marks)

(d) Given the following scenario:

A digital cinema has been opened in Batu Pahat Mall. The digital cinema's management team wanted to employ a number of technologies that can help to prevent unauthorized use of their digital cinema content. Some of the potential challenges are to prevent the recording of a movie via camcorder, and to track the source of the piracy that manages to circumvent all other protection measures.

Suggest **THREE (3)** tools to secure digital cinema content.

(6 marks)

(e) List **THREE (3)** Digital Right Management (DRM) Standard Organizations and Consortiums.

(3 marks)

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

(2 marks)

- END OF QUESTION -