Universiti Tun Hussein Onn Malaysia

# UNIVERSITI TUN HUSSEIN ONN MALAYSIA

## FINAL EXAMINATION
## SEMESTER II
## SESSION 2015/2016

| | | |
|---|---|---|
| COURSE NAME | : | MULTIMEDIA SECURITY TECHNOLOGY |
| COURSE CODE | : | BIM 33403 |
| PROGRAMME CODE | : | BIM |
| EXAMINATION DATE | : | JUNE / JULY 2016 |
| 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.

Ready Technology Sdn. Bhd. plans to develop a system to enable secure file transfer between staff within all branches located throughout Malaysia, using Internet. The staff should be able to send text, image and audio files. First, to use the system, the staff must log in via a predetermined authentication method. Then, to enable secure file transfer between two staff, cryptography algorithm is used for each session. Ready Technology Sdn. Bhd. has 5 branches, each with 20 staff.

(a) Propose **TWO (2)** authentication methods that can be used as a login mechanism for the system. For each method, provide **ONE (1)** suitable data type.

(6 marks)

(b) Calculate the number of keys required if the asymmetric cryptography is used.

(4 marks)

(c) Calculate the number of keys required if the symmetric cryptography is used.

(4 marks)

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

(6 marks)

(e) Draw **ONE (1)** flowchart to illustrate the level of security used in the system.

(5 marks)

**Q2** (a) Given the following scenario.

Movie Stream Bhd. is planning to develop a content delivery network 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. The types of content include video (e.g., film, drama, documentary, and cartoon) and audio (i.e., radio channels). The customers subscribe to the content delivery system and make payment either on monthly basis or pay-as-you-go basis.

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)

(b) Given the text message below.

The future belongs to those who believe in the beauty of their dreams.

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.

EnjoyMovie.com is a content delivery company. They decided to encrypt the content during delivery so no one can view the content before it reaches the decoder box. The encryption process should be light-weighted and can be applied in any segment of the file.

Justify either a full or selective encryption scheme is more suitable and discuss your answer.

(4 marks)

(d) Draw **ONE (1)** diagram to illustrate how steganography can be applied to an image.

(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) Draw **ONE (1)** diagram to illustrate how to securely transmit an image via Internet from device A to device B.

(6 marks)

(c) Draw **ONE (1)** diagram to illustrate how biometrics can be integrated as the authentication and access control mechanism in a smartphone.

(6 marks)

(d) Given the text message below.

```
sea seamaster master seashell shellmaster mastersea shell.
```

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

(8 marks)

**Q4** (a) Given the following scenario.

```
Adam kept a file containing copyright images in his
computer. To ensure the file can only be opened by himself,
he uses a password. The password consists of 3 characters.
Each character is represented by a small letter alphabet.
The file will be opened only if the right password is
entered.
```

Assume Adam forgot his exact password. Suggest **TWO (2)** strategies to get the right combination of the password.

(6 marks)

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

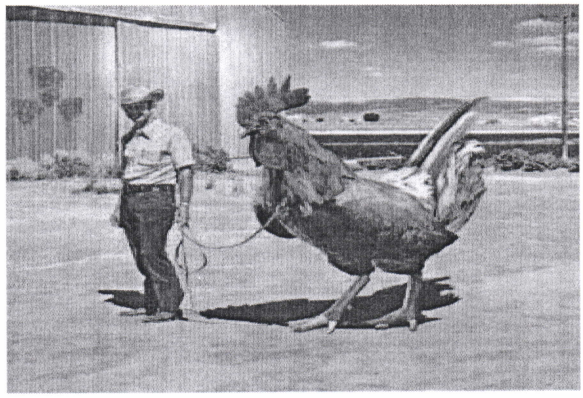

**Figure Q4(b)**

Justify the 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 tampered image if the copy move tampering method is used.

(4 marks)

(d) Given the following scenario.

Adam is a singer. He planned to sell his songs online via the Authentic Song website. In order to ensure the copyright of the songs, digital audio watermarking is used. Also, it can help to prevent unauthorized use, prevent the recording of the songs via software, and track the source of the piracy.

Justify **TWO (2)** reasons why audio watermarking is the best solution.

(6 marks)

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

(3 marks)

(f) State **ONE (1)** International Standards Organization (ISO) related to information security management system (ISMS).

(2 marks)

**- END OF QUESTION -**