UTHM
Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2014/2015

COURSE NAME	:	MULTIMEDIA SECURITY TECHNOLOGY
COURSE CODE	:	BIM 33403
PROGRAMME	:	3 BIM
EXAMINATION DATE	:	JUNE 2015/ JULY 2015
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.

```
Smart Intelligent Technology Sdn. Bhd. is required to develop the
Secure Communication System for Biznet Bhd. The main purpose of
the system is to enable staff within the organization to perform
private communication either using intranet or internet. The
staff should be able to send file, image or any other
attachments. A staff must login to the system each time
initiating secure communication. Biznet Bhd. has 100 staff. The
top management of the organization emphasizes that risk analysis
of the system must be done annually.
```

(a)   Propose **FOUR (4)** access control methods that can be used as a login mechanism for the system. For each method, provide **ONE (1)** suitable data type.

(8 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 **THREE (3)** possible different attacks to the system.

(6 marks)

(e)   Justify **ONE (1)** reason why risk analysis is important to maintain the security for the system.

(3 marks)

Q2   Questions **Q2(a) – Q2(e)** are based on the following scenario.

> Maestro Bhd. 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 (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.

(a)   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)   State **ONE (1)** tool that can be used to compress the content.

(2 marks)

(c)   Assume Maestro Bhd. 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. Justify either a full or selective encryption scheme is more suitable and discuss your answer.

(5 marks)

(d)   Suggest **ONE (1)** scheme that can be used to authenticate clients.

(2 marks)

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

(8 marks)

Q3   (a)   Describe **TWO (2)** applications where watermarking can be used.

(6 marks)

(b)   Draw a diagram to illustrate how biometrics can be integrated as the authentication mechanism in a mobile device.

(6 marks)

(c)   Draw a diagram to illustrate end-to-end media security architecture.

(6 marks)

(d)   Justify why the conventional approach for transcoding encrypted streams (that involves decryption, transcoding, and re-encryption) poses a serious security threat.

(3 marks)

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

(4 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 keys. Each key used a number system from 0 to 9. The box will be opened if the right combination of the three keys is achieved.

Suggest **THREE (3)** strategies to get the right combination of the three keys.

(6 marks)

(b)   Given the following scenario.

John intended to forge an image using Photoshop software. He wanted to add new objects, erasing existing objects and resizing some objects. The main aim is to ensure the fake image looks as real as possible.

Draw a diagram to illustrate the process of the image forgery.

(8 marks)

(c)   Given the following scenario.

Parit Raja Mall planned to open a digital cinema. The mall'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)

(d)   List **FIVE (5)** Digital Right Management (DRM) Standard Organizations and Consortiums.

(5 marks)

- END OF QUESTION -

CONFIDENTIAL