UTHM
Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
ONLINE
SEMESTER II
SESSION 2019/2020

COURSE NAME	:	MULTIMEDIA SECURITY TECHNOLOGY
COURSE CODE	:	BIM 33403
PROGRAMME CODE	:	3 BIM
EXAMINATION DATE	:	JULY 2020
DURATION	:	3 HOURS
INSTRUCTION	:	1. ANSWER **ALL** QUESTIONS
		2. THE STUDENTS SHOULD UPLOAD THE ANSWER BOOKLET (WORD FORMAT) WITHIN 30 MINUTES AFTER EXAMINATION PERIOD.

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

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

Lazuardi Technology (LazTech) decided to develop a secure desktop-based confidential data transfer application between staff within the organization. Each desktop has the capability of capturing biometric properties (i.e, thumbprint and voice). The use of the application involves all branches located within Malaysia, using Internet. First, to use the application, the staff must log in via a predetermined authentication scheme. Then, to secure the data/message being communicated between two staff, cryptography algorithm will be implemented for each session. Currently, LazTech has 2 branches, each with 2 staff.

(a) Based on 'what you know' and 'who you are' authentication approaches, propose **ONE (1)** method for each approach that can be used as the login mechanism for the application. 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.

(3 marks)

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

(4 marks)

(d) Based on the answer in **Q1 (a)**, list **TWO (2)** possible different attacks to the system. For each attack, provide **ONE (1)** possible source.

(6 marks)

(e) Assume the number of LazTech branches and staff will be doubled by the next financial year. Suggest the most suitable cryptography type to be implemented by then. Next, calculate the corresponding number of keys required.

(6 marks)

Q2 (a) Given the following scenario:

Lazuardi Banking Berhad is planning to provide an online banking system for their customers that enables viewing accounts, updating customer details and performs online transaction such as money transfer, buying top up and bill payment. The authentication and authorization strategy for enabling these online services must be balanced between usability and security.

Develop **ONE (1)** strategy that describes authentication and corresponding authorization that enables these different services: viewing accounts, updating customer details, buying top up, online bill payment and money transfer. The strategy should consider suitable authentication and authorization for each service.

(10 marks)

(b) Given the text message below:

Without commitment we will never start, but without consistency, we will never finish.

Suggest **ONE (1)** strategy to encrypt the text. Then, provide the algorithm for the strategy and **ONE (1)** corresponding example of the encrypted message.

(6 marks)

(c) Given the following scenario:

Lazuardi Capital owns an online video streaming mobile application called LazMovie. To ensure that the content only be consumed by the authorized customer, they decided to use the suitable scheme that can encrypt, compress and decrypt all parts of the video content. These processes will be performed on the fly between the server and the authorized customer's device. The encryption and compression processes should be reliable.

Propose **ONE (1)** suitable scheme and **ONE (1)** corresponding tool to perform these processes.

(4 marks)

(d) Given the following scenario:

LazCloud is an open platform mobile application that enable the user to upload and download copyright-free images, video and audio on the free public cloud. As an authentication scheme, it uses a graphical based approach that require and enforce the user to select 3 pre defined 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 a suitable complexity analysis.

(5 marks)

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

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

(5 marks)

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

(8 marks)

(c) Draw **ONE (1)** diagram to illustrate how 'what you have' 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:

A collection of digital assets is kept in a secure digital locker called LazLock application. To authorize access of the digital locker, LazLock used a simple digital key scheme that consists of three characters. Each character used a letter from A to Z. The access will be granted if the right combination of the three characters is achieved.

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

(6 marks)

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

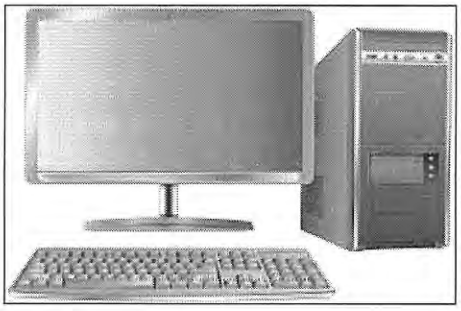

Figure Q4(b)(i)

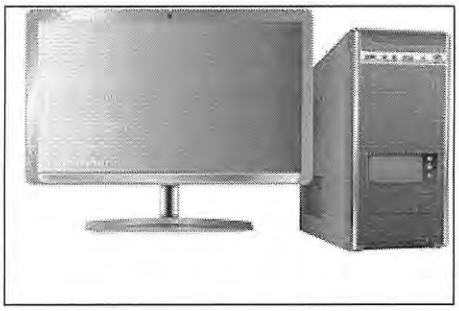

Figure Q4(b)(i)

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 **THREE (3)** applications where watermarking can be used.

(6 marks)

(e) Discuss **TWO (2)** attributes of the pyramid of an effective enforcement for Digital Right Management (DRM) for online modules for UTHM's Massive Open Online Courses (MOOC).

(5 marks)

- END OF QUESTION -