UTHM
Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2013/2014

COURSE NAME	:	INFORMATION SECURITY STANDARDS
COURSE CODE	:	BIS 33203
PROGRAMME	:	3 BIS
EXAMINATION DATE	:	JUNE 2014
DURATION	:	2 HOURS AND 30 MINUTES
INSTRUCTION	:	ANSWER **ALL** QUESTIONS

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

Q1 (a) Consider the following scenario:

```
In the days prior to Hari Raya 2013, someone installed
malware in Giant's security and payments system designed
to steal every credit card used at the company's 1,797
Malaysia stores, and detail for over 40 million credit
card numbers were stolen.
```

(i) The traditional information security goals are often represented by the acronym CIA. Explain **THREE (3)** security goals represented by these three letters.

(4 marks)

(ii) In the above scenario, determine which of the traditional security goals listed **Q1(a)(i)** is compromised.

(4 marks)

(iii) Attacks on information system can be categorized as either passive or active. For the data breach above, which type of attack has occurred?

(2 marks)

(iv) Justify your answer in **Q1(a)(iii)**.

(4 marks)

(b) Explain the difference between threat and vulnerability.

(2 marks)

(c)

```
Extensive damage to information assets occurred as a
result of the flooding in Batu Pahat from December 2006
to January 2007.
```

Give an example of a vulnerability that, if it were to coincide with the flood threat, could result in damage to information assets.

(2 marks)

(d) Many Internet applications use cookies for session management. Outline **TWO (2)** differences between persistent and non-persistent cookies.

(4 marks)

(e) Consider the following scenario:

Statistical analysis of recorded data produced the information recorded in the table below regarding threats associated with information assets at Company A.

Table 1 : Threat to the assets of Company A.

Threat to Asset	Cost per incident (RM)	Annualized Rate of Occurance
1. Unauthorized access to proprietary information	100,000	0.10
2. Unauthorized use of computing facilities	20,000	0.35
3. Loss of availability of computing facilities	7,000	1.55

(i) Computes all Annualized Loss Expectancy (ALE).

(3 marks)

(ii) Compares all threats and stated the greatest ALE.

(1 marks)

Q2 (a) Explain why applications using symmetric ciphers only cannot provide non-repudiation?

(2 marks)

(b) Cipher Block Chaining (CBC) is a mode of operation defined for any block cipher. With the aid of a clearly labelled diagram, explain how encryption is performed in CBC mode.

(6 marks)

(c) Suppose that a binary additive stream cipher (such as the one time pad) has been used to encrypt an electronic funds transfer. Assuming that no other cryptographic processing is used, outline how an attacker who knows the format of the plaintext message used for the funds transfer can change the amount of the funds transfer without knowing anything about the key that is used.

(9 marks)

(d) Hash functions are often used for providing security services related to integrity. Consider the case where Alice sends both a message, *M* and the SHA-2 hash of the message, *H*(*M*), to Bob. Bob receives message *M'*, and can compute the has value *H*(*M'*) and compare it to the received hash, *H*(*M*). This method can be used to provide some assurance that there were no accidental errors during the transmission.

(i) Explain why this process is not sufficient to provide protection against an active attacker.

(3 marks)

(ii) What can Alice and Bob use instead of the hash function described above, to provide protection against an active attacker?

(5 marks)

Q3 (a) Alice wants to send a message and an associated digital signature to Bob. Alice has a public key K_{Apub} and the associated private key K_{Apriv}. Similarly, Bob has a public key K_{Bpub}, and the associated private key K_{Bpriv}.

Illustrate the cryptographic steps necessary for:

(i) Alice to generate her digital signature, and

(4 marks)

(ii) Bob to verify Alice's digital signature.

(4 marks)

(b) In asymmetric or public key cryptography, each user has a pair of keys. For example, Alice has a pair of keys: K_{Apub} and K_{Apriv}. Alice has a digital certificate that contains among other things, her public key. She makes this available to other users who request her public key.

(i) What is the purpose of the digital certificate containing Alice's public key?

(1 marks)

(ii) Outline the difference between Alice's digital certificate and Alice's digital signature.

(3 marks)

(c) A network communications protocol known as HTTP Authentication can be performed as either *Basic* or *Digest* Authentication.

(i) Explain the major security problem associated with the use of *Basic Authentication* over an insecure channel.

(3 marks)

(ii) When used over an insecure channel, *Digest Authentication* does not have the same security problem. Explain the mechanism used in digest authentication to provide protection.

(4 marks)

(d) TLS is a commonly used network communication protocol.

(i) What the three words represented by the three letters TLS?

(1 mark)

(ii) When using the TLS Handshake protocol, the server sends the client a certificate. Outline what the client uses the certificate for?

(5 marks)

Q4 (a) Access control can be categorised into three: *discretionary, mandatory and role-based.* Compares these three access control approaches.

(6 marks)

(b) Describe *separation of duties.* Outline how role-based access control can be used to implement separation of duties.

(5 marks)

(c) Reusable passwords are commonly used to authenticate users. The passwords may be randomly generated or user selected. List **FOUR (4)** *disadvantages* associated with authentication based on user selected reusable password.

(4 marks)

(d) Security testing approaches can be categorised into two. Name and explain these **TWO (2)** approaches.

(4 marks)

(e) State **FOUR (4)** common steps in security evaluation methodology.

(4 marks)

(f) Give **TWO (2)** examples in this evaluation methodology.

(2 marks)

- END OF QUESTION -