UTHM
Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2016/2017

TERBUKA

|		
COURSE NAME	:	SOFTWARE ENGINEERING SECURITY
COURSE CODE	:	BIE 33003
PROGRAMME CODE	:	BIP
EXAMINATION DATE	:	JUNE 2017
DURATION	:	3 HOURS
INSTRUCTION	:	ANSWER **ALL** QUESTIONS

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

SECTION A

Instruction: Choose the BEST answer for each of the following questions.

Q1   The following statements are the reasons why users are told to use strong passwords.

    i.   It is more difficult to "shoulder surf" a strong password because of the additional keystrokes.

    ii.   Strong passwords are more difficult for others to guess.

    iii.   Weak passwords are susceptible to dictionary attacks.

    iv.   Passwords based on easily-discovered facts such as birthdays, spouse and pet names are easily guessed.

    A.   i, ii, iii, iv
    B.   i, ii, iii,
    C.   ii, iii, iv
    D.   i,ii, iii, iv
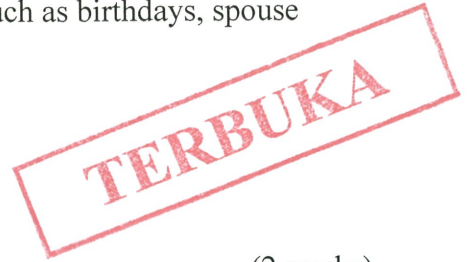
(2 marks)

Q2   A digital signature is an _____ that enables the creator of a message to attach a code that acts as a signature.

    A.   authorization approach
    B.   authentication mechanism
   C.   access procedures
    D.   encryption technique

(2 marks)

Q3   The probability that a specific vulnerability within an organization will be the target of an attack is known as _____.

    A.   probability
    B.   manageability
    C.   likelihood
    D.   practability

(2 marks)

Q4   A _____ is an application error that occurs when more data is sent to a program buffer than it is designed to handle.
- A.   buffer underrun
- B.   buffer overrun
- C.   heap overflow
- D.   heap attack

(2 marks)

Q5   The process of transforming plain text to chipper text is known as _____.
- A.   decryption
- B.   encryption
- C.   key recovery
- D.   hashing

TERBUKA
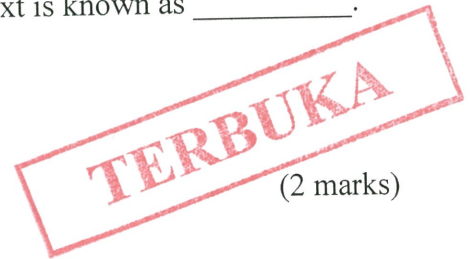
(2 marks)

SECTION B

Q6   (a)   Discuss **THREE (3)** types of threats that could affect a database system.

(6 marks)

      (b)   Suggest the controls that can be used to counteract each of the threats types answered in **Q6(b).**

(6 marks)

      CONFIDENTIAL

(c) Describe a scenario in which Role 2 users can use one or more queries to determine that there is a classified shipment on board the aircraft based on **Figure Q6(c)**.

Ahmad is a database administrator for a military transportation system. In the database there is a table named 'cargo' that contains information on the various cargo holds available on each outbound airplane. Each row in the table represents a single shipment and lists the contents of that shipments and the flight identification number. Only one shipment per hold is allowed. The flight identification number maybe cross-referenced with other tables to determine the origin, destination, flight time, and similar data. In addition, there are two roles defined for the table, which are:
1) Role 1 has full access rights to the cargo table,
2) Role 2 has full access rights only to rows of the table in which the classification field has the value as 'Unclassified'.
The cargo table is represented as **Table 1**:

Table 1: Cargo Table

Flight ID	Cargo Hold	Contents	Classification
1234	A	Boots	Unclassified
1234	B	Guns	Unclassified
1234	C	Atomic Bomb	Top Secret
1234	D	Butter	Unclassified

Figure Q6(c)

(8 marks)
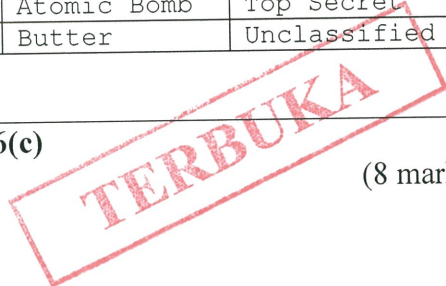
Q7 (a) Facebook, Twitter and Instagram are the examples of popular social networking in our society. As a measure to remain secured, everyone has different responsibilities; use different approaches and techniques in their daily life. Discuss the responsibilities, approaches and techniques for each of the stakeholders listed in the following:
(i)   IT Manager
(ii)   Software developer
(iii) User

(12 marks)

(b) Explain **THREE (3)** classess of intruders.

(6 marks)

CONFIDENTIAL

(c)   Determine **TWO (2)** types of system that can be used to counter the intruders' threats.

(2 marks)

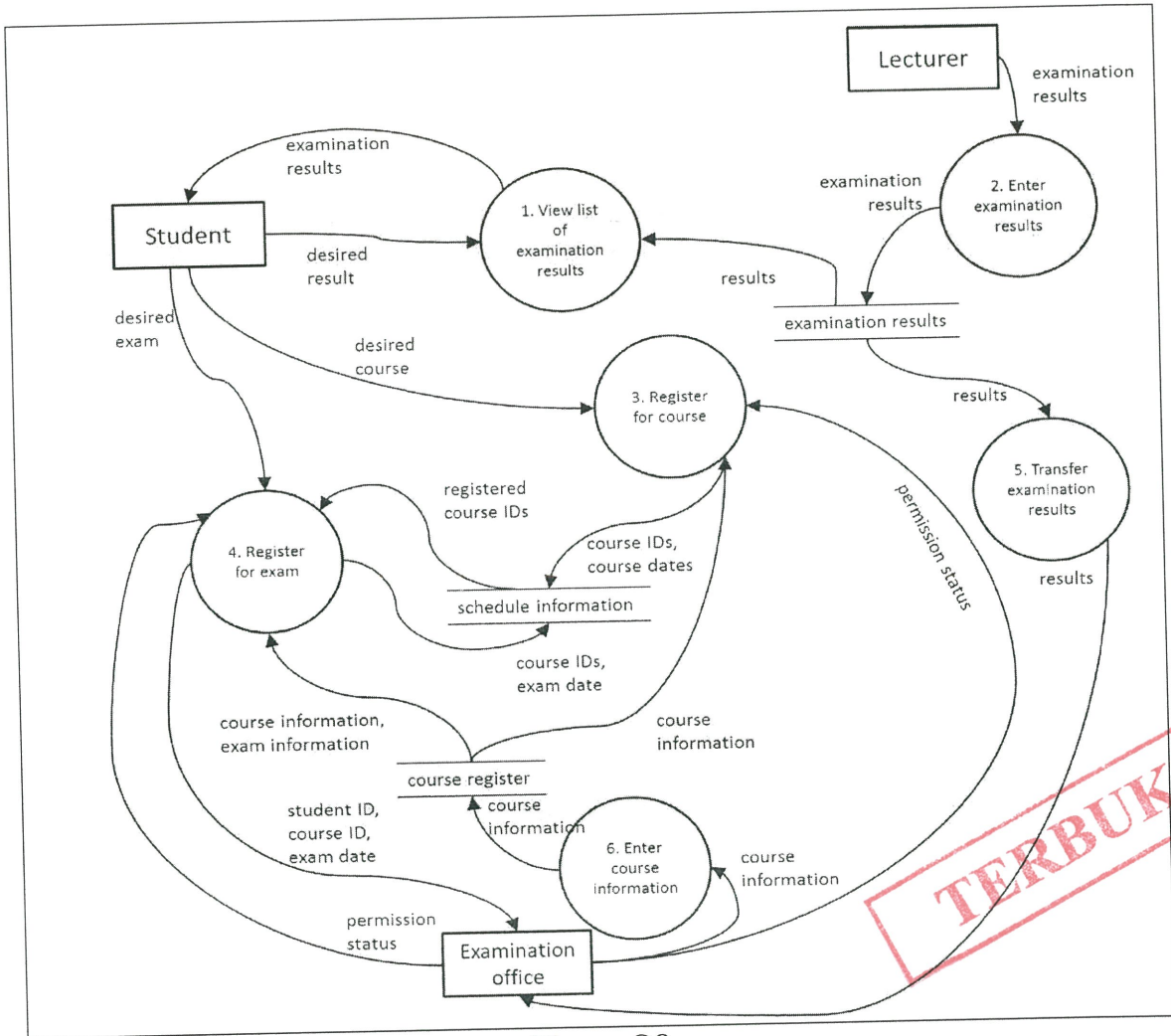Q8   Questions **Q8(a)-Q8(d)** are based on **Figure Q8.**

Figure Q8

(a)   Transform the dataflow diagram into a use case diagram.

(6 marks)

(b)   Outline **FIVE (5)** critical assets.

(8 marks)

CONFIDENTIAL

(c)   For each asset listed in **Q8(b)**,

     (i)   determine a related security goal.

                                          (12 marks)

     (ii)   determine the related threats. Support your answer with a misuse case diagram or any related diagram.

                                          (8 marks)

     (iii)   analyze the related risks.

                                          (8 marks)

     (iv)   produce the related security requirements.

                                          (8 marks)

- END OF QUESTION -