UTHM
Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2014/2015

COURSE NAME	:	FUNDAMENTAL OF INFORMATION SECURITY
COURSE CODE	:	BIS 10103
PROGRAMME	:	3 BIS
EXAMINATION DATE	:	JUNE 2015/ JULY 2015
DURATION	:	3 HOURS
INSTRUCTION	:	ANSWER **ALL** QUESTIONS

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

SECTION A

Q1 Which of the following statement is related to threat?

(A) Attacking a new web sites
(B) Phishing a web site
(C) Finding a new weakness in any network or systems
(D) Deleting files in a server

Q2 "*Controlled concurrency, simultaneous access, deadlock management and exclusive access as required.*" are examples of services related to __________.

(A) availability
(B) confidentiality
(C) integrity
(D) authorization

Q3 "*Alteration of data without permission of data owner*" is an example of attack against ___________.

(A) confidentiality
(B) integrity
(C) availability
(D) threat

Q4 What is a possible cipher text for the following plain text "*Information Security*" if the algorithm used is the common Caesar Cipher?

(A) Qwyabecbiw Vikxultbm
(B) Csyevixlifiw Zkjklmnm
(C) Lqirupdwlrq Vhfxulwb
(D) Ctiwerneicd Xxxymmu

Q5 Which of the following choices is a malicious code?

(A) Trojan
(B) Hacker code
(C) Backdoor
(D) Super code

Q6 Which of the following are tools or technique that takes advantages of vulnerability in order to exceed the user's authorized level of access?

(A) Exploits
(B) Backdoor
(C) Spyware
(D) Anti Virus

Q7 Which of the following is the activity in Reconnaissance?

(A) backup of critical data
(B) information gathering
(C) strategic planning
(D) probing the server

Q8 What will happen to the file if we changed more than 70% of its content and open the file using Microsoft Word Version 7?

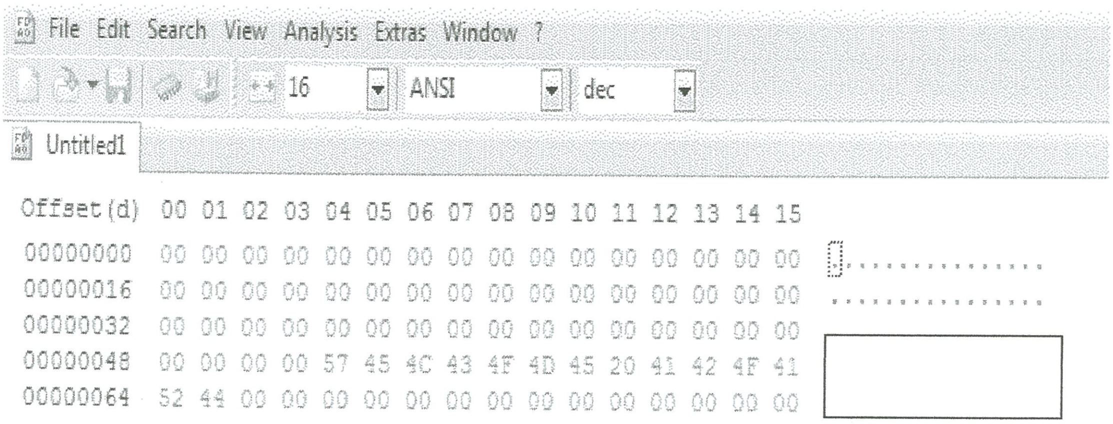
(A) File is corrupted and user is not able to view it content
(B) File is viewable with some distortion
(C) File can be view as the original file
(D) Half of the file is corrupted and only 20% file content viewable

Q9 Which of the following is **NOT** in the guidelines for password selection:

(A) Choose long password.
(B) Do not change password regularly
(C) Avoid using actual names or words.
(D) Use characters other than just A to Z.

Q10 If given Hex 41 as “A”, Hex 42 as “B”, what is the actual word in the following Hex Editor file depicted in **Figure Q8**?

(A) WHITE HAT HACKER
(B) HELLO THERE SON
(C) WELCOME ABOARD
(D) WELL DONE GUYS



```
Offset(d) 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15
00000000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000016  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000032  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000048  00 00 00 00 57 45 4C 43 4F 4D 45 20 41 42 4F 41
00000064  52 44 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

FIGURE Q8

Q11 One time passwords are very important for __________ because an intercepted password is useless.

(A) verification
(B) authorization
(C) authentication
(D) identification

Q12 Which of the following is the place that is chosen when hiding a secret message in Steganography?

(A) an email
(B) a still image
(C) another ciphertext
(D) another secret message with a very strong password

Q13 Which of the following concepts are enforced in Digital watermarking?

(A) Integrity
(B) Confidentiality
(C) Functionality
(D) Privacy

Q14 If a database is to serve as a central repository of data, users must be able to trust the _________ of the data values.

(A) accuracy
(B) integrity
(C) accuracy
(D) validity

Q15 Computer terminals in a stock, shares and bonds dealing room are set up to allow quick acceptance of trades. Which of the following would be the MOST sensible safeguard to limit loss through errors?

(A) Thorough staff training in the need to be careful integrity.
(B) Separate authorization of all trades.
(C) Confirmation of all trades before committing.
(D) Confirmation of trades which are over a set value.

(30 marks)

SECTION B

Q16 (a) Demonstrate the difference between Cryptography and Steganography in providing data protection using appropriate examples.

(6 marks)

(b) Explain **FIVE (5)** Classifications of Electronic Commerce (EC).

(10 marks)

(c) Provide **ONE (1)** example for each of the **THREE (3)** Offences under Malaysia Computer Crime Act 1997, Act 563.

(9 marks)

Q17 (a) The following RSA algorithm parameters are used to encrypt message by sender and decrypt message by receiver respectively.

Given the following values:

- Choose $p = 3$ and $q = 11$
- Choose e such that $1 < e < \varphi(n)$ and e and n are co-prime. Let $e = 3$
- Compute a value for d such that $(d * e) \bmod \varphi(n) = 1$.
- $(3 \times d) \bmod(\varphi(n)=1$
- The encryption of $m = 4$ is $c = 4^3 \bmod 33 = 31$
- The decryption of $c = 31$ is $m = 31^7 \bmod 33 = 4$

(i) Compute values of n and φ(n)?

(5 marks)

(ii) Compute corresponding values of Public Key **(e, n)** and Private Key **(d, n)?**

(5 marks)

(b) Decode the following ciphertext "RHA VTN USR EDE AIE RIK ATS OQR" using transposition cipher text if the key is "PRIZED".

(15 marks)

SECTION C

Q18 Consider the following scenario:

You just had been appointed as a new security administrator for a new ticketing system. Your team has been asked to prepare a proposal for implementing secure e-ticketing system. With this new system, customers are able to make an online booking, reschedule the book, make payment online and also view their booking status.

Outline a security design document consisting of physical and logical design, technologies, techniques and security mechanisms. Your report must address confidentiality, integrity and availability requirement associated with this system.

(20 marks)

- END OF QUESTION -