Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2022/2023

COURSE NAME	:	COMPUTER DATA SECURITY
COURSE CODE	:	BNF 43203
PROGRAMME CODE	:	BNF
EXAMINATION DATE	:	JULY / AUGUST 2023
DURATION	:	3 HOURS
INSTRUCTION	1.	ANSWER **ALL** QUESTIONS
	2.	THIS FINAL EXAM IS CONDUCTED VIA **CLOSED BOOK**
	3.	STUDENTS ARE **PROHIBITED** TO CONSULT THEIR OWN MATERIAL OR ANY EXTERNAL RESOURCES DURING THE EXAMINATION CONDUCTED VIA CLOSED BOOK

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

Q1 As an IT Engineer in a small private college, you are given a task to design a security system with the following requirements:

- Documents and files such as student's information, staff information, lecture notes, tests, financial data, salaries etc. are assigned with security classes (low level, medium level, and high-level security)
- All users (Upper management, Head of department, Lecturers, Clerks, and students) can access the system, but they were given a different security access clearance for documents and files in the server (very high, high, medium, and low security clearance respectively)
- All users were given a username with password requirement of combination of 6-digit numbers.
- The server rack will be located at the corner of IT section in the general office.

(a) There are a number of considerations need to be discussed and decided before designing a security system. For this particular company requirement, discuss **THREE (3)** design consideration and what is the decision for each one.

(6 marks)

(b) Based on the requirement, analyze and propose which security model is suitable for the system.

(6 marks)

(c) i) Analyze **THREE (3)** vulnerabilities in the system if you were to follow the requirement.

(3 marks)

ii) Propose improvement to the system to minimize the vulnerabilities.

(3 marks)

(d) A security policy for the organization contains rules and regulations to be adhered to by all users in the system. Propose a brief security policy for this college with at least **FOUR (4)** rules.

(7 marks)

Q2 (a) Illustrate the way symmetric encryption is used to send and receive private conversation in secured digital walkie-talkie.

(6 marks)

(b) Digital signature is one of the application of asymmetric encryption or public key encryption. Illustrate how it is used to confirm authenticity of sender in a legal email document.

(5 marks)

(c) Hash or digest is used to encrypt password for authentication of user to access a system. Explain how hackers cracked a user password using dictionary attack and compare the process with brute force attack.

(6 marks)

(d) Illustrate the detail of block chain process and how it is used to setup a new digital currency.

(8 marks)

Q3 (a) Differentiate the following malwares based on how they are spread:

(i) Worms
(ii) Viruses
(iii) Trojan Horses
(iv) Drive-by

(8 marks)

(b) Elaborate **FOUR (4)** malware detection methods in an antivirus software.

(8 marks)

(c) Describe the characteristics of "good" worm and how it is used in antivirus program.

(3 marks)

(d) Debate the advantages and disadvantages of passive and active intrussion detection system.

(6 marks)

Q4 (a) **Table Q4 (a)** represent the substitution cipher for encryption coding. The numbers are used for the RSA encryption.

Given the RSA keys below:

Public key, $K_V = (7, 33)$
Private Key, $K_R = (3, 33)$

Decrypt the following ciphertext message:

Ciphertext message: **! ? L X Y S I T N**

(6 marks)

(b) Using the same RSA keys in question **Q4(a)**, encrypt the following message:

Message : **H I J A C K E R S**

(6 marks)

(c) Explain with illustration the basic algorythm of DES encryption.

(7 marks)

(d) Explain **FOUR (4)** protocols used in Virtual Private Network (VPN).

(6 marks)

-END OF QUESTIONS –

FINAL EXAMINATION

SEMESTER / SESSION : SEM II / 2022/2023
COURSE NAME : COMPUTER DATA SECURITY
PROGRAMME CODE : BNF
COURSE CODE : BNF 43203

Table Q4 (a)

No	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Char	-	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
No	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Char	P	Q	R	S	T	U	V	W	X	Y	Z	.	!	?	$	/