Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER I
SESSION 2019/2020

COURSE NAME	:	COMPUTER DATA SECURITY
COURSE CODE	:	BNF 43203
PROGRAMME CODE	:	BNF
EXAMINATION DATE	:	DECEMBER 2019 / JANUARY 2020
DURATION	:	3 HOURS
INSTRUCTION	:	ANSWER **ALL** QUESTIONS

THIS QUESTION PAPER CONSISTS OF **FOUR (4)** PAGES

Q1 (a) Describe **THREE (3)** security properties. Elaborate each of them.

(5 marks)

(b) There are **FOUR (4)** types of security breach. Explain each of them and give an example of each breach.

(6 marks)

(c) Compare the difference between Stream cipher and Block cipher.

(3 marks)

(d) Explain **THREE (3)** considerations that need to be studied before designing a security system.

(6 marks)

Q2 (a) Draw a diagram on how the private encryption key can be used to secure the transfer of document between computers through the internet. Explain **ONE (1)** disadvantage using this method.

(5 marks)

(b) Explain how the public encryption keys is used to solve the private key encryption.

(4 marks)

(c) Secured Hash Algorithm (SHA) is one of the Hash algorithm standard. List another **FIVE (5)** standards of Hash algorithm.

(5 marks)

(d) Illustrate the detail of block chain process and how it can be used by Suruhanjaya Pilihan Raya Malaysia (SPRM) in the voting process for Malaysia.

(6 marks)

Q3 (a) Explain how the following malware are spread:

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

(8 marks)

(b) Explain **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.

(4 marks)

Q4 (a) Number in **Table Q4 (a)** represent the character for encryption coding. The numbers are used for the RSA encryption.

Given the RSA keys of

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

Decrypt the following ciphertext message:

Ciphertext message: **T N ? S ! T L I $**

(6 marks)

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

Message : **C Y B E R T E C H**

(6 marks)

(c) Explain the process of DES encryption.

(8 marks)

Q5 (a) State **TWO (2)** best known general attacks against block cipher and explain how they implement the attack.

(4 marks)

(b) List **FOUR (4)** security models and compare them in terms of their concepts and level of securities.

(8 marks)

(b) Differentiate **FOUR (4)** types of Intrusion Detection System (IDS) in terms of their advantages and disadvantages.

(8 marks)

-END OF QUESTIONS –

FINAL EXAMINATION

SEMESTER / SESSION : SEM I / 2019/2020
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	.	!	?	$	/