BRAINWARE UNIVERSITY

Coursework Examination 2018 – 19 (June 2019)

Programme – Ph.D. (CS) / Ph.D. (CSE)

Course name - Network Security

Course Code - PHD-CS-02

Time allotted: 3 Hours **Full Marks : 100**

[The figure in the margin indicates full marks. Candidates are required to give their answers in their own words as far as practicable.]

Group –A

(Multiple Choice Type Question) 10 x 1 = 10

1. *Choose the correct alternative from the following*

(i) Confidentiality with asymmetric-key cryptosystem has its own

a. Entities b. Data

c. Problems d. Translator

(ii) SHA-l has a message digest of

a. 160 bits b. 512 bits

c. 628 bits d. 820 bits

(iii) Message authentication is a service beyond

a. Message Confidentiality b. Message Splashing

c. Message Integrity d. Message Sending

(iv) The encryption standard having 48 bit round key is called as,

a. DES b. IDEA

c. AES d. RSA

(v) _____ does not allow the sender of a message to refute the claim of not sending that message.

a. Access control b. Availability

c. Non-repudiation d. Integrity

(vi) In Message Confidentiality, transmitted message must make sense to only intended

a. Receiver
b. Sender
c. Modulor
d. Translator

(vii) A hash function guarantees integrity of a message. It guarantees that message has not be

a. Replaced
b. Over view
c. Changed
d. Violated

(viii) In the _____ technique, the characters of plain text messages are replaced by other characters, numbers or symbols.

a. transposition
b. cipher
c. substitution
d. none of these

(ix) The working of SHA includes

a. Padding
b. Append length
c. Divide the input into 512 bit block
d. All of these

(x) Error detection technique is which of the following:

a. Cyclic redundancy check
b. Parity
c. Hamming codes
d. None of the above

Group – B

(Short Answer Type Questions) 6 x 5 = 30

2. Describe the basic uses of message encryption. 5
3. Discuss several attacks in network security. 5
4. What are the features of SSL? 5
5. Write the firewall design principals. 5
6. Explain web security threats with suitable example. 5
7. Explain SHA algorithm. 5
8. Explain DES algorithm. 5
9. Explain the five ingredients of symmetric encryption scheme. 5

Group – C

(Long Answer Type Questions) 6 x 10 = 60

Answer any *six* from the following

10.		Write down the principles of security with suitable example.	10
11.		Explain RSA algorithm and give example of generation of public and private keys and generation of cipher text through RSA.	10
12.		Explain RSA algorithm with suitable example.	10
13.		What is encryption and decryption? What is active and passive attacks?	10
14.		List the various types of attacks on encrypted system.	10
15.	(a)	What is cryptography?	3
	(b)	Distinguish between symmetric and asymmetric key cryptography.	4
	(c)	Explain substitution and transposition techniques.	3
16.		Write the digital signature standard algorithm.	10
17.	(a)	What is message digest?	5
	(b)	Write down the PGP operational description.	5
