USN | | | | | | | | | | |

10EC832

Eighth Semester B.E. Degree Examination, June/July 2018
Network Security

Time: 3 hrs. Max. Marks:100

Note: ***Answer any FIVE full questions, selecting at least TWO questions from each part.***

PART – A

1 a. List the examples of security attacks each of which has a risen in a number of real world cases. **(04 Marks)**

b. Give the table showing the relationship between security services and mechanism. **(08 Marks)**

c. Explain Gate keeper function with network access security model. **(08 Marks)**

2 a. Describe block cipher modes of operation in detail. **(10 Marks)**

b. Draw the single round of DES algorithm and explain the process. **(10 Marks)**

3 a. User A and B use D-H algorithm with a common prime q = 71 and primitive root $\alpha = 7$.
i) If user A has private key $X_A = 5$, what is A's public key Y_A?
ii) If user B has private key $X_B = 12$, what is B's public key Y_B?
iii) What is shared secret key K_A and K_B? **(03 Marks)**

b. Perform encryption and decryption using RSA algorithm for p = 12, q = 31, e = 7, $\mu = 2$. **(05 Marks)**

c. Write short notes on:
i) Digital signature standard
ii) Direct and arbitrated digital signature. **(12 Marks)**

4 a. Discuss briefly the working KERBEROS authentication protocol. **(12 Marks)**

b. Define the classes of message authentication functions. **(03 Marks)**

c. Describe the requirements for a Hash functions. **(05 Marks)**

PART – B

5 a. With a neat diagram, explain hand shake protocol action and the operation of record protocol of SSL. **(12 Marks)**

b. Explain in detail the following transactions supported by SET.
i) Purchase request
ii) Payment authorization **(08 Marks)**

6 a. Explain UNIX password scheme with a diagram. **(06 Marks)**

b. Explain the architecture of distributed intrusion detection with a neat diagram. **(08 Marks)**

c. Give examples of metrics that are useful for profile based intrusion detection. **(06 Marks)**

7 a. Give the taxonomy of malicious programs. List the software threats and explain them. **(08 Marks)**

b. With a diagram, explain digital immune systems. **(08 Marks)**

c. Write short notes on behaviour blocking software. **(04 Marks)**

8 a. Explain with neat diagram the various types of firewall configuration. **(09 Marks)**

b. Write short notes on: i) Reference monitor property
ii) Multilevel security requirements. **(06 Marks)**

c. With a neat diagram, explain the working of a packet-filter router. **(05 Marks)**

* * * * *