USN □□□□□□□□□□

10EC832

Eighth Semester B.E. Degree Examination, Dec.2016/Jan.2017

Network Security

Time: 3 hrs. Max. Marks:100

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

PART – A

1 a. What are the different types of active and passive attacks? **(05 Marks)**

b. Draw the model for network security and specify the four major tasks performed by it. **(04 Marks)**

c. For the cipher text "IMWNIAUP" find the plain text using the key "MINIMUM" using playfair cipher. **(05 Marks)**

d. In an S – DES encryption system the 10 bit key is given as 1001000110. P_{10} is given as $P_{10} = 2\ 7\ 1\ 6\ 3\ 5\ 4\ 9\ 10\ 8$. P_8 is given as $P_8 = 3\ 5\ 6\ 7\ 10\ 2\ 4\ 9$. Deduce sub keys K_1 and K_2. **(06 Marks)**

2 a. Explain with neat block diagrams a single round of DES encryption. **(10 Marks)**

b. Given the cipher text "E M Q Y". Find the plain text using the key $\begin{pmatrix} 1 & 1 \\ 3 & 2 \end{pmatrix}$ in Hill cipher. **(07 Marks)**

c. Write three differences between conventional cryptosystems and public key crypto systems. **(03 Marks)**

3 a. Write the RSA algorithm. **(05 Marks)**

b. In a public key system using RSA intercept the cipher text is 10, sent to a user where public key is 5 and n = 35. Deduce the plain text. **(05 Marks)**

c. What are message Authentication codes? Give the block diagrams to show how MAC is obtained for i) Authentication ii) Confidentiality and authentication tied to plain text and iii) confidentiality and authentication tied to cipher text. **(10 Marks)**

4 a. Draw a block diagram to show any one use of hash functions. **(02 Marks)**

b. Explain the arbitrated digital signature approach of the digital signature function. **(10 Marks)**

c. Explain with diagrams the signing and verifying of digital signature algorithm. **(08 Marks)**

PART – B

5 a. Show the SSL record protocol operation and the details of SSL record format with diagram and explain. **(06 Marks)**

b. Who are the participants of SET? Give the sequence of events required for SET. Explain with appropriate diagram. **(10 Marks)**

c. What are the requirements for digital signature? **(04 Marks)**

6 a. Explain why we need web security. **(02 Marks)**

b. Explain with diagrams how a new password is loaded and how a password is verified. **(10 Marks)**

c. Explain with diagram the distributed intrusion detection. **(08 Marks)**

7 a. Explain how the compression virus propagates. **(08 Marks)**

b. Explain the digital immune system. **(10 Marks)**

c. What are the limitations of fire walls? **(02 Marks)**

8 a. What are the characteristics of a bastion host? **(10 Marks)**

b. Explain with a diagram the application level gateway. **(10 Marks)**

* * * * *

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.
2. Any revealing of identification, appeal to evaluator and /or equations written eg, 42+8 = 50, will be treated as malpractice.