U.S.N □□□□□□□□□□

P.E.S. College of Engineering, Mandya - 571 401

(An Autonomous Institution affiliated to VTU, Belgaum)

Eighth Semester, B.E. - Information Science and Engineering

Semester End Examination; June - 2016

Network Security and Cryptography

Time: 3 hrs *Max. Marks: 100*

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

PART - A

1. a. Explain briefly the different consideration for an effective telecommunications use policy by outlining a sample ISP. 10

b. What is Business Impact Analysis? Explain the different stages of BIA conducted by a contingency planning team. 10

2 a. What is a VPN? What are the functions performed by a VPN? Explain transport mode and tunnel mode VPNs. 10

b. Describe briefly the five major processing-mode categories of firewalls. 10

3 a. Explain network-based IDPS stating the advantages and disadvantages. 10

b. List and describe the three control strategies proposed for IDPS control. 10

4 a. Explain briefly the different types of attacks on cryptosystems. 8

b. Explain the following :

i) Securing internet communication with S-HTTP and SSL. 12

ii) Securing E-mail with S/MIME.

PART - B

5 a. What is Kerberos realm? Explain how Kerberos supports interrealm authentication along with the details of exchanges. 10

b. Describe the general format of X.509 certificate. Also explain how certificates are revoked. 10

6. a Explain briefly the steps involved in PGP message generation and message reception. 10

b. List and explain the five header fields defined in MIME. Also describe S/MIME functionality and cryptographic algorithms used in S/MIME. 10

7 a. List and explain the different parameters which uniquely identify and define a security association. Also list the selectors which determine an SPD entry. 10

b. Explain transport and tunnel modes of IPSec ESP service. 10

8 a. Write a note on SSL record, alert and change cipher specification protocols. 10

b. Discuss the key features of SET and the sequence of events required for SET. 10

* * * *