Student Exam No: _____

GANPAT UNIVERSITY
M. TECH. SEM. - II COMPUTER ENGINEERING
REGULAR EXAMINATION APRIL - JUNE - 2016
3CE205: PUBLIC KEY INFRASTRUCTURE

Time: 3 Hours] **[Total Marks: 60**

Instructions:

1. Figures to the right indicate full marks.
2. Each section should be written in a separate answer book.
3. Be precise and to the point in your answer.

SECTION - I

Q:1 (a) Discuss the role of AS and TGS in Kerberos authentication protocol with the suitable diagram. **(6)**

(b) How do the digital certificates get created? Explain. **(4)**

OR

Q:1 (a) Elaborate the Feige-Fiat-Shamir protocol. **(6)**

(b) Discuss PGP. **(4)**

Q:2 (a) Using the Elgamal signature Scheme, p=71 and d=100. Choose r =17 and e1=11. Find values of S1, S2, V1 and V2. **(10)**

OR

Q:2 (a) Using the RSA signature scheme, p=51, q=43 and d= 31. Calculate the e and then create the signature S1 of the Message M=3 and verify it also. **(10)**

Q:3 (a) Discuss ESP Protocol in IPSEC. **(3)**

(b) Discuss various password based authentication scheme. **(5)**

(c) Briefly explain Zero knowledge. **(2)**

SECTION - II

Q.4 (a) Discuss about MD-5 Process using suitable diagram. (4)

(b) What is Certificate Path? Discuss it in brief. (3)

(c) What is the difference between CA and RA? (3)

OR

Q.4 (a) Discuss about certificate path construction of mesh and hierarchical PKI Architecture. (4)

(b) Show the comparison of MD-5 and SHA-1. (3)

(c) How Digital Certificates are used for Digital Signature? Explain it using suitable Diagram. (3)

Q.5 (a) What is Certificate Revocation List? How it is work? Explain it with suitable example. (4)

(b) Discuss about various parameters/fields of Digital Certificate. (3)

(c) Why the roaming certificate is needed? Explain it in brief. (3)

OR

Q.5 (a) How to protect the private keys? Explain about various mechanism of protecting private keys. (4)

(b) Which PKI Architecture should you important? Justify your answer. (3)

(c) Explain about E-voting Protocol in brief. (3)

Q.6 (a) Explain about following: (6)
1. Internet Key Exchange Protocol
2. PKCS

(b) What is Smart Card? Explain it in brief. (4)

END OF PAPER