Date: 18/05/2017

Exam No: _____

GANPAT UNIVERSITY

M. TECH SEM- II (Computer Engineering/Information Technology)

REGULAR EXAMINATION APRIL-JUNE 2017

3CE207/3IT207 : Public Key Infrastructure

MAX. TIME: 3 HRS **MAX. MARKS: 60**

Instructions: (1) This Question paper has two sections. Attempt each section in separate answer book.
(2) Figures on right indicate marks.
(3) Be precise and to the point in answering the descriptive questions.

SECTION: I

Q.1 **[A]** How 3-D secure Protocol differ than SET Protocol? Discuss about 3-D Protocol in brief. **(6)**

[B] Explain Replay Attack of IPSEC with suitable diagram. Consider W=64, N=50. Sender send packets, numbered 51 to 250, because of network traffic receiver receives packet number 100 first. What would be the movement of window? If receiver receives packet 52 after receiving packet 200 then, is that accept or reject? **(4)**

OR

Q.1 **[A]** What is IPSEC? Discuss about Transport Mode and Tunnel Mode with suitable Diagram. **(6)**

[B] On which layer of TCP/IP protocol suite SSL provides security? Explain record protocol and alert protocol of SSL in detail. **(4)**

Q.2 **[A]** What is the difference between PEM and S/MIME? Explain PEM step by step. **(6)**

[B] Based on following Parameters Check whether the verifier authenticate claimant successfully or not using Fiat-Shamir protocol. **(4)**
p=17, q=23, r=231, c=0 (Note: Perform only one round process)

OR

Q.2 **[A]** Discuss about challenge response entity authentication protocol using symmetric key cipher, asymmetric-key cipher and digital signature with diagram. **(6)**

[B] Explain Lempel-Ziv algorithm. Compress following text. **(4)**
"Jingle bells Jingle bells Jingle all the way"

Q.3 **[A]** Discuss about Dual Signature with suitable diagram. **(6)**

[B] Assume a 24-bit input as 111100000101100110101010, and transform it into its Base-64 encoding. (Note: Mapping Values: 6-bit values (0 to 25 -> A to Z, 26 to 51-> a to z, 52 to 61 -> 0 to 9, 62-> + ,63-> /, (padding) -> =) **(4)**

SECTION: II

Q.4 [A] What is PKI? Discuss about PKI Components in brief. (6)

[B] Discuss about Certificate Creation steps one by one. (4)

OR

Q.4 [A] Discuss various steps of Message Digest – 5 Algorithm. (6)

[B] How trust is established in PKI environment? What is out-of-band? (4)

Q.5 [A] Discuss about following: (6)
1. Hierarchical PKI Architecture
2. Technical Details of Digital Certificate

[B] How a CA Signs a Certificate? And How a Digital Certificate can be verified? (4)

OR

Q.5 [A] Discuss about following: (6)
1. CRL
2. PKCS
3. CPS

[B] What is the difference between OCSP and SCVP? (4)

Q.6 [A] How Kerberos protocols authenticate the client to access any service from the application server? Explain it with necessary diagram. Which types of problems addresses by Kerberos protocol? (6)

[B] Discuss about following protocols with reference to KDC. (4)
1. Needham-Schroeder Protocol
2. Otway-Rees Protocol

----------END OF PAPER----------