Student Exam No: _____

GANPAT UNIVERSITY
M. TECH. SEM. - II INFORMATION TECHNOLOGY
REGULAR EXAMINATION APRIL - JUNE - 2016
3IT205: 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 Kerberos protocol **(6)**

(b) Describe the properties of digital signature. **(4)**

OR

Q:1 **(a)** Given p=41, q=43 and n=1763. Choose s=71 and r=101. Simulate the steps of Fiat-Shamir Protocol. **(6)**

(b) Describe various approaches used in Challenge-Response mechanism for Authentication briefly. **(4)**

Q:2 **(a)** Discuss S/MIME briefly **(6)**

(b) Explain the concept of "Dual signature" in SET. And also explain its objective. **(4)**

OR

Q:2 **(a)** Using the RSA signature scheme, p=41, q=43 and d= 21. Calculate the e and then create the signature S1 of the Message M=3 and verify it also. **(10)**

Q:3 **(a)** Explain each following word in the context of PKI **(6)**
(i) Certification Authority
(ii) Registration Authority
(iii)Digital certificate

(b) Answer the following detail. **(4)**
(i) Explain How Bob finds out what cryptography algorithm Alice has used when he received S/MIME message from her.
(ii) What is the usage of key rings in PGP? Explain.

SECTION - II

Q.4	(a)	How PKI build up the trust in between the clients? Discuss about the various functions that needs to perform.	(4)
	(b)	Discuss about "Padding" and "Append Length" steps of MD-5 Algorithm.	(3)
	(c)	Discuss about components of PKI?	(3)

OR

Q.4	(a)	Explain about following PKI Architecture: 1. Single CA Architecture 2. Basic Trust list model	(4)
	(b)	How Digital Certificates are used for Message Encryption? Explain it using suitable Diagram.	(3)
	(c)	Discuss about Out-of-Band Transmission Channel with suitable example.	(3)
Q.5	(a)	What is the difference between OCSP and SCVP?	(4)
	(b)	What is the difference between direct digital signature and arbitrated digital signature?	(3)
	(c)	How CA Signs a Digital Certificate? Explain it with suitable diagram.	(3)

OR

Q.5	(a)	How to protect the private keys? Explain about various mechanism of protecting private keys.	(4)
	(b)	Explain about Certificate Practice Statement with example.	(3)
	(c)	Explain about E-voting Protocol in brief.	(3)
Q.6	(a)	Explain about following: 1. AH and ESP (IPSec main protocol) 2. MAC and MD-5	(6)
	(b)	What is Smart Card? Explain it in brief.	(4)

END OF PAPER