Student Exam No: _____

GANPAT UNIVERSITY

B. TECH. SEMESTER – VII COMPUTER ENGINEERING/INFORMATION TECHNOLOGY

REGULAR EXAMINATION NOVEMBER/DECEMBER - 2014

2CE704 / 2IT704: PUBLIC KEY INFRASTRUCTURE

TIME:-3 HOURS] [TOTAL MARKS: 70

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) How does public key cryptography work? Discuss about any one algorithm of public key cryptography. [4]

(B) Discuss about following: [4]

a. Certificate Authority b. PKI Clients

(C) Explain about Single CA Architecture with Example. [4]

OR

Q – 1 (A) Discuss about Key Expansion Process of AES. [4]

(B) Discuss about following: [4]

a. Registration Authority b. Certificate Distribution System or Repository

(C) Explain about Enterprise PKI Architecture with Example [4]

Q– 2 (A) Discuss about steps which are involved in working with PKI. [6]

(B) What is the Digital Certificate? Discuss about the Technical details of Digital certificates. [5]

OR

Q – 2 (A) Discuss about Hierarchical PKI Architecture. How the certificate path construction starts in a Hierarchical PKI Architecture. [6]

(B) Discuss about Structure of X.509 Digital Certificate. [5]

Q – 3 (A) Explain about Certificate Revocation and discuss about following: [6]

a. CRL b. OCSP

(B) Convert the Byte (8B) into (3D) using Sub Byte Transformation of AES using GF(2^8) with the irreducible polynomial $x^8 + x^4 + x^3 + x + 1$. [6]

Constant Matrix: $\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$ Constant Column Vector: $\begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$

SECTION – II

Q – 4	(A)	Discuss about following steps of MD5. **a.** Padding **b.** Append Length	[4]
	(B)	Discuss about following Authentication Token Types. **a.** Challenge/Response Tokens **b.** Time-based Tokens	[4]
	(C)	What is Dual Signature? Discuss it in brief.	[4]

OR

Q – 4	(A)	Explain about 'something Derived from Passwords' with reference to Password based Authentication.	[4]
	(B)	Explain about MD5 Algorithm with suitable Diagram.	[4]
	(C)	Discuss about Record Protocol and Alert Protocol of SSL.	[4]
Q – 5	(A)	Explain about Secure Multipurpose Internet Mail Extensions (S/MIME).	[6]
	(B)	Explain about Secure Electronic Transaction Participants.	[5]

OR

Q – 5	(A)	How PGP Certificates does works? Discuss about Introducer trust and Certificate trust.	[6]
	(B)	What is Kerberos? How does Kerberos Works?	[5]
Q – 6	(A)	Discuss about following with reference to Handshake protocol of SSL. **a.** Establish security capabilities **b.** Server Authentication and key exchange	[6]
	(B)	How Pretty Good Privacy (PGP) works? Discuss it in brief.	[6]

END OF PAPER