Student Exam No. ______________

GANPAT UNIVERSITY

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

REGULAR EXAMINATION NOV - DEC 2015

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) What is PKI? Discuss about PKI Components in brief. [4]

(B) Discuss about following with reference to Processes in PKI: [4]
a. Certificate Requests b. Certificate Revocation

(C) Discuss about "Alice can obtain the CAs public key out–of–band" [4]

OR

Q – 1 (A) Discuss about Mixing and Shift-Row Transformation of AES. [4]

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

(C) Explain about Basic Trust List model with suitable Example. [4]

Q– 2 (A) Discuss Certificate creation steps in brief. [6]

(B) Discuss about the contents of a Digital Certificate in brief. [5]

OR

Q – 2 (A) Explain about Certificate Hierarchies and Self-signed Digital Certificates. [6]

(B) How CA signs a Digital Certificate? Discuss it with suitable Diagram. [5]

Q – 3 (A) Discuss about CRL and OCSP with suitable Diagrams. [6]

(B) Convert the Byte (FF) into (16) 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 Secure Electronic Transaction (SET) Participants. [4]

(B) Explain about 'something Derived from Passwords' with reference to Password based Authentication. [4]

(C) What is Dual Signature? Discuss it in brief. [4]

OR

Q – 4 (A) Step by step list out the Secure Electronic Transaction (SET) Process. [4]

(B) Discuss about 3-D Secure Protocol in brief. [4]

(C) Discuss about following with reference to PEM. [4]
1. Canonical Conversion 2. Base-64 Encoding

Q – 5 (A) Explain about The working process of Pretty Good Privacy (E-mail security protocol). [6]

(B) Discuss about Login and Obtaining a Service Granting Tickets (TGT) steps of KERBEROS. [5]

OR

Q – 5 (A) Encrypt the letter "G" using Knapsack Crypto System. Super increasing tuple b=[1,2,3,6,12,24,48] , Permutation Table [4,2,5,3,1,7,6], modulus n=98 and random integer r=5 is given. [Binary value of "G" is 1100111] [6]

(B) Discuss about Record Protocol and Alert Protocol of SSL. [5]

Q – 6 (A) Discuss about step by step working process of MD5. [6]

(B) Based on given Input Matrix and Constant Matrix, Convert the Byte (A6) into (ED) using Mixing Transformation of AES. [6]

Input Matrix:

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

Constant Matrix:

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

END OF PAPER