Student Exam No. ______________

GANPAT UNIVERSITY
B. TECH. SEMESTER – VII COMPUTER ENGINEERING/INFORMATION TECHNOLOGY
REGULAR EXAMINATION NOV - DEC 2016
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) Discuss about Needham-Schroeder Protocol with suitable Example. [4]

(B) Discuss about Four Round Process of MD-5 Algorithm with suitable Diagram. [4]

(C) Discuss about SET Participants with suitable Diagram. [4]

OR

Q – 1 (A) Discuss about KDC in brief. [4]

(B) Explain about Knapsack Crypto System in brief. [4]

(C) Explain about PAYMENT AUHORIZATION and PAYMENT CAPTURE with reference to SET Protocol. [4]

Q– 2 (A) Discuss about following Term: [6]

1. Digital Signature 2. Digital Certificate 3. Digital Envelope

(B) Based on given Input Matrix and Constant Matrix, Convert the Byte (8C) into (A5) using Mixing Transformation of AES. [5]

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

OR

Q – 2 (A) Convert the Byte **00** into **52** using Inverse Sub Byte Transformation of AES using GF(2^8) with the irreducible polynomial $x^8 + x^4 + x^3 + x + 1$. Constant matrix and Constant Column Vector is given below: [6]

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

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

Q – 3 (A) List out the components of PKI. Explain functionality of all the components in detail and show how all components are correlated to each other with suitable diagram. [5]

(B) Explain the PKI architecture in which cross certificate is there, also write advantages and disadvantages. [4]

(C) Name the four key steps in the creation of digital certificate. Explain all in detail. [3]

SECTION – II

Q – 4 (A) Discuss about Something Derived Password Technique in brief. [4]

(B) Discuss about LOGIN Process of KERBEROS in brief. [4]

(C) Discuss about Key Expansion Process of AES Algorithm. [4]

OR

Q – 4 (A) How the 3D Secure Protocol works? Discuss it in brief. [4]

(B) Discuss about following Term with reference to AES Algorithm. [4]

1. Mixing Transformation
2. Key adding Transformation

(C) Explain about Smart Card Based User Authentication in brief. [4]

Q – 5 (A) What is Authentication Token? Explain about Time based Authentication Token in brief. [6]

(B) Perform Encryption and Decryption using Elgamal Cryptosystem. Required parameters are given below: [5]
P=11, d=3, e1=2,r=8 and Plain Text=10

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 Biometric based Authentication in brief. [5]

Q – 6 (A) Explain the working of PEM in detail. [4]

(B) Answer the following: [4]

1. PEM allows __________ security operations.
   a. 2 b. 3 c. 4 d. 5

2. A way of verifying both the sender of information and the integrity of a message is through the use of _____________.
   a. Digital Certificate
   b. Digital Signature
   c. Public Key Encryption
   d. Private Key Encryption

3. Which of the following is true about Public Key Infrastructure?
   A. PKI is a combination of digital certificates, public-key cryptography, and certificate authorities that provide enterprise wide security.
   B. PKI uses two-way symmetric key encryption with digital certificates, and Certificate Authority.
   C. PKI uses private and public keys but does not use digital certificates.
   D. PKI uses CHAP authentication.

4. Define: Delta CRL

(C) Answer the following: [4]

1. What is Lampel - Ziv algorithm? Apply Lampel – Ziv algorithm on following message:
   "Welcome to the world of security. The world of security is full of interesting problems and solutions."
2. Explain web of trust in PGP.

END OF PAPER