Student Exam No: ________

GANPAT UNIVERSITY
M. TECH. SEMESTER – I COMPUTER ENGINEERING
REGULAR EXAMINATION DECEMBER - 2013
3CE105: CRYPTOGRAPHY AND NETWORK SECURITY

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 Digital Signature. [3]

(B) Encrypt the following plain text Message using One Time Pad Algorithm.
Plain Text: "Software Engineering" Key: "dpgjcswalnmtrxhbrof" [3]

(C) Discuss about Security Principles in brief. [6]

OR

Q – 1 (A) Encrypt and Decrypt the following Plain Text message Using Rail Fence Transposition Technique.
Plain text: "Secure Data Transmission" . Fence Value: 7 [4]

(B) Discuss about Feistel Cipher Structure with Example. [4]

(C) Discuss about Following term: [4]
1) DNS Spoofing
2) Masquerading

Q– 2 (A) Explain about Man in the Middle Attack with suitable Diagram [5]

(B) Discuss about Any Two Algorithm Modes with suitable example. [6]

OR

Q – 2 (A) Discuss about DMZ with reference to Firewall. [5]

(B) Discuss about Key Expansion Process of DES in brief. [6]

Q – 3 (A) Decrypt the following Cipher Text Message using 3x3 hill Cipher. [6]
(Note: you may get unknown information)

Cipher Text: "TRDWUN " **Key Matrix:** $\begin{bmatrix} 2 & 1 & 1 \\ 1 & 1 & 2 \\ 1 & 0 & -2 \end{bmatrix}$

(B) How PGP (Pretty Good Privacy) Works? Explain it in brief. [6]

SECTION – II

Q – 4 **(A)** Solve following equations [3]
$2x - 7y = 5 \bmod 11$

(B) Find out Inverse of 103 in GF (2347). [3]

(C) Give the last two bytes of output word from Mix column round of AES if [6]
input word is $\begin{bmatrix} 50 \\ ed \\ 13 \\ a4 \end{bmatrix}$ and matrix of mix column is $\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$

OR

Q – 4 **(A)** Solve following congruence operations using Chinese reminder Theorem [4]
$X = 3 \bmod 11$
$X = 2 \bmod 5$
$X = 2 \bmod 3$

(B) Discuss about following Term in brief. [8]
1) HMAC
2) Secure Socket Layer

Q – 5 **(A)** Check primality of given numbers using Fermat and Miller-Rabin test. [5]
561, 61

(B) Explain how RSA algorithms works with suitable key pair (e, d) and message (M). [6]

OR

Q – 5 **(A)** Find out GCD (987, 1246). [2]

(B) Find out order of group, order of each elements and primitive roots for Z^*_{13}. [3]

(C) Simulate Rabin cryptosystem for set of prime numbers p = 13, q = 19 ad message M = 23. [6]

Q – 6 **(A)** How Elgamal cryptosystem works? Simulate it with prime number p = 11 and message M = 13. [6]

(B) Given the super increasing sequence b = [2, 5, 7, 9, 10, 12], w = 13 and modulus = 47, simulate knapsack cryptosystem for letter ‘P’. [6]

END OF PAPER