Student Exam No: ________

JAN 2012

GANPAT UNIVERSITY
M. TECH. SEMESTER – I INFORMATION TECHNOLOGY
REGULAR EXAMINATION
PGIT-105: INFORMATION 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 One Time Key pad. [3]

(B) What is the Difference between Cryptography and Stegnography? [3]

(C) Discuss about following Terms: [6]
a) Non repudiation b) Replay attack c) DOS attack

OR

Q – 1 (A) Decrypt the following Encrypted message using playfair Cipher Technique. [6]
Encrypted Message: "XFOLIXMKPVLR"
Keyword: "Parallel Processing"

(B) Discuss about following Substitution Technique: [6]
1. Variable Caesar Cipher
2. Poly-alphabetic Cipher

Q– 2 (A) Alice and Bob want to establish a secret key using the diffie-hellman key exchange protocol. Assuming the values as n = 509, g = 11, x = 18, y = 124, Find out the values of A, B and the secret key K1 and K2. [6]

(B) Discuss about Feistel Cipher Technique [4]

(C) What is Cryptology? [1]

OR

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

(B) Discuss about Claude Shannon Concepts. [5]

(C) What is Block Cipher? [1]

Q – 3 (A) Encrypt the following Plain Text data using Hill cipher technique. [8]

Plain text: "Wonderful" **Key Matrix:** $\begin{bmatrix} 1 & 3 & 1 \\ 1 & 1 & 2 \\ 2 & 3 & 4 \end{bmatrix}$

(B) Discuss about Dynamic Packet Filter with reference to Firewall. [4]

SECTION – II

Q – 4 (A) Explain about Digital Envelope in Brief. [6]

(B) Explain about SSL in brief. [6]

OR

Q – 4 (A) Discuss about Following Terms: [6]

a) Birthday Attack b) application gateway

(B) Discuss about E - Mail Privacy Protocol. [6]

Q – 5 (A) Compute the multiplication of {FA} and {25} in the GF(2^8) modulo the irreducible polynomial {01}{1B} used in AES. [5]

(B) Encrypt the message 10001 10110 using Merkle-Hellman scheme. [6]

OR

Q – 5 (A) Mathematically prove the working of RSA cryptosystem. [5]

(B) Consider the Cryptanalysis of affine cipher in Z_{26} where letter 'R' is the encryption of letter 'E' and letter 'K' is the encryption of letter 'T'. Then find the key of affine cipher corresponds to above cryptanalysis. [6]

Q – 6 (A) If Public key in RSA is (31, 3599) then find the corresponding private key. [6]

(B) **Answer the followings.** [6]

1. Give the elements of Z^*_{30}.
2. Give 6^{30} mod 31 = _____ and 6^{240} mod 31 = _____

END OF PAPER