Student Exam No: _________

GANPAT UNIVERSITY
M. TECH. SEMESTER – I COMPUTER ENGINEERING
REGULAR EXAMINATION
PGCE – 105: CRYPTOGRAPHY AND NETWORK SECURITY

- JAN 2012

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) Encrypt the following plain text Message using Variable Caesar Cipher. **[3]**
Plain Text: "Network Security" Key: 2X + Y

(B) What is DNS spoofing? Explain it in brief. **[3]**

(C) Discuss about following Security Principles **[6]**
a) Confidentiality b) Authentication c) Access Control

OR

Q – 1 (A) Encrypt the following Plain Text message Using Double columnar Transposition Technique. **[4]**
Plain text: "Computer engineering" **Keyword:** 24135

(B) What is the difference Between Stream cipher and Block Cipher **[4]**

(C) Encrypt the following message with vigenere cipher with key "abcdef" **[4]**
Plain text: "crypto is for cryptography"

Q– 2 (A) Explain The Key transformation Steps of DES algorithm with suitable diagram. **[5]**

(B) Discuss about Following Algorithm Modes: **[6]**
a) ECB b) CBC

OR

Q – 2 (A) Discuss about Types of Firewall in brief. **[5]**

(B) Explain about double DES and Triple DES in Brief. **[6]**

Q – 3 (A) Encrypt the following plain text message using 3x3 hill cipher. **[6]**

Plain Text: "Operating system" **Key Matrix:** $\begin{bmatrix} 2 & 1 & 1 \\ 1 & 1 & 2 \\ 1 & 0 & -2 \end{bmatrix}$

(B) Alice and Bob want to establish a secret key using the diffie-hellman key exchange protocol. Assuming the values as n = 353, g = 3 , x = 97 , y = 233, find out the values of A,B and the secret key K1 and K2 **[6]**

SECTION – II

Q – 4 (A) Discuss about Firewall Configurations. [4]

(B) Discuss about following Phases of SSL Handshake Protocol. [8]

1. Establish Security Capabilities
2. Server Authentication and key exchange
3. client Authentication and key exchange
4. Finish

OR

Q – 4 (A) Discuss About Following with reference to SSL protocol [4]

a) The record protocol b) The Alert protocol

(B) What is MAC? Discuss about HMAC in Brief [8]

Q – 5 (A) If Public key in RSA is (19, 3599) then find the corresponding private key. [5]

(B) Comment whether the sequence <2 3 6 13 27 52> can be used as a Merkle-Hellman key or not. If it can, then specify the private and public keys to be used in the scheme and encrypt the message 011000110101. [6]

OR

Q – 5 (A) Explain key Distribution in Secret Key Cryptography. [5]

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

Q – 6 (A) Compute the multiplication of {57} and {83} in the GF(2^8) modulo the irreducible polynomial {01}{1B} used in AES. [6]

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

1. Find $(-939)^{-1}$ mod 26
2. 19 ≡ ____ mod 101
3. Find 10^{126} mod 127 = ____ and 10^{882} mod 127 = ____

END OF PAPER