Student Exam No: _____

GANPAT UNIVERSITY
M. TECH. SEM. - I COMPUTER ENGINEERING / INFORMATION TECHNOLOGY
REGULAR EXAMINATION JANUARY - 2013
3CE105/3IT105: 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 following: **(6)**
1) Non Repudiation 2) Sniffing 3) Masquerade

(b) Decrypt the following Encrypted message using playfair Cipher Technique. **(3)**
(**Note:** put j and i both combine as a single field)
Encrypted Message: tmazinyamtluazinekla
Keyword: india is my country

(c) Find out the multiplicative inverse of 79 in GF (3220). **(3)**

OR

Q.1 **(a)** Discuss about CBC and CFB algorithm modes with suitable diagram. **(6)**
(b) Find the inverse of e = 17 for RSA where p = 101 and q = 199 **(4)**
(c) If there are 956 users in the network then how many key pairs is required in symmetric cryptography operation? **(2)**

Q.2 **(a)** Perform mix column transformation of AES on following column matrix. **(6)**
Required constant matrix is given below.

Column matrix: $\begin{bmatrix} 4D \\ 90 \\ 4A \\ D8 \end{bmatrix}$ **Constant matrix:** $\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$

(b) What is the value of Ø(13) and Ø(240)? **(5)**

OR

Q.2 **(a)** Decrypt the following Cipher Text message using 3x3 Hill Cipher. **(6)**
Cipher Text: edxphy **Key Matrix:** $\begin{bmatrix} 2 & 1 & 1 \\ 1 & 1 & 2 \\ 1 & 0 & -2 \end{bmatrix}$

(b) Discuss about mathematical theory behind the Diffe Hellman key exchange Algo. **(5)**

Q.3 **(a)** Show how the byte **0E** is transformed to **AB** by subbyte routine in AES using $GF(2^8)$. Required constant matrix for calculation is given below. **(6)**

Constant Matrix:
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

Constant column matrix:
1
1
0
0
0
1
1
0

(b) Perform the Primality Test using Fermat's theorem and Miller Rabin Test. (6)
1) 18 2) 17 3) 14

SECTION-II

Q.4 (a) Discuss about Principle of Security in Brief. (6)

(b) Explain about Symmetric key and Asymmetric key cryptography together with Digital Envelope method. (6)

OR

Q.4 (a) Alice and Bob want to establish a secret key using the diffie-hellman key exchange protocol. Assuming the values as n = 23, g = 5, x = 6, y = 8, Find out the values of A, B and the secret key K1 and K2. (6)

(b) Discuss about Record protocol and Alert Protocol of SSL in brief (6)

Q.5 (a) What is HMAC? Explain it. (4)

(b) Discuss about Problem of Key Distribution or Key exchange in symmetric key cryptography. (4)

(c) Explain about Feistel Cipher Structure with diagram. (3)

OR

Q.5 (a) Discuss about Network Address Translation with Example. (4)

(b) Discuss about Types of Firewall in brief. (4)

(c) Give the elements of set Z^*_{35} (3)

Q.6 (a) Discuss about E-mail Security using PGP. (6)

(b) Discuss about Key Transformation process of DES step by step. (6)

END OF PAPER