Exam No: _____

GANPAT UNIVERSITY

M. TECH SEM- I (IT) REGULAR EXAMINATION – NOV-DEC: 2014

3IT105: Cryptography And Network Security

MAX. TIME: 3 HRS MAX. MARKS: 60

Instructions: (1) This Question paper has two sections. Attempt each section in separate answer book.
(2) Figures on right indicate marks.
(3) Be precise and to the point in answering the descriptive questions.

SECTION - I

Q.1 **(a)** Perform decryption in Playfair Cipher algorithm with cipher text as " XFOLIXMKPVLR" and obtain original plain text. Keyword is "PLAYFAIR EXAMPLE". (Note: 1. Put j and i both combine as a single field in 5*5 matrix). **[5]**

(b) Explain below mentioned attacks: **[5]**
1) Replay Attack 2) Traffic analysis 3) DoS Attack

OR

Q.1 **(a)** Define Cryptography and Steganography. Discuss these two with example. **[5]**

(b) Draw block diagram to show steps of one round in DES and explain 'Expansion Permutation' step with example. **[5]**

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

Column matrix: $\begin{matrix}87\\6E\\46\\A6\end{matrix}$ **Constant matrix:** $\begin{bmatrix}02 & 03 & 01 & 01\\01 & 02 & 03 & 01\\01 & 01 & 02 & 03\\03 & 01 & 01 & 02\end{bmatrix}$

(b) Describe one time pad algorithm with example. **[4]**

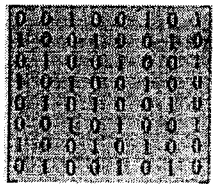
OR

Q.2 **(a)** Explain CBC and CFB algorithm modes with diagram. **[6]**

(b) Using the Diffie-Hellman key exchange algorithm Alice and Bob want to agree upon a secret key. Assuming the values as n = 17, g = 5, x = 4, y = 6, Find out the values of A, B and the secret key K1 and K2. **[4]**

Q.3 **(a)** Differentiate block cipher and stream cipher algorithm with example. **[3]**

(b) Show how the byte **AB** is transformed to **OE** by Invsubbyte routine in AES using *GF* (2^8). Required constant matrix for calculation is given below. **[7]**

Constant Matrix:  **Constant column matrix:** 

SECTION-II

Q.4 (a) Given the super increasing Tuple b= [7, 11, 23, 43, 87,173,357] and modulus n = 1001, encrypt the letter 'g' using knapsack Cryptosystem. Use [7, 6, 5, 1, 2, 3, 4] as the permutation table. (note: ASCII value of 'g' is 1100111) [5]

(b) Explain Alert protocol and Handshake protocol in SSL. [5]

OR

Q.4 (a) Explain Rabin Cryptosystem with example. [5]

(b) Describe symmetric key and asymmetric key cryptography with digital envelope using block diagram. [5]

Q.5 (a) Find the inverse of e = 23 for RSA where p = 101 and q = 199 [5]

(b) Describe static packet and dynamic packet filter in firewall. [5]

OR

Q.5 (a) Find the multiplicative inverse of following numbers in Z_{180} using the extended Euclidean algorithm. 1) 132 2) 24 3) 7 4) 38 [6]

(b) Explain about email security using Pretty Good Privacy Protocol. [4]

Q.6 (a) Explain Application gateway and Birthday attack. [5]

(b) Perform the Primality Test using Fermat's theorem and Miller Rabin Test. 1) 43 2) 31 [5]

END OF PAPER