Student Exam No: _____

GANPAT UNIVERSITY
M. TECH. SEM. - I COMPUTER ENGINEERING/INFORMATION TECHNOLOGY
REGULAR EXAMINATION NOVEMBER - DECEMBER - 2015
3CE105/3IT105: CRYPTOGRAPHY AND NETWORK SECURITY

Time: 3 Hours] **[Total Marks: 60**

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: **(4)**
1) IP spoofing 2) Phishing

(b) Decrypt the following Encrypted message using 6x6 playfair Cipher Technique. **(3)**
Encrypted Message: UOMOSKFRSTSJGQIOLANETAUOSR
Keyword: NATIONAL INSTITUTE OF STANDARD AND TECHNOLOGY

(c) Discuss about set of residues, congruence, and residue class with reference to modulus. **(3)**

OR

Q.1 **(a)** What are algorithm modes? Discuss it in brief. **(4)**

(b) Discuss about Euler's phi Function (Ø (n)) with example. **(4)**

(c) What is the difference between mono-alphabetic Vs. Poly-alphabetic? **(2)**

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

Input Matrix:

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

Constant Matrix:

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

(b) Solve the Linear Congruence: $2x+3y \equiv 5 \pmod 8$ **(4)**
$x+6y \equiv 3 \pmod 8$

OR

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

(b) How the Diffie-Hellman Algorithm solve the problem of key exchange in between two users? **(4)**

Q.3 **(a)** Encrypt the letter "G" using Knapsack Crypto System. Super increasing tuple b=[1,2,3,6,12,24,48] , Permutation Table [4,2,5,3,1,7,6], modulus n=98 and random integer r=5 is given. (note: ASCII value of 'g' is 1100111) **(6)**

(b) Perform the Miller-Rabin Primality Test on following. **(4)**
1) 83 2) 97

SECTION-II

Q.4 (a) Discuss about digital signature using suitable diagram. (5)

(b) Discuss about HMAC in brief. (5)

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 = 31, g = 17, x = 8, y = 10, Find out the values of A, B and the secret key K1 and K2. (5)

(b) Solve the following Equation using Chinese Remainder Theorem. (5)
$X \equiv 2 \bmod 17$
$X \equiv 3 \bmod 13$
$X \equiv 5 \bmod 11$

Q.5 (a) Discuss about attacker's techniques to break the security of packet filter. (4)

(b) Discuss about "PGP allows three security options when sending an email message". (4)

(c) What is Digital Envelope? (2)

OR

Q.5 (a) Discuss about NAT with suitable Example. (4)

(b) Discuss about Handshake protocol of SSL. (4)

(c) Solve the Quadratic Equation: $X^2 \equiv 7 \pmod{19}$ (2)

Q.6 (a) Discuss about Rabin Cryptosystem with suitable Example. (4)

(b) Show how the byte **5F** is transformed to **CF** by subbyte routine in AES using *GF* (2^8). Required constant matrix for calculation is given below. (6)

Constant Matrix:
$$\begin{bmatrix} 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \\ 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \end{bmatrix}$$

Constant Column Vector:
$$\begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

END OF PAPER