Exam No: _____

GANPAT UNIVERSITY

M. TECH SEM- I (Computer Engineering/Information Technology)

REGULAR EXAMINATION NOV-DEC 2017

3CE103/3IT103: 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) Discuss about following with reference to Modulus (6)
1. Set of residues
2. Congruence
3. Residue class

(B) Solve the following Linear Congruence. (4)

1. $5x \equiv 12 \pmod{23}$
2. $210x \equiv 40 \pmod{212}$

OR

Q. 1 (A) Perform mix column transformation of AES on Second 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) What is the difference between Man in the middle attack and meet in the middle attack? (4)

Q.2 (A) Encrypt the following Plain Text message using 3x3 Hill Cipher. (6)

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

(B) Perform the Miller-Rabin Primality Test on following. (4)
1) 79 2) 92

OR

Q.2 (A) What is Secure Socket Layer? Discuss about "Establish Security Capabilities" and "Server Authentication and key exchange" Phases of SSL Handshake Protocol. (6)

(B) Discuss about Virus and Trojan Horse attack in brief. (4)

Q.3 (A) Discuss about Feistel Cipher Structure in brief. (4)

(B) What are the best characteristics of symmetric key and asymmetric key? (4)

(C) What is additive inverse and multiplicative inverse? (2)

SECTION: II

Q.4 (A) What is Message Authentication Code? How the HMAC is differing than MAC? **(6)**

(B) If Public key in RSA is (19, 3599) then find the corresponding private key. **(4)**

OR

Q.4 (A) What is Firewall? Discuss it in brief. **(6)**

(B) Discuss about attacks on RSA. **(4)**

Q.5 (A) Discuss Vigenere Cipher algorithm and encrypt the message "I LOVE INDIA" using the keyword "AHMEDABAD". **(6)**

(B) Solve the following using Chinese remainder theorem **(4)**
$4x \equiv 2 \pmod 6$
$3x \equiv 5 \pmod 8$

OR

Q.5 (A) Discuss about following **(6)**
1. Digital Envelope
2. Digital Signature
3. Message Digest

(B) Discuss about Rabin Cryptosystem with suitable Example. **(4)**

Q.6 (A) Compute the multiplication of {57} and {83} in the GF (2^8). Irreducible polynomial {01}{1B} is given. **(6)**

(B) **Answer the followings.** **(4)**
1. Find $(-939)^{-1} \bmod 26$
2. $19 \equiv$ ____ mod 101

----------**END OF PAPER**----------