Student Exam No: _____

GANPAT UNIVERSITY
B. TECH. SEM.-VI COMPUTER ENGINEERING/INFORMATION TECHNOLOGY
REGULAR EXAMINATION APRIL-JUNE - 2017
2CE603/2IT603: INFORMATION SYSTEM 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)** Find $456^{17} \bmod 17 =$ _____ and $145^{102} \bmod 101 =$ _____ using fermat's theorem. **(4)**

(b) Explain Extended Euclidean algorithm and find out the Multiplicative Inverse of 23 in Z_{100}. **(3)**

(c) Explain Vernam cipher (one time pad) with example. **(3)**

OR

Q.1 **(a)** Solve the following Linear equations: **(4)**

(i) $9x + 4 \equiv 12 \pmod 7$

(ii) $232x + 42 \equiv 248 \pmod{50}$

(b) Explain Euler's phi-function Ø(n) with all rules, then Solve the following using its applicable rules: **(3)**

(i) Ø (240)

(ii) Ø (49)

(c) Explain about Virus, Worms and Trojan Horse. **(3)**

Q.2 **(a)** Explain Polyalphabetic encryption and encrypt the following message with vigenere cipher with key "PASCAL" and Plain text: "She is listening". **(5)**

(b) Explain complete algorithm of Miller-Rabin test and check whether 201 pass the Miller-Rabin test or not? **(5)**

OR

Q.2 **(a)** Describe Chinese Remainder Theorem and solve the following equations using Chinese Remainder Theorem. **(5)**

$X \equiv 4 \bmod 5$

$X \equiv 10 \bmod 11$

(b) Describe Rail fence cipher technique with example (take depth=3). **(5)**

Q.3 **(a)** Find out the Multiplicative Inverse for the following values using Fermat Theorem. (take a=2) **(5)**

(i) $5^{-1} \bmod 23$ (ii) $60^{-1} \bmod 101$

(b) Write technique of Square Root Primality Test, then perform test on "17". **(5)**

SECTION – II

Q.4 **(a)** How encryption and decryption is performed using cipher feedback algorithm mode? Explain it in detail with diagram. **(3)**

(b) What is message digest? What are the key requirements of message digest? Explain it with diagram. **(4)**

(c) What is symmetric key cryptography? What are the problems with symmetric key encryption? How to solve the problem of symmetric key encryption? **(3)**

OR

Q.4 **(a)** Explain Feistel cipher structure in detail with diagram. **(5)**

(b) Explain Digital envelope in detail with diagram. **(5)**

Q.5 **(a)** In which variation of DES meet-in-the-middle attack is possible? Why? Explain meet-in-the-middle attack in DES with diagram. **(5)**

(b) Given two prime numbers P=3 and Q=11, find out N,E and D using RSA algorithm. Perform encryption on plaintext character 'G' and decrypt the generated cipher text character. (Note: map A to Z with 0 to 25) **(5)**

OR

Q.5 **(a)** Explain broad level steps for PGP in detail with necessary diagram. **(5)**

(b) Which security principles are achieved by MAC? Explain working of MAC in detail with diagram. **(5)**

Q.6 **(a)** Define following terms: **(2)**
(i) Confusion
(ii) Diffusion

(b) Draw the broad level steps for working of DES. Explain details of one round with diagram. **(6)**

(c) Write about packet filter firewall in brief. **(2)**

End of Paper