Student Exam No: _____

GANPAT UNIVERSITY

B. TECH. SEMESTER – VI COMPUTER ENGINEERING/INFORMATION TECHNOLOGY

REGULAR EXAMINATION APRIL - JUNE - 2015

2CE603/2IT603: INFORMATION SYSTEM 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 Network Address Translation with reference to Firewall. [4]

(B) Discuss about Additive Inverse and Multiplicative Inverse with Example. [4]

(C) Find out the value of phi (ø) for given values. [4]
1) 529 2) 40000

OR

Q – 1 (A) Find out the Multiplicative inverse of 23 in Z_{121} using Extended Euclidean Algorithm. [4]

(B) What is the difference between MD and MAC? Explain about Birthday Attack with reference to MD. [4]

(C) Prove that Miller-Rabin is stronger then Fermat Little Theorem. [4]

Q– 2 (A) Discuss Merkle-Hellman Knapsack using following parameter and perform encryption and decryption on plain text letter "G". [6]
1. Super increasing tuple b= {2, 4, 7, 15, 33} 2. Consider modulo n = 67 and r=11 3. permutation order = {1,5,3,2,4}

(B) Find all solutions of the following Linear Equations. [5]
$7x + 11y \equiv 3 \pmod 7$, $9x + 2y \equiv 5 \pmod 7$

OR

Q – 2 (A) Explain about RSA Algorithm with suitable example. Why RSA is better than DES? [6]

(B) Discuss Encryption and Decryption process of Rabin Crypto System. [5]

Q – 3 (A) Discuss about following: [6]
1. Record Protocol in SSL
2. Alert Protocol in SSL

(B) Compare the Symmetric key and Asymmetric key with respect to following characteristics. [6]
1. Size of resulting encrypted text
2. key used for encryption and decryption
3. speed of encryption and decryption

SECTION – II

Q.4 (A) Discuss about following principles of security with real life examples : [6]

1) Confidentiality 2) Integrity 3) Availability

(B) Describe Mono-alphabetic Cipher with example and possibility of cryptanalysis for it. [6]

OR

Q.4 (A) Explain Feistel Cipher Structure and its design features with diagram. [6]

(B) Perform encryption for the plaintext "computer" using Hill Cipher. Key matrix is given below. [6]

$$\text{Key Matrix} \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

Q.5 (A) Explain about man in the middle attack in DES with suitable example. [4]

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

(C) What are the differences between Confusion and Diffusion? [3]

OR

Q.5 (A) Discuss about CTR and CFB algorithm modes with suitable diagram. [6]

(B) Explain how following practical approaches used by attackers for security violation. [5]

1) Applets 2) Trojan Horse 3) Cookies

Q.6 (A) Describe double DES and triple DES with suitable diagram. [6]

(B) Discuss about mathematical theory behind the Diffie Hellman key exchange Algorithm. [6]

END OF PAPER