Student Exam No._____

GANPAT UNIVERSITY

B. Tech. Semester: VI Computer Engineering/Information Technology

Regular Examination April – June 2016

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

Que. – 1 A. Compare symmetric key and asymmetric key cryptography. [4]

B. What is the purpose of message digest in information security? Give its requirements. [4]

C. Find all solutions of the linear equation $5x + 3 \equiv 13 \pmod 7$. [4]

OR

Que. – 1 A. Check whether 37 is prime or not using Fermat and Miller-Rabin primality test. [4]

B. Find all solutions of the linear equation $6x \equiv 12 \pmod 9$. [4]

C. Give example of super increasing knapsack with 5 elements and convert it to non-super increasing knapsack using Merkle-Hellman scheme. [4]

Que. – 2 A. Explain the following terms with suitable diagram: [6]
1) NAT 2) CFB

B. Discuss the following terms in detail : [5]
1) SSL Handshake Protocol 2) CTR

OR

Que. – 2 A. Discuss the difference between ECB and CBC with appropriate diagram. [6]

B. Perform the encryption and decryption of message "great" using Affine cipher. [5]

Que. – 3 A. Show the encryption of message "HI" using RSA algorithm (Choose suitable RSA parameters). Also show the decryption process. [6]

B. Find the multiplicative inverse of 581 in Z_{647} using Extended Euclidean algorithm. [4]

C. Find the value of Euler's totient function ø(214). [2]

Section – II

Que. – 4 A. Discuss encryption and decryption of transposition cipher with suitable example. [6]

B. Do the encryption using play fair cipher where key is ICC T20 WORLD CUP and plain text is WINNER25. Show the decryption also. [6]

OR

Que. – 4 A. Discuss encryption and decryption of Vernam cipher with suitable example. [6]

B. Find the cipher text using a Hill cipher where key matrix is $\begin{matrix} 1 & 1 & 0 \\ -1 & 0 & 1 \\ 1 & 1 & 1 \end{matrix}$ and plain text is GNU. Show the decryption also. [6]

Que. – 5 A. Define key distribution problem and find the K1 and K2 using Diffie-Hellman algorithm where g=19, n=23, x=4, y=8. [6]

B. Define worm and discuss security goals in brief. [5]

OR

Que. – 5 A. Define lock-key pair. Discuss man in middle attack with suitable example. [6]

B. What is Pharming? Explain passive attacks with suitable example. [5]

Que. – 6 A. Draw the broad level diagram of DES. Explain expansion permutation in DES. [4]

B. Explain Meet-in-the-middle attack with appropriate example. [4]

C. Define Confusion. If the input for the following S-Box 2 in DES is 011011 then find out the output. [4]

S_2

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

END OF PAPER