Student Exam No: _____

GANPAT UNIVERSITY

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

REGULAR EXAMINATION – MAY 2014

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) Explain about Digital Envelope with suitable diagram. [4]

(B) Discuss about following with reference to modular arithmetic. [4]
1) Set of residues
2) additive Inverse and Multiplicative Inverse

(C) Find out the value of phi (ø) for given values. [4]
1) 1716 2) 165

OR

Q – 1 (A) What is Congruence? Find all solutions of the following Linear Equations. [4]
$9x + 4 \equiv 12 \pmod 7$

(B) Apply the Fermat and Miller-Rabin Primality test on following values and justify your answers. (Note: base a=2) [4]
1) 561 2) 37

(C) Discuss about Miller-Rabin Primality Test with suitable Example. [4]

Q– 2 (A) For given P=5 and Q=11, calculate the Encryption Key(e) and Decryption key(d) and perform the Decryption operation on following Plain Text using RSA. (Note: A to Z map with 0 to 25) [6]
PT: "ROYAL"

(B) Find all solutions of the following Linear Equations. [5]
$7x + 3y \equiv 3 \pmod 7$, $4x + 2y \equiv 5 \pmod 7$

OR

Q – 2 (A) Solve the following equation using Chinese remainder theorem. [6]
$X \equiv 31 \pmod{49}$
$X \equiv 6 \pmod{20}$

(B) alice & bob want to establish a secret key using the Diffie-hellman key exchange protocol. Assume the values as n=17, g=23, x=4 and y=6. Find out the values of A, B and secret key K1 and K2. [5]

Q – 3 (A) What is the difference between Mono-alphabetic and Poly-alphabetic Cipher? Discuss about vigenere Cipher [6]

(B) Discuss about Types of Firewall in brief. [6]

SECTION – II

Q – 4	(A)	Discuss about use of S-BOXES in DES.	[4]
	(B)	Discuss about following Term: 1) Stream cipher and block cipher 2) Confusion and Diffusion	[4]
	(C)	Explain about following Security goals. 1) Authentication 2) Access control	[4]

OR

Q – 4	(A)	Discuss about key distribution problem in Symmetric key cryptography.	[4]
	(B)	Discuss about following term with reference to DES analysis. 1) key 2) S-Boxes	[4]
	(C)	Discuss about Message Digest in brief.	[4]
Q – 5	(A)	Explain about RSA algorithm with suitable example.	[6]
	(B)	Discuss about Meet in the Middle Attacks in brief.	[5]

OR

Q – 5	(A)	What is SSL? Discuss it in brief.	[6]
	(B)	Is it possible to identify the message from Message Digest? Justify your answer with example.	[5]
Q – 6	(A)	Perform the Encryption and Decryption on following Plain Text Message using 6 by 6 matrix Play Fair Cipher. PT: "MY NAME IS JOY AND MY DATE OF BIRTH IS 29101978" KEY: "OPERATION VIJAY 3456MHAD12"	[6]
	(B)	Discuss about Vigenere Cipher with example.	[6]

END OF PAPER