Student Exam No.________________

GANPAT UNIVERSITY

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

Regular Examination May – June 2013

2CE603/2IT603: INFORMATION SYSTEM SECURITY

Time: 3 Hours **Total Marks: 70**

Instruction:

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 Find GCD (970, 566) [4]

B Find out multiplicative inverse 20 & 50 in GF (101) using extended Euclidean method. [4]

C Write brief short note on [4]

i) Broadcast attack

ii) Coppersmith Theorem attack

OR

Que. – 1

A Find out QR and QNR for Z_{13}* [4]

B Test the primality of following numbers using Millar-Rabin Test and Fermet's Test [4]

(i) 561 (ii) 2047

C Explain significance of totient function in Euler's theorem with suitable example. [4]

Que. – 2

A Explain chosen cipher text attack on RSA with example. [6]

B Using Chinese Reminder Theorem, solve following set of congruence [5]

i) x = 7 mod 13

ii) x = 5 mod 11

iii) x = 4 mod 7

OR

Que. – 2

A What is Primitive root? Find out Primitive roots of < Z_{21}*, *> [4]

B Solve the following equation [4]

i) 3x - 2 = 6 mod 13

ii) 2x + 8 = 13 mod 11

C In RSA N = 3937 and e = 17, find d. (Do factorization of N). [3]

Que. – 3

A **Under Knapsack cryptosystem,** Given super increasing sequence <12 17 33 74 157 316>, M = 737 and W = 635, Encrypt number 51 and also decrypt the cipher. (Convert the number in binary form). [6]

B Given p = 31, q = 19 **Under Rabin cryptosystem**, encrypt message M = 21 to find cipher text, also find equally probable four roots by decrypting cipher text and obtain plain text. [6]

Section – II

Que. – 4

A Explain principle of information security with example and discuss possible active and passive attacks on information. [6]

B What is Brand theft and Identity theft? Explain using Phishing attack. [4]

C Explain Confusion and Diffusion in brief. [2]

OR

Que. – 4

A Explain Play Fair cipher and encrypt the following plain text. [4]
Plain text: MEETING IS SCHEDULED AT 10AM
Keyword: STUDENTS OF SEMESTER 6

B Perform **double** columnar transposition technique on following plain text data and convert it into cipher text. Also explain on how to get back original text data. (key = 1357462) and Plain text = 'ganpat university' [4]

C Discuss an attack that breaks the security of a packet filter. [4]

Que. – 5

A Find out key using Diffie-Hellman key exchange algorithm on which Alice & Bob agreed upon for future communication with values given below. [6]
Large prime nos. known to Alice & Bob are n = 21 and g = 17

- Alice choose value (x) = 8
- Bob choose value (y) = 15

Can Diffie-Hellman key exchange algorithm solve all problems associated with key exchange? Explain your answer with example.

B Explain Feistel cipher with 32-bits block size and 48 bits key size having 4 rounds. [5]

OR

Que. – 5

A Discuss about following algorithm modes with diagram. [6]

1. Electronic Code Block (ECB)
2. Cipher Feedback Mode (CFB)

B Explain about Network Address Translation (NAT) in brief. If Two users with same IP want to communicate with single remote host then how NAT perform such communication. [5]

Que. – 6

A Key exchange problem with symmetric key encryption algorithms [3]

B State the use of Initialization Vector (IV) in CBC mode? Is it necessary to keep IV secret, why? [3]

C "Combining two cryptography techniques are better than single cryptography technique". Explain with example. [3]

D Explain Message Digest (MD) and Massage Authentication Code (MAC) in brief. [3]

END OF PAPER