Student Exam No. _____

GANPAT UNIVERSITY

B. Tech SEMESTER VI COMPUTER ENGINEERING / INFORMATION TECHNOLOGY

REGULAR EXAMINATION MAY/JUNE - 2012

CE/IT 603: 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) Find GCD (1970, 1066) **[3]**

(B) Solve the following equation **[4]**

$3x + 5y + 7z = 3 \bmod 16$

$x + 4y + 13z = 3 \bmod 16$

$2x + 7y + 3z = 3 \bmod 16$

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

OR

Q.1

(A) Discuss RSA cryptosystem with example. **[4]**

(B) Using Fermat's theorem, find out $22^{-1} \bmod 211$ **[3]**

(C) Elaborate the Fermat primality test for n = 561 **[2]**

(D) Find out QR and QNR for Z_7^* **[2]**

Q.2

(A) Under **Knapsack cryptosystem**, Given super increasing sequence <12 17 33 74 157 316>, M = 737 and W = 635, Encrypt number 50 and also decrypt the cipher. (Convert the number in binary form). **[4]**

(B) Explain significance of totient function in Euler's theorem with suitable example. **[4]**

(C) Write brief short note on **[4]**

i) Broadcast attack

ii) Coppersmith Theorem attack

OR

Q.2

(A) Using Chinese Reminder Theorem, solve following set of congruence **[4]**

i) $x = 5 \bmod 13$

ii) $x = 3 \bmod 5$

iii) $x = 6 \bmod 11$

(B) What is Primitive root? Find out Primitive roots of $< Z_{11}^*, * >$ **[4]**

(C) In RSA given p=41 and q=43, Public key e= 11. Encrypt the message M = 100. Also find out private key d. **[4]**

Q.3

(A) Given p = 47, q = 11 **Under Rabin cryptosystem**, encrypt message M = 19 to find cipher text, also find equally probable four roots by decrypting cipher text and obtain plain text. **[5]**

(B) Explain chosen cipher text attack on RSA with example. **[5]**

(C) Explain Related Message attack in brief. **[2]**

SECTION-II

Q.4

(A) Explain Diffie Hellman key exchange algorithm and mathematically proves correctness of algorithm. **[6]**

(B) Explain Play Fair cipher and decrypt the following cipher text. **[6]**
(Use J / I as combine letter)
Cipher text: QMAKAGMTWTWTTHMNMEBHDNTS
Keyword: MASTER OF TECHNOLOGY

OR

Q.4

(A) Explain about Network Address Translation (NAT) in brief. If Two users with one IP wants to communicate with single remote host then how NAT perform such communication. **[6]**

(B) Discuss about following algorithm modes with diagram. **[6]**
1. Electronic Code Block (ECB)
2. Cipher Block Chaining (CBC)

Q.5

(A) Discuss about Message Authentication Code (MAC) in brief. **[4]**

(B) Explain DES with major steps with diagram. **[4]**

(C) Alice and Bob want to establish a secret key using the Diffie Hellman key exchange protocol. Assuming the values as n = 37, g = 5, x = 14, y = 134, **[3]**
Find out the values of A, B and the secret key K1 and K2.

OR

Q.5

(A) Discuss about Message Digest with example. **[4]**

(B) Discuss about following Terms **[4]**
1. Cryptography 2. Steganography

(C) Write a short note on Pharming. **[3]**

Q.6

(A) Compare Double DES and Triple DES. **[4]**

(B) Discuss Vigenere classical cipher algorithm with example. **[4]**

(C) Encrypt the following message using Variable Caesar cipher algorithm. **[4]**
Message: good morning Key = 4 + position of character

--- END OF PAPER ---