COLLEGE OF ENGINEERING, PUNE

(An Autonomous Institute of Government of Maharashtra.)
SHIVAJI NAGAR, PUNE - 411 005

END Semester Examination

(CT-14002) Cryptography and Network Security

Course: B.Tech Branch: Computer Engineering

Semester: Sem VII

Year: 2014-2015 Max.Marks:60

Duration: 3 Hours Time:- 2pm - 5pm Date: 26 NOV 2014

Instructions: MIS No. | | | | | | | | | |

1. Figures to the right indicate the full marks.
2. Mobile phones and programmable calculators are strictly prohibited.
3. Writing anything on question paper is not allowed.
4. Exchange/Sharing of anything like stationery, calculator is not allowed.
5. Assume suitable data if necessary.
6. Write your MIS Number on Question Paper

Q.1. (a) **List and explain different types of security services.** **[5]**

(b) **Use transposition cipher to encrypt the message** **[5]**
"MEET ME AT BOAT CLUB CANTEEN"
The key for encryption is: "EXAMPLE"

Q.2. (a) **An old woman goes to market and a horse steps on her basket and crushes the eggs. The rider offers to pay for the damages and asks her how many eggs she had brought. She does not remember the exact number, but when she had taken them out two at a time, there was one egg left. The same happened when she picked them out three, four, five, and six at a time, but when she took them seven at a time they came out even. What is the smallest number of eggs she could have had?** **[6]**

(b) State whether 4 is the primitive root of 5. Justify your answer. [2]

(c) Find the totient value of 81. [2]

Q.3. Use simplified IDEA algorithm for encryption of the message below: [10]

Message: 1110 1111 1001 0101

Key:

1100 0110 0011 0101 1111 0111 0101 1010

Q.4 (a) Compare Asymmetric Encryption and Symmetric Encryption. [5]

(b) Use RSA algorithm to encrypt the message M =123 using following parameters [5]

$$p = 11, q = 3, e = 13$$

Q.5. (a) What is the size of hash value for SHA-1. If the message size is 746, state whether padding is needed. If yes how many numbers of bits are required for padding this message? If no why? Justify your answer for both the cases. [5]

(b) What is the roll of SSL protocol in network security. Explain the various phases of SSL handshake protocol. [5]

OR

(b) Explain the Kerberos protocol V4 for key distribution. Explain the functionality of each step. Also discuss the roll of TGS in Kerberos. [5]

Q.6. (a) With neat diagrams, briefly explain the all types of firewalls. [4]

(b) Explain following malwares: [6]

i) Virus

ii) Worms

iii) Trojans

OR

(b) What are the different types of intruders? Discuss each with example. [6]