Total No. of Pages: 1 *Roll No. .....*

EIGHT SEMESTER **B.TECH (SE)**

MID SEMESTER EXAMINATION *(MARCH 2019)*

SE-408 INFORMATION SECURITY

Time: 1.5 hours *Max. Marks: 25*

Note: Attempt **all** questions.
Assume suitable missing data, if any.

1. How is privacy different from security? What are the principles of security and various attacks possible? What is the privacy issue in various applications used like Whatsapp, Facebook, Gmail etc. (5)

2. How is symmetric encryption different from asymmetric encryption? Explain Meet in the Middle Attack in Diffie Hellman Key Exchange (DHKE)? Compute group key for g=3, p=11 and private no. of Alice is 3 and private no. of Bob is 4. (5)

3. Explain DES encryption with block diagram. What is birthday paradox? Show meet in the middle attack on triple DES? (5)

4. Explain Elgamal Encryption with example. Compute RSA keys for p=53 and q = 59 and encrypt and decrypt m = "HI".[Use value of H as 8 and I as 9 to compute m] (5)

5. Write short note on (any two): (5)

   a. IDEA with block diagram
   b. Polyalphabetic vs Mono alphabetic Cipher
   c. Any two substitution Cipher