Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

CAT – I Question Paper – Jan'2020

Programme: B. Tech | **Slot : A1**
Course : Cryptography Fundamentals | **Code : CSE1011**
Max. Marks: 50 | **Duration: 1½ Hrs**

[5 X 10M = 50M]

Answer ALL Questions

1. a) Enlighten the modes of block cipher that can be used to encrypt/decrypt the variable size of data. *[7 Marks]*

   b) In CBC mode, bits **17** and **18** in ciphertext block 9 are corrupted during transmission. Find the possible corrupted bits in the plaintext. *[3 Marks]*

2. Mr. Ravi works in a government office where encrypted messages are regularly received. He knows that an affine cipher is the standard method of encryption used by the office, and has access to the machine which encrypts. One day, when there is not much work to do, Ravi decides to work out the affine function used in the machine. He inputs 1 and the machine outputs 5. He inputs 2 and the machine outputs 19. Show step by step how he uses this to obtain the function.

3. Explain the key generation and encryption/decryption procedure of IDEA.

4. a) A 6×2 S-box exclusive-ors the odd-numbered bits to get the left bit of the output and exclusive-ors even-numbered to get the right bit of the output. If the input is 110010, what is the output? If the input is 101101, what is the output? **[5 marks]**

   b) State the properties of the Euler's totient function Ø(n). **[5 marks]**

5. a) Use the Playfair cipher to encipher the message "hidden". The secret key can be made by filling the first and part of the second row with the word "GUIDANCE" and filling the rest of the matrix with rest of the alphabet. **[7 Marks]**

   b) A small club has only 100 members. How many secret keys are needed if all members of the club need to send secret messages to each other using symmetric key cryptosystem. **[3 Marks]**

****