BIRLA INSTITUTE OF TECHNOLOGY, MESRA, RANCHI
(MID SEMESTER EXAMINATION)

CLASS: BE **SEMESTER: VI**
BRANCH: IT **SESSION : SP/2020**

SUBJECT : IT6023 COMPUTER NETWORK AND SECURITY

TIME: 1.5 HOURS **FULL MARKS: 25**

INSTRUCTIONS:
1. The total marks of the questions are 30.
2. Candidates may attempt for all 30 marks.
3. In those cases where the marks obtained exceed 25 marks, the excess will be ignored.
4. Before attempting the question paper, be sure that you have got the correct question paper.
5. The missing data, if any, may be assumed suitably.

Q1 (a) What are the different types of classical encryption techniques? [2]
(b) Discuss the different types of Modes of Operation using a suitable block diagram. [3]

Q2 (a) Compare the symmetric-key and asymmetric-key cryptography. [2]
(b) Given the key 'GYBNQKURP', apply the Hill cipher to the plaintext 'ACT'. Prove the authenticity of the message. [3]

Q3 (a) Why we are using XOR operation in the Feistel cipher? [2]
(b) Discuss the different types of transformation involved for decryption in AES cipher. [3]

Q4 (a) Write the steps to produce ciphertext C from plain text p using triple DES with two keys. [2]
(b) Explain the meet-in-the-middle attack. [3]

Q5 (a) Define the discrete logarithmic problems. [2]
(b) How sender can send a message securely to receiver by using RSA algorithm. Explain the different steps involved in this during encryption, and decryption. [3]

Q6 (a) Define the different possible attacks on RSA. [2]
(b) What are the steps for key calculation by sender, receiver and attacker in the man-in-the-middle attack? [3]

:::::: 03/03/2020 ::::::M