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

CLASS: BE **SEMESTER: VI**
BRANCH: IT **SESSION : SP/2019**

SUBJECT : IT6023 COMPUTER NETWORKS 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) Explain the key principles of security? What are the security approaches to implement in security model? [2]
(b) List and briefly define categories of passive and active security attacks with example. [3]

Q2 (a) Distinguish between Stream Cipher & Block Cipher? Give examples. [2]
(b) Using the Vigenere cipher, encrypt the word "cryptography" using the key house. Also perform decryption. [3]

Q3 (a) What is the life cycle of a key? [2]
(b) Encrypt the message "good morning" using the Hill cipher with key k= $\begin{bmatrix}6 & 4\\ 5 & 7\end{bmatrix}$. [3]

Q4 (a) Define algorithm modes. Explain Cipher feedback with suitable example. [2]
(b) With suitable block diagram explain the working of DES Algorithm. [3]

Q5 (a) Differentiate between Symmetric and Asymmetric Cryptography with suitable example. [2]
(b) Given two prime numbers P=47, Q=71, find out n,e and d in the RSA encryption process. [3]

Q6 Write short notes on:
i) Affine Cipher
ii) Diffie –Hellman key exchange

[2.5*2]

:::: 06/03//2019 E::::::