

NAVODAYA INSTITUTE OF TECHNOLOGY, RAICHUR

SUBJECT: CRYPTOGRAPHY & NETWORK SECURITY (BCS703)

Assignment-1 Questions

Module 1

1. Define Cryptography & explain symmetric cipher model?
2. Explain Hill Cipher & apply it to encrypt Plain text = **paymoremoney** with key.

$$K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 9 \end{bmatrix}$$

3. Explain Play fair Cipher and its rules for the following example:
Ex: Keyword: "MONARCHY" Plaintext: a. "ATTACK"
b. "CRYPTOGRAPHY"
4. Explain Feistel Encryption & Decryption in detail.
5. Explain working of DES Algorithm with Example?
6. Explain DES construction in detail with a neat diagram.
7. List and explain the block cipher design principles.
8. Explain Vernam Cipher & OTP.

Module 2

9. Explain the public key cryptosystem with a neat diagram.
10. List the difference between Conventional and public key encryption