**Time: 3 Hrs** **Marks: 80**

**Note:**

1. **Question 1 is compulsory.**
2. **Attempt any 3 questions out of the remaining questions.**

Q1.

| | | |
|---|---|---|
| a. | Explain active and passive attack with example. | 05 |
| b. | Compare and contrast block and stream chiper | 05 |
| c. | Encrypt the message "ENEMY ATTACKS TONIGHT" with keyed columnar transposition cipher with encryption key 31452 | 05 |
| d. | Explain the difference between virus and worm | 05 |

Q2

| | | |
|---|---|---|
| a. | Explain Needham-Schroeder protocol for secret key distribution with suitable diagram. | 10 |
| b. | Write a short note on MD5 and its working | 10 |

Q3.

| | | |
|---|---|---|
| a. | Explain how entity authentication can be achieved using digital signatures | 10 |
| b. | Describe the various components of Kerberos and explain how it works | 10 |

Q4.

| | | |
|---|---|---|
| a. | List and explain security services and security mechanisms in detail. | 10 |
| b. | Explain working of PGP protocol | 10 |

Q5.

| | | |
|---|---|---|
| a. | Explain the man-in-the-middle attack for Diffie-Hellman. How to overcome the same. | 10 |
| b. | Explain AES algorithm in detail | 10 |

Q6.

| | | |
|---|---|---|
| a. | What are confusion and diffusion in cryptography? | 05 |
| b. | Explain different types of DOS attack? | 05 |
| c. | Using Affine cipher, encrypt the plaintext "SECURITY" with key pair (5,2) | 05 |
| d. | Short note on different types of authentication. | 05 |

**********



75D8E3CF77ED0252F6C15C1FD68F7372