CBCS SCHEME

USN | | | | | | | | | | |

15CS743

# Seventh Semester B.E. Degree Examination, June/July 2019
## Information and Network Security

Time: 3 hrs. Max. Marks: 80

**Note: Answer any FIVE full questions, choosing ONE full question from each module.**



### Module-1

1 a. Given the Caesar's cipher find plain text from the ciphertext DQWUDUHSVSRQJERHER **(03 Marks)**

b. Encrypt the message "We are all together" using a double transposition cipher with 4 rows and 4 columns, using the row permutation (1, 2, 3, 4) → (2, 4, 1, 3) and column permutation (1, 2, 3, 4) → (3, 1, 2, 4). **(05 Marks)**

c. Justify that one fine pad is provably secure. Also give the reason why we cannot use the key twice. **(08 Marks)**

**OR**

2 a. Define the terms confusion and diffusion in the context of cryptology. **(02 Marks)**

b. Explain three broad categories of ciphers. **(06 Marks)**

c. Given the taxonomy of cryptanalysis. **(08 Marks)**

### Module-2

3 a. Elaborate Birthday problem and correlate it with hash functions. **(06 Marks)**

b. Justify that Tiger hash is fast and secure, elaborating its working principle. **(10 Marks)**

**OR**

4 a. Discuss different schemes used in secret sharing with special reference to key Escrow. **(08 Marks)**

b. Mention the significance of generating proper random numbers, with special reference to Texas Hold'em Poker. **(08 Marks)**

### Module-3

5 a. Explain different types of Freshness mechanisms. **(08 Marks)**

b. Explain Dynamic password scheme with an example. **(08 Marks)**

**OR**

6 a. List the components of cryptographic protocol. Also mention the stages involved in protocol design. **(08 Marks)**

b. Explain about Deffie – Hellaman key agreement protocol. **(08 Marks)**

### Module-4

7 a. Briefly explain the key Life cycle. **(06 Marks)**

b. Explain different types of key generation in detail. **(10 Marks)**

**OR**

8 a. Briefly explain the concept of IDPKC. **(06 Marks)**

b. Explain different public key Management modules in detail. **(10 Marks)**

## Module-5

9 a. Explain how cryptography is used in SSL. **(06 Marks)**

b. Discuss about SSL handshake protocol. **(06 Marks)**

c. List the design issues in SSL. **(04 Marks)**

**OR**

10 a. Explain about Cryptography use in magnetic stripe cards. **(06 Marks)**

b. Discuss in detail, Cryptography for home users with respect to File protection and Email security. **(10 Marks)**

* * * * *