CBCS SCHEME

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

15CS743

Seventh Semester B.E. Degree Examination, Aug./Sept. 2020
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. Define the following terms :
i) Cryptography ii) Plaintext iii) Ciphertext iv) Encryption v) Decryption. **(05 Marks)**

b. Find the plaintext and the key from the ciphertext given that the cipher is a simple substitution of the shift – by – n variety.
IRXUVFRUHDAGVHYHABHDUVDIR **(05 Marks)**

c. Encrypt the message attack at down using a double transposition cipher with 3 rows and 4 columns, using the row permutation (1, 2, 3) → (3, 2, 1) and the column permutation (1, 2, 3, 4) → (4, 2, 1, 3). **(06 Marks)**

OR

2 a. Using the following letter encodings

e	h	i	k	ℓ	r	s	t
000	001	010	011	100	101	110	111

Encrypt the given plaintext "heilhitter" using the key "trsrtℓerse" with one time pad cipher. Discuss drawbacks of the time pad? **(08 Marks)**

b. What is HASH function? Discuss the uses of hash functions. **(08 Marks)**

Module-2

3 a. Explain the detail the Tiger hash cryptographic function. **(08 Marks)**

b. What is randomness briefly; discuss the approaches to generating randomness. **(08 Marks)**

OR

4 a. With a neat diagram, explain how passwords are protected in Unix operating systems. **(08 Marks)**

b. What is freshness mechanism? Briefly discuss Nonce based freshness mechanism. **(08 Marks)**

Module-3

5 a. Discuss the need for cryptographic protocols in detail. **(08 Marks)**

b. Discuss in detail the different stages in designing a cryptographic protocol. **(08 Marks)**

OR

6 a. What is dynamic password scheme? Illustrate with diagram how a user is authenticated in dynamic password scheme. **(08 Marks)**

b. Describe the man – in – the – middle attack on the Diffie – Hellman protocol in detail. **(08 Marks)**

Module-4

7 a. With diagram, explain the different phases of key lifecycle. **(08 Marks)**
  b. Discuss the reasons why cryptographic keys have finite lifetimes. **(08 Marks)**

OR

8 a. Discuss the different public key certificate management models. **(08 Marks)**
  b. Briefly discuss the SSL security requirement and security issues. **(08 Marks)**

Module-5

9 a. Discuss the handshake and Record cryptographic protocol employed in SSL. **(08 Marks)**
  b. Briefly discuss the different attacks on WEP. **(08 Marks)**

OR

10 a. Briefly discuss the key management issues relating to cryptography in payment cards. **(08 Marks)**
  b. With diagram, discuss the eID card issuing process. **(08 Marks)**

* * * * *