CBCS SCHEME

63

USN | | | | | | | | | |

15CS743

Seventh Semester B.E. Degree Examination, Dec.2019/Jan.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. With a neat diagram, explain crypto as a block box. **(05 Marks)**

b. Using vernam cipher encrypt the Plaintext "heihilter" to cipher text and from Ciphertext to plaintext using the key

110 101 110 101 111 100 000 101 110 000

And the corresponding binary representation of letter as below table :

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

(06 Marks)

c. Explain the taxonomy of cryptography. **(05 Marks)**

OR

2 a. Write a brief note on double transposition with an example. **(05 Marks)**

b. Explain the taxonomy of cryptanalysis. **(06 Marks)**

c. Write a short notes on :

i) Project VENONA

ii) Codebook cipher. **(05 Marks)**

Module-2

3 a. What is cryptographic hash function? What are the needs that cryptographic hash function must provide? **(06 Marks)**

b. With a diagram, explain Tiger hash outer round and inner round for F_m. **(06 Marks)**

c. What are the techniques used in information hiding? Explain. **(04 Marks)**

OR

4 a. With a neat diagram, explain secret sharing in detail and its types. **(08 Marks)**

b. With an example, explain HMAC function in detail. **(08 Marks)**

Module-3

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

b. Explain the idea behind the dynamic password scheme. With a neat diagram, explain the example of dynamic password scheme. **(08 Marks)**

OR

6 a. List and explain the stages and challenges of the protocol design. **(06 Marks)**

b. With a neat diagram, explain the reflection attack against protocol – 3. **(05 Marks)**

c. What are the typical AKE protocol goals? Explain. **(05 Marks)**

Module-4

7 a. What are the reasons for cryptographic key with finite lifetime? What are the measures taken for choosing a key length? Explain. **(08 Marks)**

b. With a neat diagram, explain generic unique key per transaction schemes and its types. **(08 Marks)**

OR

8 a. What are the various techniques that can be used to provide tamper resistance? Explain. **(05 Marks)**

b. With a neat diagram, explain key storage risk zones. **(06 Marks)**

c. With a neat diagram, explain identify–based public–key cryptography. **(05 Marks)**

Module-5

9 a. With a neat diagram, explain simple SSL handshake protocol description. **(05 Marks)**

b. What are the serious problem with WEP management? **(04 Marks)**

c. With a neat diagram, explain GSM authentication and encryption. **(07 Marks)**

OR

10 a. Explain the process of issuing eID card with a neat diagram. **(06 Marks)**

b. What are the challenging tasks for key management for video broadcasting? **(05 Marks)**

c. What are the potential security concern for file protection and Email? **(05 Marks)**

* * * * *