CBCS SCHEME

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

17CS743

Seventh Semester B.E. Degree Examination, July/August 2021
Information and Network Security

Time: 3 hrs. Max. Marks: 100

Note: Answer any FIVE full questions.

1 a. Encrypt the message: "Do Something Great". Using 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) **(06 Marks)**

b. Describe Simple Substitution cipher method with an example. **(06 Marks)**

c. Differentiate between:
(i) Substitution and transposition cipher
(ii) Plaintext and ciphertext
(iii) Block and stream cipher
(iv) Cryptography and cryptanalysis **(08 Marks)**

2 a. Discuss on the taxonomy of cryptography. **(06 Marks)**

b. Write short notes on:
(i) Code book cipher
(ii) Cipher of the election of 1876. **(06 Marks)**

c. Using Vernam cipher encrypt the plaintext "knowledge" to cipher text and from cipher text to plaintext using the key.

110 101 110 101 111 100 000 101 110

Letter	k	o	n	e	ℓ	w	d	g
Binary	000	001	010	011	100	101	110	111

(08 Marks)

3 a. Define cryptographic hash function. Explain the properties of hash function. **(06 Marks)**

b. Demonstrate birthday problem with an example. **(06 Marks)**

c. Explain secret sharing in detail and its types with an example. **(08 Marks)**

4 a. Discuss HMAC function in detail with an example. **(08 Marks)**

b. Explain Tiger hash outer round and inner round for 'F' with a neat diagram. **(08 Marks)**

c. Describe the techniques used in information hiding. **(04 Marks)**

5 a. Describe the basic model of a deterministic generator. **(06 Marks)**

b. Differentiate hardware and software based non-deterministic generator. **(06 Marks)**

c. Briefly describe the first candidate protocol in detail. **(08 Marks)**

6 a. Illustrate Diffie-Hellman key agreement protocol. **(08 Marks)**

b. Explain the stages of cryptographic protocol design and its challenges. **(08 Marks)**

c. Describe cryptographic password protection with an example. **(04 Marks)**

7 a. Discuss a three-level key hierarchy with a neat diagram. (06 Marks)
b. Illustrate the key life cycle with suitable diagram. (06 Marks)
c. Explain closed and connected certification model with a neat diagram. (08 Marks)

8 a. With a neat diagram, explain identity based public key cryptography. (07 Marks)
b. Describe quantum key establishment method in detail. (07 Marks)
c. Explain reputation based certification model. (06 Marks)

9 a. Explain the application of cryptography for secure payment card transactions. (08 Marks)
b. Explain the applications of cryptography in
(i) File protection
(ii) E-mail security (08 Marks)
c. Discuss the serious problem with WEP management. (04 Marks)

10 a. Describe the use of cryptography in eID cards and also explain its security and design issues. (10 Marks)
b. Explain GSM Authentication and encryption with a neat diagram. (10 Marks)

* * * * *