

CBCS SCHEME

USN

| | | | | | | | | | |
|--|--|--|--|--|--|--|--|--|--|
| | | | | | | | | | |
|--|--|--|--|--|--|--|--|--|--|

15CS743

Seventh Semester B.E. Degree Examination, Dec.2018/Jan.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. Differentiate between :
- Substitution and Transposition Cipher
 - Symmetric and Asymmetric Cipher
 - Block and stream Cipher
 - Cryptography and Cryptanalysis
 - Plaintext and Cipher text
- (10 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 the column Permutation (1, 2, 3, 4) → (2, 4, 1, 3). (06 Marks)

OR

- 2 a. Using the letter encodings in the Table the following two cipher text messages were encrypted with the one-time pad "KHHLTK" and "KTHLLE"

Table : Abbreviated Alphabet

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

Find all possible plaintext for each message and the corresponding one-time pad for the key

111 101 110 101 111 100

(08 Marks)

- b. Explain the following :
- Code book cipher
 - Ciphers of the election of 1876.
- (08 Marks)

Module-2

- 3 a. What is a Cryptographic Hash Function? Explain the properties of Hash Function. (08 Marks)
- b. Demonstrate Birthday problem with example. (08 Marks)

OR

- 4 a. Illustrate the Birthday Attack with example. (06 Marks)
- b. Explain the uses (Non Standard) for Hash Functions. (10 Marks)

Module-3

- 5 a. Illustrate Dynamic password Schemes with suitable diagram. (08 Marks)
- b. Differentiate Hardware – Based and Software based non-deterministic generators. (08 Marks)

OR

- 6 a. Explain the Diffie – Hellman key agreement protocol. (08 Marks)
- b. Explain the stages in protocol design and its challenges. (08 Marks)

Module-4

- 7 a. With suitable diagram, illustrate the key lifecycle in key management. (10 Marks)
b. Explain the key storage risk factors. (06 Marks)

OR

- 8 a. Illustrate X.509 public key certificates. (08 Marks)
b. Explain the certificate life cycle. (08 Marks)

Module-5

- 9 a. Explain briefly the application of Cryptography on the internet. (10 Marks)
b. Explain the application of cryptography for secure payment card transactions. (06 Marks)

OR

- 10 a. Describe the use of cryptography in eID cards and also explain its security and design issues. (06 Marks)
b. Explain the applications of cryptography in i) File protection ii) Email security. (10 Marks)
