Total No. of Printed Pages—3

3 SEM TDC ITN (CBCS) DSC 3

2020

(Held in April–May, 2021)

INFORMATION TECHNOLOGY

(Discipline Specific Course)

Paper : DSC–3

(Computer System Security)

Full Marks : 80
Pass Marks : 32

Time : 3 hours

The figures in the margin indicate full marks for the questions

1. Answer the following as directed : 2×5=10

(a) What is encryption?

(b) Define symmetric key.

(c) What is Trojan Horse?

(d) DES stands for _____.
(Fill in the blank)

(e) What is data confidentiality?

2. (a) What are the key principles of information security? Explain. 4

(b) Differentiate between passive attack and active attack. 2

(c) Define the following : 2×2=4

(i) Virus

(ii) Worm

3. (a) What is transposition cipher? Explain keyless and keyed transposition cipher with example. 4+4=8

Or

Discuss the design principles of block cipher technique. What are the differences between stream and block cipher? 4+4=8

(b) What is substitution cipher? Explain with an example. 5

(c) What is the difference between monoalphabetic and polyalphabetic cipher? 2

4. (a) Describe the DES structure. What is double DES and what are the disadvantages of it? 3+2+3=8 *(b)* What is brute force attack? 4

(c) Briefly explain the following (any *one*) : 5

(i) Triple DES

(ii) Differential cryptanalysis

5. *(a)* Explain RSA algorithm along with its applications. 10

Or

Using RSA algorithm, find n, d, if p 11, q 3, e 3. Encrypt 'Helloworld' message. 10

(b) What are the possible threats for RSA algorithm? 4

6. *(a)* What is message authentication? How is it different from message integrity? 2+2=4

(b) What is digital signature? How is signing and verification done in digital signature? 2+8=10

Or

What are the types of attacks addressed by message authentication? Explain. 10

★ ★ ★