

2017

M.Sc.

3rd SEMESTER EXAMINATION

COMPUTER SCIENCE

PAPER—COS—303

Full Marks : 50

Time : 2 Hours

The figures in the right-hand margin indicate full marks.

Candidates are required to give their answers in their own words as far as practicable.

Illustrate the answers wherever necessary.

(Cryptography & Network Security)

Answer any four questions. 4×10

1. (a) Explain Additive cipher and playfair cipher for data encryption. 5
- (b) Define Diffusion and Confusion. 2
- (c) Explain the round of a product cipher with diagram. 3
2. Draw and explain the general structure of DES encryption scheme. 10

(Turn Over)

3. Draw and explain general design of AES encryption cipher in cryptography. 10
4. Write data embedding and data extraction scheme of F4 algorithm. 10
5. Write data hiding and data delocking algorithm of Jsteg algorithm. What are the drawbacks of Jsteg algorithm? 8+2

[Internal Assessment — 10 Marks]
