M.Sc. 3rd Semester Examination, 2018

CRYPTOGRAPHY AND NETWORK SECURITY

PAPER – COS-303

Full Marks : 50

Time : 2 hours

Answer any **four** questions

The figures in the right hand margin indicate marks

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

Illustrate the answers wherever necessary

1. (*a*) Write the differences between cryptography and steganography. 　2

 (*b*) Differenciate between monoalphabetic and polyalphabetic cipher with example. 　4

 (*c*) Write the following plain text to cipher text using play fair cipher technique. 　4

 "VIDYASAGAR"

2. (a) Describe the heart of DES (DES function). 5

   (b) Explain different types of P-boxes. 5

3. (a) What is confusion and diffusion ? 1 + 1

   (b) What is avalanche effect and complete-
   ness ? 1 + 1

   (c) Write the key generation scheme in DES. 6

4. Write F_3 algorithm for embedding and extraction
   bits in image. 5 + 5

5. Explain PVD scheme with a numerical
   example. 5 + 5

6. Explain data hiding and data extraction using
   weighted matrix with an example. 5 + 5

[*Internal Assessment* — 10 marks]

————————