# 2016

## MCA

## 5th Semester Examination

## CRYPTOGRAPHY & STEGANOGRAPHY

**PAPER—MCA-505**

*Full Marks* : 100

*Time* : 3 Hours

*The figures in the margin indicate full marks.*

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

*Illustrate the answers wherever necessary.*

### Group-A

*( Cryptography )*

[ Full Marks : 35 ]

Answer Q. No. *1* and any *three* from the rest.

**1.** Answer following multiple choice questions : 5

(i) _____ ensures that a mess age was received by the receiver from the actual sender and not from an attacker
(a) Authentication ; (b) Authorization ;
(c) Integration ; (d) None of these.

(ii) Which of the following is a passive attack ?
(a) Masquerade ; (b) Replay ;
(c) Denial of Service ; (d) Traffic Analysis.

(iii) The multiplicative inverse of 13 in $Z_{15}$ is _____
(a) Five ; (b) Seven ; (c) Nine ; (d) Eight.

(iv) The Hill Cipher belongs to the category of ciphers, named _____
(a) Stream Cipher ; (b) Block Chipher ;
(c) Both (a) and (b) ; (d) None of these.

(v) Each round in DES uses _____ S-boxes
(a) Five ; (b) Ten ; (c) Eight ; (d) Six.

2. (a) Describe DES algorithm and explain its key structure.
(b) Define session key. Give an example. 5+5

3. (a) Explain the structure of P-Boxes.
(b) How many types of P-boxes are available ? Describe them. 5+5

4. (a) What do you mean by diffusion and confusion ? Give example.
(b) What is Feistel Cipher ? Explain. 5+5

5. Explain Advanced Encryption Standard (AES). 10

6. Explain the RSA Cryptosystem. 10

## Group-B

*( Steganography )*

[ Full Marks : 35 ]

Answer Q. No. 7 and any *three* from the rest.

**7.** Answer following multiple choice questions : 5

(i) The meaning of steaganography is _____
(a) Secret writing ; (b) Coverered writing ;
(c) Both (a) and (b) ; (d) None.

(ii) _____ is refer to the degree of difficulty required to determine hidden message.
(a) Perceptability ; (b) Steganalysis ;
(c) Robustness ; (d) Capacity.

(iii) The secret message can be modify by
(a) Passive attacker ; (b) Active attacker ;
(c) Malicious attacker ; (d) None of them.

(iv) The process of data hiding is called
(a) Hide and Seek ; (b) DCT ; (c) Encoding ; (d) Decoding.

(v) The Shrinkage can be handlled by the algorithm
(a) JSTEG ; (b) Hide and Seek ; (c) Outguess ; (d) F4.

**8.** (a) Differenciate between spatial domain and frequency domain steganography. 2

(b) Define Robustness and Perceptability. 4

(c) Describe active and malicious attacks. 4

**9.** (a) Write the algorithm of outguess 0.1 for data embedding and data extraction. 8

(b) What are the weekness of outguess 0.1. 2

**10.** Write the encoding and dicoding process of F3 algorithm. What are the weakness of F3 algorithm. 10

**11.** How F4 algorithm over come the weakness of F3 algorithm ? Write decoding and encoding F4 algorithm. 10

**12.** Write short notes on (any *two*) : 5×2

(a) PVD ;

(b) Steganalysis ;

(c) Watermarking ;

(d) Steganographics attacks.

*[ Internal Assessment : 30 ]*