2012

MCA

5th SEMESTER EXAMINATION

CRYPTOGRAPHY & STEGANOGRAPHY

PAPER—3504

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*)

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

1. Answer any *two* : $2\times2\frac{1}{2}$

(a) Distinguish between Cryptography and Steganography.

(b) Distinguish between Stream Cipher and a Block Cipher.

(c) What is the one-way function in RSA?

(d) What do you mean by Non-Repudiation?

2. (a) Define Cryptography.

(b) What are the criteria that a technique is secured? $2\times2\frac{1}{2}$

(c) What are the differences between Polyalphabetic and monoalphabetic substitution cipher. Explain with example. 5

3. (a) Encrypt the following message "VIDYASAGAR UNIVERSITY" using playfair cipher where secret key is a 5×5 matrix of alphabet starting from the top left hand corner. 5

(b) Use the Vigenere cipher with keyword "HEALTH" to encipher the message "Life is a full of surprises". 5

4. (a) What is the block size, cipher key size and round key size in DES? 3

(b) How many mixer and swappers are used for encryption and decryption algorithm in DES? 2

(c) How many permutation are used in DES algorithm? 2

(d) Why does the round key generation needed a parity drop permutation in DES? Explain. 3

5. (a) Compare DES and AES. 5

(b) List the parameters (block size, key size and the number of round) for the three AES versions. 5

6. (a) Distinguish between public and private keys in an asymmetric key cryptosystem. 4

(b) Write the RSA algorithm. 5

(c) What is digital signature? 1

Internal Assessment **15**

Group — B

(*Steganography*)

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

7. Answer any *two* : $2\times2\frac{1}{2}$

(a) Differentiate between Steganography and Watermaking.

(b) Define Malicious Steganalyst.

(c) What is blockiness ?

(d) What is PRNG (Pseudo Random Number Generator) ?

8. (a) Write an algorithm for encoding and decoding using J-steg. What are the disadvantages of this algorithm ? 3+3+1

(b) What is DCT ? 3

9. (a) Write outgess 0.1 algorithm for encoding and decoding any message. 3+3

(b) Write the weakness of F3 Algorithm. 4

10. (a) Discuss F4 algorithm of encoding a message in the cover. What is the drawback of the algorithm ? 5+2

(b) Define Chi-squared Test for statistical attacks. 3

11. (a) What do you mean by Histogram attacks ? 4

(b) Compare between Targeted and Blind steganalysis. 6

12. Write short note (any *two*) : **5+5**

(a) Hide & Seek method ;

(b) LSB method ;

(c) JPEG Compression.

Internal Assessment **15**
