http://www.makaut.com

Name : .....

Roll No. : .....

Invigilator's Signature : .....

CS/M.Tech-IT(SE)/SEM-3/MSE-303E/2009-10

2009

DATA ENCRYPTION AND COMPRESSION

Time Allotted : 3 Hours | Full Marks : 70

The figures in the margin indicate full marks.

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

Answer any *five* of the following.

1. a) What are the key principles of security ? 2

   b) i) Why are some attacks called as passive ? 2

   ii) Why are other attacks called as active ? 2

   c) i) What is worm ? 2

   ii) How it differs from virus ? 1

   iii) What is the principle of Trojan Horse ? 2

   d) Explain how cookies can be misused to invade people's privacy. 3

2. a) How does Transposition technique differ from Substitution technique ? 3

   b) Explain with example man-in-the-middle attack. 3

   c) Explain with block diagram Cipher Block Chaining (CBC) and Cipher Feed Back (CFB). 8

3. a) Compare between symmetric and asymmetric cryptographies. 3

   b) Explain how advantages of both techniques can be used. 3

   c) Describe the working of IDEA briefly. 8

4. a) How does certificate based Authentication work ? 3

   b) What do you mean by FAR and FRR ? 2

   c) Write down the advantages of IP security (IPSec). 4

   d) Describe VPN architecture. 5

5. a) Describe general communication model with block diagram. 3

   b) A message comprises just the characters *A* through *H*. Analysis has shown that the probability of each character is as follows :

      A and *B* = 0·25, *C* and *D* = 0·14, *E*, *F*, *G* and *H* = 0·055.

      i) Use Shannon's formula to derive minimum average number of bits per character. 4

      ii) Use Huffman coding to derive a code word set. 4

   c) Describe RLE with example. 3

6. a) Describe DPCM with block diagram. 4

b) How does ADPCM differ from DPCM ? 2

c) Write an algorithm to encode a stream of input symbols with a floating point output number. Apply it to encode "JISCE". 3 + 5

7. Write short notes on any *four* of the following : $4 \times 3\frac{1}{2}$

a) L-Z coding

b) SHA-1

c) DCT

d) JPEG compression

e) Frequency & Temporal Masking

f) Digital Signature

g) Key range and size.