Name : .....

Roll No. : .....

Invigilator's Signature : .....

CS/B.Tech(IT)/SEP. SUPPLE/SEM-8/IT-803A/2012

2012

DATA COMPRESSION & CRYPTOGRAPHY

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.

GROUP – A

(Multiple Choice Type Questions)

1. Choose the correct alternatives for any *ten* of the following : $10 \times 1 = 10$

i) If a computer system is not accessible, the principle of ..... is violated.

a) confidentiality b) authentication

c) availability d) access control.

ii) The ..... attack is related to integrity.

a) interception b) fabrication

c) modification d) interruption.

iii) In ..... attacks there is no modification to message contents.

a) passive b) active

c) both of these d) none of these.

iv) ..... increases the redundancy of plain text.

a) Confusion b) Diffusion

c) both of these d) none of these.

v) DES encrypts blocks of ..... bits.

a) 32 b) 56

c) 64 d) 128.

vi) ..... is based on the IDEA Algorithm.

a) S/MIME b) PGP

c) SET d) SSL.

vii) In AES, the 16 bytes key is expanded into

a) 200 bytes b) 78 bytes

c) 176 bytes d) 184 bytes.

viii) MAC is ..... message digest.

a) same as b) different from

c) subset of d) none of these.

ix) A Registration Authority (RA) ..... issue digital certificates.

a) can b) may or may not

c) has to always d) can never.

x) Lossy image simplification is based on ..... operation.

a) DCT b) CCIT

c) ISO d) DMS.

xi) Typical lossless compression for manaul image is

a) 3 : 1 b) 4 : 1

c) 2 : 1 d) 4 : 3.

GROUP – B
(Short Answer Type Questions)

Answer any *three* of the following. 3 × 5 = 15

2. Compare between lossless and lossy compression technique.
3. Determine Lempel-Ziv code for the following bit stream

   0100111110010100000101010110011000 0
4. Considering "KOLKATA" as a keyword construct a Playfair matrix and then encrypt the plain text "WEST BENGAL UNIVERSITY OF TECHNOLOGY".
5. What are the typical contents of Digital Certificate ? Discuss Key exchange protocol. 3 + 2
6. Discuss the concept of DES with basic block diagram.

GROUP – C
(Long Answer Type Questions)

Answer any *three* of the following. 3 × 15 = 45

7. a) Differentiate between Fixed Length Coding and Variable Length Coding with suitable example.

   b) Consider a source generating three symbols with following probabilities ; $P(A) = 0{\cdot}5$, $P(B) = 0{\cdot}25$ and $P(C) = 0{\cdot}25$. Find the exact number of bits required to represent the word "CAB". Use Arithmetic Encoding Method.

   c) Discuss the concept of Run Length Encoding. 4 + 6 + 5

8. a) Consider a DMS with seven possible symbols x_i, $i = 1, 2, ..., 5$ and the corresponding probabilities $p_1 = 0{\cdot}47$, $p_2 = 0{\cdot}23$, $p_3 = 0{\cdot}16$, $p_4 = 0{\cdot}11$ and $p_5 = 0{\cdot}03$. Find the self information and codeword for each symbol using Huffman Coding technique.

   b) Why is Data Compression required ? What is Compression Ratio ?

   c) Draw the flow diagram of RC5 technique.

   6 + (2 + 2) + 5

9. a) Explain Knapsack encryption technique with for the Plain Text stream 1110011000111101101 using the Knapsack wrapper

1, 7, 8, 12, 14, 20

b) Discuss different levels of Multi Factor Authentication technique.

c) Distinguish between Challenge (Response) Token and Time Based Token. 5 + 6 + 4

10. a) Explain the contrast Cipher Block Chaining (CBC) and Cipher Feedback (CFB) with the help of proper block diagram.

b) Explain Rail fence Algorithm with the text : "meet me tomorrow at my office".

c) Why is Asymmetric key cryptography advantageous over Symmetric key cryptography ?

d) Explain a Hybrid Encryption technique which utilizes both Symmetric and Asymmetric method. 5 + 2 + 3 + 5

11. Write short notes on any *three* of the following : 3 × 5

a) SHA-1

b) Prefix code

c) Denial of Service (DoS) attacks

d) Book Cipher / Vernam Cipher

e) Biometric Authentication Technique.