Seat No. : _____

DC-113

December-2013

5 Years M.Sc. (CA & IT) Integrated (K.S.) 5th Year M.Sc.

Data Compression and Encryption

Time : 3 Hours] **[Max. Marks : 100**

1. Attempt any **four** : **20**
   (a) Explain substitution cipher with example.
   (b) Explain public key encryption which provides authentication & security with diagram.
   (c) Explain RSA with example.
   (d) Give key size for Blowfish. Explain the Blowfish algorithm in detail.
   (e) Differentiate between Link Encryption & End-to-End Encryption.

2. Attempt any **four** : **20**
   (a) Draw figure for AES Encryption Round & explain in brief.
   (b) Explain with figure schemes for the Distribution of Public Keys.
   (c) Using Play Fair Cipher Encrypt the following message.
   Plain text : Attrackers are here.
   Key : Hello.
   (d) Define the following terms :
      (i) Stream cipher
      (ii) Confusion
      (iii) Crypt analysis
      (iv) Message Authentication code.
   (e) Explain Rotor machine in detail with diagram.

Data Compression

3. (A) Encode sequence "entropy entop entropy entropy" using LZW technique. **5**

   (B) Explain various rice code methods. **4**

   OR

   Explain with a diagram how vector quantization works.

   (C) Answer any **six** : **6**
      (1) What is unary code of 5 ?
      (2) Remote sensing applications will use lossy/lossless scheme.
      (3) Which are the different types of coding ?
      (4) Calculate compression ratio of an image in % when it is converted from 3 MB BMP to 1331 KB JPEG file.
      (5) In prefix code all code words are internal nodes.
      (6) Why unit interval is used in Tag generation ?
      (7) What is fidelity ?

(D) Generate Arithmetic Coding Tag for sequence "ERROR" where FX (E) = 0.39, FX (R) = 0.501, FX (0) = 1 . **5**

4. (A) Define following terms : (any **six**) **6**
   (1) Decision Boundary
   (2) Redundancy
   (3) Prefix code
   (4) Self Information
   (5) Static model
   (6) Quantization
   (7) SNR
   (8) Rate-Distortion theory

(B) Explain Algorithm for Differential Encoding Scheme. **3**

OR

Write down observations and conditions required for Huffman Procedure (Optimality for prefix code).

(C) Encode sequence "Monno nno monno mon" using LZ77 dictionary scheme with & as both buffer size. **4**

(D) A source with alphabet $\{a_1, a_2, a_3, a_4, a_5\}$ has P (a_1) = 0.125, P (a_2)= 0.25, P (a_3) = 0.025, P (a_4)= 0.37, P (a_5)= 0.23
   (1) Generate Huffman code. **4**
   (2) Calculate entropy & avg. length of source. **3**

5. (A) Give count array for -1, 0, 1 and 2 order context for sequence "Prefix fix fix" to be encoded using PPM algorithm. **4**

(B) Which probability models are used in lossy compression ? **4**

OR

Give difference between lossy & lossless compression.

(C) Answer any **four** : **8**
   (1) What is difference between midrise & midtread quantization ?
   (2) Find colomb code for n=1, 2 which is parameterized by m = 3.
   (3) Check for prefix code {10, 000, 010, 1000}
   (4) Check unique decodability {1, 00,01, 010, 011}
   (5) Find 6^{th} split sample option for 8 bit number 23.

(D) Give differences (any **two**) : **4**
   (1) LZ77 – LZW
   (2) Huffman coding – Fix length coding
   (3) Uniform – Non – Uniform quantization.

———————