QP Code : **2254**

(3 Hours) [Total Marks : 100

N.B. : (1) Question no **1** is **compulsory**
(2) Answer **any four** out of remaining
(3) Assume suitable data if necessary and justify the same.

1. Answer in brief :
    (a) Give classifications Data Compression techniques Give an example of each   5
       type.
    (b) Explain different redundancies in text, digital images and digital videos. How   5
       are they important for data compression?
    (c) Differentiate between private key crypto systems and public key cryptosystems.   5
       Give an example of each.
    (d) Solve the following congruence using Chinese Remainder Theorem (and not   5
       by trial-and-error)
       $X \equiv 1 \bmod 3$
       $X \equiv 4 \bmod 5$
       $X \equiv 5 \bmod 7$

2 (a) For the following alphabet and probasilities, find as real valued tag for arithmetic   10
       coding, for the sequence $a_1 a_1 a_3 a_2 a_3 a_1$

Letter	Probability
a_1	0.2
a_2	0.3
a_3	0.5

   (b) With a suitable example, explain LZ-77 dictionary compression technique. Also   10
   explain the worst case in LZ-77 and show how compression ratio is computed in LZ-77.

3. (a) An alphabet is given with following letters and probabilities. Perform minimum   10
    variance Huffman coding. Find the coding redundancy. Also find the compression
    ratio for the sequence $a_1 a_1 a_1 a_4 a_4 a_4 a_2 a_3$

Letters	a_1	a_2	a_3	a_4
Probabilities	0.1	0.3	0.25	0.35

[TURN OVER]

QP-Con. 11333-15.

(b) With a neat block diagram, explain the JPEG lossy compression technique.   10

4. (a) Explain DPCM and ADPCM techniques with neat block diagrams.   10
   (b) What are I-, P - and B - frames in digital videos? Explain the principle of video   10
   compression used in MPEG standard

5. (a) The prime numbers used in RSA algorithm are P=19 and g=23. If the public key e is   10
   3 find ϕ (n) and d; the decryption key where ϕ (n) has usual meaning. Write encryption
   and decryption equations.
   (b) Explain "Man-in-the-middle" attack happening in Define- Hellman key exchange   10
   system. How can it be avoided?

6 (a) Give overall block diagram of the DES standard. Explain one round in detail.   10
   (b) What are MAC and Hash functions? Give one example of each. Also explain what are   10
   the requirements on MAC and Hash functions.

7. Write short notes on any **two** :   20
   (a) MP-III encoder and decoder
   (b) JPEG- 2000 standard
   (c) Viruses and worms