

(3 Hours)

[Total Marks :80

- N.B. : (1) Question No.1 is compulsory
 (2) Solve any **three** questions from remaining **five** questions.
 (3) Assume suitable data wherever necessary with proper justification.

1. Answer the following (Any five)

- (a) What are the measures of performances for lossy and lossless compression techniques? 4
- (b) Illustrate the worst case in LZ-77 dictionary compression technique. 4
- (c) What is "frequency/auditory masking" temporal masking"? 4
- (d) Which redundancies are exploited in JPEG lossy standard? Which are the processes using these redundancies? 4
- (e) State Fermat's little theorem (FLT) and Euler's theorem. Illustrate with an example how FLT can be used to find modular inverse. 4
- (f) Using modular arithmetic and theorems, prove that decrypted text is same as plain text in the RSA algorithm. 4
- (g) What do you mean by "confusion" and "diffusion"? Which components are used in ciphers to introduce confusion and diffusion? 4

2. (a) Generate a binary tag using arithmetic coding technique for the sequence : 10
 a b a c a b b

symbol	count
a	37
b	38
c	25

- (b) Perform LZW dictionary compression on the following text string : wabba- 10
 wabba-wabba-wabba-woo-woo-woo Initial dictionary:-

Index	1	2	3	4	5
Entry	-	a	b	o	w

3. (a) Explain MP-III audio compression standard with a neat block diagram. 10
 (b) What are different approaches for compressing an image? Explain JPEG-LS standard. 10
4. (a) Explain double DES and the need for it. Also explain the "meet-in-the-middle" attack. 10
 (b) Explain any one digital signature algorithm in detail. 10

[TURN OVER

5. (a) Encrypt the plain text 63 using RSA algorithm which uses prime numbers $p = 7$ and $q = 11$. The public key $e = 13$. Verify that the deaypted text is same as the plain text. 10
- (b) Alice chooses her private key $x = 3$ and Bob chooses $y = 6$. If both of them use the primitive root $g = 7$ for prime $p = 23$, what is the key exchanged between Alice and Bob using diffie. Hellman key exchange? 10
6. Write short notes on two. 20
- (a) Adaptive Huffman coding
 - (b) H.264 encoder-decoder
 - (c) Eliptic curve cryptography
 - (d) Intrusion detection system
-

MUNDHURI (W) 6/6/2016 10:25:52 AM MUPD16448 SARDAR ENGINEERING

QP Code : 31308

(3 Hours)

[Total Marks : 80

- N.B. :** (1) Question no.1 is compulsory.
(2) Write any **three** questions from remaining **five** questions.
(3) Assume suitable data where ever necessary.

1. (a) What is the role of GPRS in enhancing 2G GSM systems. **20**
(b) Explain factors affecting small scale fading.
(c) Elaborate the concept of IMT 2000 family.
(d) Differentiate between WCDMA & CDMA 2000.
2. (a) Describe the difference between service data units & protocol data units. **10**
How is mapping from one to other is done.
(b) Explain IS-95 forward & reverse channel structure in detail. **10**
3. (a) Explain GSM architecture & elaborate function of each block. **10**
(b) Draw the block diagram of LTE transmitter & Receiver. Explain them in detail. **10**
4. (a) Consider geographical area of a cellular system is 480sqkm. A total of **10**
910 radio channels are available for traffic handling suppose, area of a cell
is 8sq km.
(1) How many times would the cluster size of 7 have to be replicated in
order to cover the entire service area? Calculate the number of channels
per cell and system capacity.
(2) If the cluster size is decreased from 7 to 4 then does it result into
increase in system capacity.
(b) Explain power control mechanism in 3G. **10**
5. (a) Compare & contrast FDMA, TDMA, SDMA, OFDM, SSMA. **10**
(b) Explain concept of MIMO w.r.t. 4G technology. **10**
6. Write notes on (**any two**) **20**
(a) EDGE architecture
(b) Call procedures in GSM
(c) Software defined radio.