

Vidyavardhini's College of Engineering & Technology, Vasai(w)
Department of Electronics & Telecommunication Engineering
Curriculum Scheme: Rev2016
Examination: TE Semester: V

Course Code: ECCDLO 5014

Time: 2 Hour

Course Name: Data Compression & Encryption

Max. Marks: 80

Q1.	Choose the correct option for following questions. All the Questions are compulsory and carry equal marks	20 Marks																		
1.	<p>From the following given tree, what is the code word for the character 'a'?</p> <div style="text-align: center;"> <pre> graph TD Root(()) --- L(()) Root --- R(()) L --- LL(()) L --- LR(()) LR --- LRL((b)) LR --- LRLR((a)) </pre> </div>																			
Option A:	011																			
Option B:	010																			
Option C:	100																			
Option D:	101																			
2.	<p>Using Huffman Code , calculate the avg. word length</p> <div style="text-align: center;"> <p>SYMBOL PROBABILITY</p> <table style="margin-left: auto; margin-right: auto;"> <tr><td>A</td><td>.36</td></tr> <tr><td>B</td><td>.15</td></tr> <tr><td>C</td><td>.13</td></tr> <tr><td>D</td><td>.11</td></tr> <tr><td>E</td><td>.09</td></tr> <tr><td>F</td><td>.07</td></tr> <tr><td>G</td><td>.05</td></tr> <tr><td>H</td><td>.03</td></tr> <tr><td>I</td><td>.01</td></tr> </table> </div>	A	.36	B	.15	C	.13	D	.11	E	.09	F	.07	G	.05	H	.03	I	.01	
A	.36																			
B	.15																			
C	.13																			
D	.11																			
E	.09																			
F	.07																			
G	.05																			
H	.03																			
I	.01																			

Option A:	2.68
Option B:	1.36
Option C:	2.77
Option D:	1.78

3. Complete the dictionary for given stream, Using LZ78 algorithm.

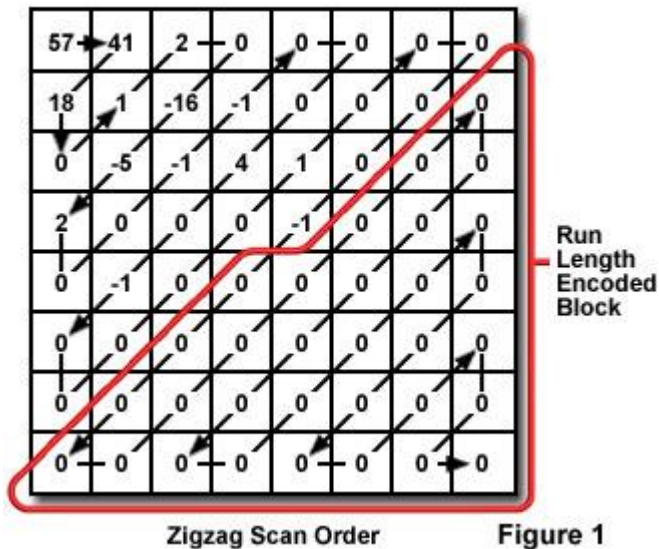
ABBCBCABABCAABCAAB

OUTPUT	DICTIONARY
(0,A)	A
(0,B)	B
(2,C)	BC
(3,A)	BCA
(2,A)	BA
(4,A)	BCAA

Option A:	(4,A)-BCAA
Option B:	(5,B)- CAAB
Option C:	(6,B)-BCAAB
Option D:	(7,A)- BCAB

4. Which is DC coefficient in the following blocks

Run Length Encoding of DCT Blocks



Option A:	-16
Option B:	18
Option C:	0
Option D:	57

5.	<p>What is predicted sequence of MPEG frames</p>
Option A:	IBPPBIPBBI
Option B:	IBBPBBPBBBI
Option C:	PBBIBBIBBP
Option D:	BPPIPPIPPB
6.	The characteristics of compressor in μ -law companding are
Option A:	Continuous in nature
Option B:	Logarithmic in nature
Option C:	Linear in nature
Option D:	Discrete in nature
7.	In cryptography, the order of the letters in a message is rearranged by _____.
Option A:	transpositional ciphers
Option B:	substitution ciphers
Option C:	both transpositional ciphers and substitution ciphers
Option D:	quadratic ciphers
8.	Use Caesar's Cipher to decipher the following HQFUBSWHG WHAW
Option A:	ABANDONED LOCK
Option B:	ENCRYPTED TEXT
Option C:	ABANDONED TEXT
Option D:	ENCRYPTED LOCK
9.	Another name for Message authentication codes is
Option A:	cryptographic codebreak
Option B:	cryptographic codesum
Option C:	cryptographic checksum
Option D:	cryptographic checkbreak
10.	A concern of authentication that deals with user rights.
Option A:	General access
Option B:	Functional authentication
Option C:	Functional authorization
Option D:	Auto verification
11.	Which of the following is not a secured mail transferring methodology?
Option A:	POP3

Option B:	SSMTP
Option C:	Mail using PGP
Option D:	S/MIME
12.	S/MIME is abbreviated as _____
Option A:	Secure/Multimedia Internet Mailing Extensions
Option B:	Secure/Multipurpose Internet Mailing Extensions
Option C:	Secure/Multimedia Internet Mail Extensions
Option D:	Secure/Multipurpose Internet Mail Extensions
13.	MP3 produces three data rates from 96 Kbps
Option A:	128 kbps
Option B:	256kbps
Option C:	320 kbps
Option D:	164kbps
14.	The second phase of JPEG is
Option A:	quantization
Option B:	DCT transformation
Option C:	data compression
Option D:	All of the above
15.	What is data encryption standard (DES)?
Option A:	block cipher
Option B:	stream cipher
Option C:	bit cipher
Option D:	byte cipher
16.	The multiplicative Inverse of 550 mod 1769 is
Option A:	434
Option B:	224
Option C:	550
Option D:	Does not exist
17.	A concern of authentication that deals with user rights.
Option A:	General access
Option B:	Functional authentication
Option C:	Functional authorization
Option D:	Auto verification
18.	Which one of the following algorithm is not used in asymmetric-key cryptography?
Option A:	RSA algorithm
Option B:	Diffie-hellman algorithm
Option C:	Electronic code book algorithm
Option D:	DSA algorithm

19.	Cryptographic hash function takes an arbitrary block of data and returns _____
Option A:	Fixed size bit string
Option B:	Variable size bit string
Option C:	Both fixed size bit string and variable size bit string
Option D:	Variable sized byte string
20.	Adaptive DPCM is used to
Option A:	Increase bandwidth
Option B:	Decrease bandwidth
Option C:	Increase SNR
Option D:	None of the mentioned
Q2	Solve any Two 20 Marks
1	What is the significance of prime number in public key cryptography? Explain RSA algorithm with suitable example?
2	Explain the working of DES, How long is the DES key?
3	A Source emits letters from alphabet $M = [m_1, m_2, m_3, m_4, m_5]$ with probabilities $P(m_1) = 0.15$, $P(m_2) = 0.05$, $P(m_3) = 0.25$, $P(m_4) = 0.05$ and $P(m_5) = 0.50$. i) Calculate entropy of this source. ii) Find Huffman code for this source. iii) Find Average length of this code. iv) Finds its redundancy.
Q.3	Solve any Four 20 Marks
1	Using LZW algorithm encode the sequence BABACABABA ?
2	Encrypt the plain Text "MEET ME" using the key 421635.name the type of ciphering used here. How does it differ from Substitution ciphering?
3	Why we use DCT in JPEG?
4	What are the various models used for data compression?
5	Explain Chinese Remainder theorem (CRT) with example?
6	Define Euler's theorem and Euler's Totient function and find $\phi(35)$?