University of Mumbai

Examination 2020 under cluster 4 (PCE)

Program: BE Electronics and Telecommunication Engineering
Curriculum Scheme: Rev2012
Examination: Final Year Semester VII
Course Code: ETE 701 DLOC 1 and Course Name: Data Compression and Encryption
Time: 1 hour Max. Marks: 50

Note to the students:- All the Questions are compulsory and carry equal marks .

Q1.	Amongst the following which one is the loslesss type of data
Option A:	Audio
Option B:	Video
Option C:	Text
Option D:	Speech
Q2.	In which technique the output of encoder is obtained in triplets
Option A:	Static dictionary
Option B:	LZ77
Option C:	LZ78
Option D:	LZW
Q3.	For a source S={ 0.4,0.2,0.2,0.1,0.1} having symbols {a,b,c,d,e}. The entropy value is
Option A:	2.56 b/s
Option B:	2.12 b/s
Option C:	2 b/s
Option D:	3.56 b/s
Q4.	The tag value on aritmetic coding is calculated as
Option A:	(l+u)/n
Option B:	(l-u)/n
Option C:	(u-l)/n
Option D:	(l+u)/(u-l)
Q5.	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
Q6.	MPEG 1 Audio layer III is designed to provide _____for stereo sound.
Option A:	120Kbit/s
Option B:	180Kbit/s
Option C:	128Kbit/s
Option D:	124Kbit/s
Q7.	Gray-level interpolation deals with the assignment of gray levels to _____ in

	the spatially transformed image.
Option A:	Pixels
Option B:	Coordinates
Option C:	Points
Option D:	Edges
Q8.	Moving Picture Experts Group (MPEG-1), was designed for a
Option A:	PC
Option B:	CD
Option C:	DVD
Option D:	Floppy
Q9.	Before audio or video signals can be sent on Internet, they need to be
Option A:	Channelised
Option B:	Managed
Option C:	Digitised
Option D:	Organised
Q10.	In Video Compression, an independent frame that is not related to any other frame is called
Option A:	B frame
Option B:	C frame
Option C:	I frame
Option D:	P frame
Q11.	Moving Picture Experts Group (MPEG-2), was designed for high-quality DVD with a data rate of
Option A:	3 to 6 Mbps
Option B:	4 to 6 Mbps
Option C:	5 to 6 Mbps
Option D:	7 to 6 Mbps
Q12.	DES follows
Option A:	Hash Algorithm
Option B:	Caesars Cipher
Option C:	Feistel Cipher Structure
Option D:	SP Networks
Q13.	AES uses a _____ bit block size and a key size of _____ bits.
Option A:	128; 128 or 256
Option B:	64; 128 or 192
Option C:	256; 128, 192, or 256
Option D:	128; 128, 192, or 256
Q14.	A(n) _____ is a keyless substitution cipher with N inputs and M outputs that uses a formula to define the relationship between the input stream and the output stream.
Option A:	T-Box

Option B:	P-Box
Option C:	K-Box
Option D:	S-Box
Q15.	Choose from among the following cipher systems, from best to the worst, with respect to ease of decryption using frequency analysis.
Option A:	Random Polyalphabetic, Plaintext, Playfair
Option B:	Random Polyalphabetic, Playfair, Vignere
Option C:	Random Polyalphabetic, Vignere, Playfair, Plaintext
Option D:	Random Polyalphabetic, Plaintext, Beaufort, Playfair
Q16.	The DES Algorithm Cipher System consists of _____rounds (iterations) each with a round key
Option A:	12
Option B:	14
Option C:	15
Option D:	16
Q17.	In the DES algorithm the Round Input is 32 bits, which is expanded to 48 bits via _____
Option A:	Scaling of the existing bits
Option B:	Duplication of the existing bits
Option C:	Addition of zeros
Option D:	Addition of ones
Q18.	In a RSA cryptosystem, a participant A uses two prime numbers p = 13 and q = 17 to generate her public and private keys. If the public key of A is 35, then what is the value of private key of A
Option A:	8
Option B:	11
Option C:	6
Option D:	3
Q19.	Suppose that two parties A and B wish to set up a common secret key (D-H key) between themselves using the Diffie Hellman key exchange technique. They agree on 7 as the modulus and 3 as the primitive root. Party A chooses 2 and party B chooses 5 as their respective secrets. Their D-H key is-
Option A:	3
Option B:	4
Option C:	5
Option D:	6
Q20.	In hash functions MD refers to
Option A:	Message digest
Option B:	Message dictionary
Option C:	Message directory
Option D:	Message delay

Q21.	gcd(36,60) is
Option A:	10
Option B:	24
Option C:	15
Option D:	12
Q22.	3 ^ (201) mod 11 = ?
Option A:	5
Option B:	3
Option C:	10
Option D:	6
Q23.	In public key cryptosystem which is kept as public
Option A:	Encryption key
Option B:	Decryption key
Option C:	Both keys
Option D:	None of the keys
Q24.	Which one is not the application of IPSec?
Option A:	Secure Remote access
Option B:	Hacking
Option C:	Secure branch office connectivity
Option D:	Secure E-Commerce
Q25.	_____ will ensure the merchant and their payment information.
Option A:	Digital certificate
Option B:	Merchant
Option C:	Certificate authority
Option D:	Dual signature

University of Mumbai

Examination 2020 under cluster 4 (PCE)

Program: BE Electronics and Telecommunication Engineering
Curriculum Scheme: Rev2012
Examination: Final Year Semester VII
Course Code: ETE 701 DLOC 1 and Course Name: Data Compression and Encryption
Time: 1 hour Max. Marks: 50

Question	Correct Option (Enter either 'A' or 'B' or 'C' or 'D')
Q1.	C
Q2.	B
Q3.	B
Q4.	A
Q5.	A
Q6.	C
Q7.	A
Q8.	B
Q9.	C
Q10.	C
Q11.	A
Q12.	C
Q13.	D
Q14.	D
Q15.	C
Q16.	D
Q17.	A
Q18.	B
Q19.	B
Q20.	A
Q21.	D
Q22.	B
Q23.	A
Q24.	A
Q25.	D