U.S.N □□□□□□□□□□

P.E.S. College of Engineering, Mandya - 571 401

(An Autonomous Institution affiliated to VTU, Belagavi)

Fifth Semester, B.E. - Electronics and Communication Engineering

Semester End Examination; Feb. - 2021

Information Theory Coding and Cryptography

Time: 3 hrs *Max. Marks: 100*

Course Outcomes

The Students will be able to:

CO1: Apply knowledge of mathematics to understand concepts of Probability, Information theory, communication channel, source codes and cryptography.

CO2: Analyze different source codes for its efficiency used with communication channels.

CO3: Design coding schemes for a given specifications and evaluate for their error correcting capability.

CO4: Discuss different lossy / lossless data compression schemes and analyze various decoding schemes for reconstruction of transmitted data.

CO5: Discuss various cryptography algorithms for secured communication.

***Note**: **I) PART - A** is compulsory. **Two** marks for each question.*

***II) PART - B**: Answer any **Two** sub questions (from a, b, c) for Maximum of **18 marks** from each unit.*

Q. No.	Questions	Marks	BLs	COs	POs
	I : PART - A	**10**			
I a.	Define mutual information and conditional entropy.	2	L1	CO1	PO1
b.	Define Hamming weight and Hamming distance.	2	L1	CO1	PO1
c.	Write a note on BCH codes.	2	L2	CO3	PO3
d.	Explain the concept of IDEA.	2	L2	CO5	PO2
e.	Define DES standard used in cryptography.	2	L2	CO5	PO2
	II : PART - B	**90**			
	UNIT - I	**18**			
1 a.	Consider a zero memory source with $S = \{S1, S_2, S_3, S_4, S_5, S_6, S_7\}$; $P = \{0.4, 0.2, 0.1, 0.1, 0.1, 0.05, 0.05\}$. Construct a binary Huffman code by placing the composite symbol as low as possible. Determine; i) Average length ii) Entropy iii) Code efficiency	9	L3	CO2	PO2
b.	Given the source alphabet $S = \{A, B, C, D\}$ with $P(A) = 0.5$, $P(B) = 0.25$, $P(C) = 0.15$ and $P(D) = 0.10$. Construct the arithmetic code for the input symbol sequence *ABCD*.	9	L3	CO2	PO2
c.	Explain JPEG standard for lossy and lossless compression.	9	L3	CO1	PO1
	UNIT - II	**18**			
2 a.	Apply Shannon limit to analyze different channel and its capacity.	9	L3	CO1	PO1
b.	For (6, 3) linear block code given parity check matrix; $H = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$ Find its generator matrix, d_{min} and all possible code vectors.	9	L3	CO3	PO3
c.	Explain the construction of LDPC code.	9	L3	CO3	PO3

Contd....2

	UNIT - III	**18**			
3 a.	Let the polynomial *g(x)* = $x^3 + x + 1$ be the generator polynomial for a systematic (7, 4) cyclic code, i) Find the generator polynomial *G* ii) Find the parity check matrix *H* iii) How many errors can this code correct?	9	L3	CO3	PO3
b.	Define cyclic codes and explain how cyclic codes are generated from the generating polynomial.	9	L2	CO3	PO3
c.	Explain the following: i) Reed Solomon code ii) BCH code	9	L2	CO2	PO2
	UNIT - IV	**18**			
4 a.	Define the following: i) Block cipher ii) Stream cipher iii) Key iv) Public key algorithm	9	L2	CO5	PO2
b.	Explain briefly RSA algorithm with an example.	9	L3	CO5	PO2
c.	Discuss about International Data Encryption algorithm.	9	L3	CO5	PO2
	UNIT - V	**18**			
5 a.	Explain in detail the design principles of block cipher.	9	L2	CO5	PO2
b.	What is differential and linear cryptanalysis? List the differences between the same.	9	L2	CO5	PO2
c.	Write a note on; i) Finite field arithmetic ii) AES transformation functions	9	L2	CO5	PO2

* * *