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; February / March - 2023
Information Theory Coding and Cryptography

Time: 3 hrs   *Max. Marks: 100*

Course Outcome

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.

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

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

Q. No.	Questions	Marks	BLs	COs	POs
	I : PART - A	**10**			
1 a.	Define Joint entropy.	2	L1	CO1	PO1
b.	Define Critical rate.	2	L1	CO1	PO1
c.	Mention the typical applications of Reed-Solomon code.	2	L1	CO1	PO1
d.	Define Plain text and Encryption.	2	L1	CO1	PO1
e.	Define Cipher text and Secret key.	2	L1	CO1	PO1
	II : PART - B	**90**			
	UNIT - I	**18**			
2 a.	Consider a source S giving out symbols S1, S2, S3 with probabilities of ½, ¼ and ¼ respectively; i) Find the entropy of the source ii) Write all the symbols of the 2nd extension of S and find its entropy iii) Hence find relation between $H(S^2)$ and $H(S)$	9	L4	CO3	PO3
b.	Consider the source alphabets with p(e) = 0.3, p(n) = 0.3, p(t) = 0.2 p(w) = 0.1, p(.) = 0.1. Construct the arithmetic code for the input symbol sequence *went*.	9	L4	CO3	PO3
c.	Discus the JPEG standard for lossless compression.	9	L4	CO4	PO2
	UNIT - II	**18**			
3 a.	With the mathematical equation, discuss and explain noisy channel coding theorem.	9	L3	CO1	PO1

b. Consider(6, 3) linear block whose parity matrix is,

$$P = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

9	L4	CO2	PO2

i) Construct Generator and Parity check matrix

ii) Find all Code vectors

iii) Compute Error detecting and Correcting capability of the code

c. For a systematic linear block code, the three parity check digits, C4, C5, and C6 are given by,

C4 = d1⊕d2⊕d3   C5 = d1⊕d2   C6 = d1⊕d3

i) Construct generator matrix

ii) Prepare the suitable decoding table

iii) Decode the received words 101100 and 000110

9	L4	CO2	PO2

UNIT - III   **18**

4 a. Write a short note on the following:

i) Quasi Cyclic code

ii) Shortened Cyclic codes

iii) Fire codes

9	L1	CO1	PO1

b. Generator polynomial of a (7, 4) cyclic code $g(x) = x^3 + x + 1$. Find all the code vectors for the code in non systematic form.

9	L2	CO4	PO3

c. Explain the process of decoding BCH code with an example.

9	L2	CO2	PO2

UNIT - IV   **18**

5 a. With the help of neat figure, discuss the process of encryption and decryption. And also explain the operations used by encryption algorithms.

9	L3	CO5	PO2

b. Discuss International Data Encryption Algorithm (IDEA).

9	L3	CO5	PO2

c. Discuss Asymmetric (Public-Key) algorithms.

9	L3	CO5	PO2

UNIT - V   **18**

6 a. Discuss the block Cipher principles.

9	L3	CO5	PO2

b. With a neat flow diagram, discuss general depiction of DES encryption algorithm.

9	L3	CO5	PO2

c. Discuss AES encryption process.

9	L3	CO5	PO2

✳ ✳ ✳