Module 1: Basics of Information Theory (6 Hrs)

(6 hrs → around 5–6 MCQs.)

1.
The unit of information is:
a) Bit
b) Byte
c) Nibble
d) Word

Answer: a) Bit

2.
If the probability of an event is $\frac{1}{4}$, what is the information content (in bits)?

a) 2

b) 4

c) 1

d) 0.5

Answer: a) 2
Reason: Information = $-\log_2(P)$ = $-\log_2(1/4) = 2$

3.
The entropy H(X)H(X)H(X) of a random variable XXX is maximum when:
a) All outcomes are equally likely
b) One outcome is certain
c) Probabilities are different
d) None of these

Answer: a) All outcomes are equally likely

4.
Mutual Information I(X;Y)I(X;Y)I(X;Y) is zero if and only if:
a) XXX and YYY are dependent
b) XXX and YYY are independent
c) Entropy is zero
d) Information rate is zero

Answer: b) XXX and YYY are independent

5.
Which channel model assumes no memory and independent errors?
a) AWGN channel
b) Binary Symmetric Channel
c) Fading Channel
d) Erasure Channel

Answer: b) Binary Symmetric Channel

6.
Channel capacity is defined as:
a) Minimum achievable data rate
b) Maximum achievable data rate
c) Average achievable data rate
d) Zero achievable data rate

Answer: b) Maximum achievable data rate

Set 1

Match the following:

Left Side	Right Side
Entropy	Average information per symbol

Information Rate	Information per second
Mutual Information	Shared information between two variables

Answer Set 1:

- Entropy → Average information per symbol (Definition)
- Information Rate → Information per second (Rate = bits/sec)
- Mutual Information → Shared information between two variables (Common part)

Set 2

Match the following:

Left Side	Right Side
Joint Entropy	Entropy of combined variables
Conditional Entropy	Uncertainty of one variable given another
Shannon's Theorem	Limit for reliable communication

Answer Set 2:

- Joint Entropy → Entropy of combined variables (H(X, Y))
- Conditional Entropy → Uncertainty of one variable given another (H(Y|X))
- Shannon's Theorem → Limit for reliable communication (Defines channel capacity)

Set 3

Match the following:

Left Side	Right Side
Noiseless Channel	No error
Channel Capacity	Maximum possible data rate
Channel Model	Represents channel behavior

Answer Set 3:

- Noiseless Channel → No error (Ideal case)
- Channel Capacity → Maximum possible data rate (Upper bound)
- Channel Model → Represents channel behavior (Includes noise, distortion, etc.)

Module 2: Data Compression (14 Hrs)

1.
Which of the following is a variable-length, prefix-free code?
a) Shannon-Fano code
b) Huffman code
c) Arithmetic code
d) Both a and b

Answer: d) Both a and b

2.
In Huffman coding, the two symbols combined at each step have:
a) Highest probabilities
b) Lowest probabilities
c) Equal probabilities
d) Random probabilities

Answer: b) Lowest probabilities

3.
The source coding theorem states that the average codeword length is:
a) Equal to entropy
b) Always greater than entropy
c) Always less than entropy
d) Close to entropy but not less

Answer: d) Close to entropy but not less

4.
Which coding technique achieves compression by grouping similar adjacent pixel values?
a) Run Length Encoding (RLE)
b) Huffman Coding

c) Arithmetic Coding
d) LZW Coding

Answer: a) Run Length Encoding (RLE)

5.
In arithmetic coding, a message is represented as:
a) A binary tree
b) A sequence of fixed codes
c) A fractional interval
d) A vector of codewords

Answer: c) A fractional interval

6.
LZW coding is best suited for:
a) Random data
b) Highly redundant data
c) Encrypted data
d) Compressed data

Answer: b) Highly redundant data

7.
Which of the following is NOT a type of Quantization?
a) Scalar Quantization
b) Vector Quantization
c) Differential Quantization
d) Arithmetic Quantization

Answer: d) Arithmetic Quantization

8.
Transform coding is based on the idea of:
a) Encoding frequently occurring patterns
b) Reducing signal energy

c) Representing signals in another domain
d) Replicating the signal

Answer: c) Representing signals in another domain

9.
Which transform is most commonly used in JPEG image compression?
a) Fourier Transform
b) Hadamard Transform
c) Discrete Cosine Transform
d) Wavelet Transform

Answer: c) Discrete Cosine Transform

10.
Sub-band coding divides a signal into:
a) Time intervals
b) Frequency bands
c) Amplitude levels
d) Signal energy parts

Answer: b) Frequency bands

11.
Which compression method is generally used for audio signals?
a) Run Length Encoding
b) Huffman Coding
c) Sub-band coding
d) Arithmetic Coding

Answer: c) Sub-band coding

12.
Video compression primarily exploits:
a) Frequency redundancy
b) Spatial and temporal redundancy

c) Signal distortion
d) Quantization error

Answer: b) Spatial and temporal redundancy

Set 1

Match the following:

Left Side	Right Side
Shannon-Fano Coding	Based on symbol probability
Huffman Coding	Optimal prefix code
Arithmetic Coding	Represents entire message as one number

Answer Set 1:

- Shannon-Fano Coding → Based on symbol probability (Builds tree based on probability)
- Huffman Coding → Optimal prefix code (Greedy algorithm)
- Arithmetic Coding → Represents entire message as one number (Interval coding)

Set 2

Match the following:

Left Side	Right Side

Run Length Encoding	Good for repetitive data
Scalar Quantization	Single value mapping
Sub-band Coding	Divides signal into frequency bands

Answer Set 2:

- Run Length Encoding → Good for repetitive data (e.g., images, black/white areas)
- Scalar Quantization → Single value mapping (One symbol quantization)
- Sub-band Coding → Divides signal into frequency bands (Compression technique)

Set 3

Match the following:

Left Side	Right Side
Differential Coding	Stores difference between values
Vector Quantization	Group-based quantization
Transform Coding	Converts signal to another domain

Answer Set 3:

- Differential Coding → Stores difference between values (Delta coding)

- Vector Quantization → Group-based quantization (Block coding)
- Transform Coding → Converts signal to another domain (e.g., DCT)

Set 4

Match the following:

Left Side	Right Side
Audio Coding	Compression based on human hearing
Video Compression	Exploits spatial and temporal redundancy

Answer Set 4:

- Audio Coding → Compression based on human hearing (e.g., MP3)
- Video Compression → Exploits spatial and temporal redundancy (e.g., MPEG)

Module 3: Linear Block Codes (6 Hrs)

1.
Error control coding is needed primarily to:
a) Increase transmission speed
b) Reduce bandwidth
c) Detect and correct errors
d) Encrypt the data

Answer: c) Detect and correct errors

2.
In linear block codes, the set of valid codewords forms a:
a) Vector space
b) Matrix space
c) Affine space
d) Random set

Answer: a) Vector space

3.
Which of the following matrices is used for detecting errors?
a) Generator matrix
b) Parity check matrix
c) Syndrome matrix
d) Transformation matrix

Answer: b) Parity check matrix

4.

The syndrome vector in error detection is computed as:

a) $S = H \times C^T$

b) $S = H \times R^T$

c) $S = G \times C^T$

d) $S = G \times R^T$

Answer: b) $S = H \times R^T$

Reason: H = parity matrix, R = received word.

5.

A linear block code with minimum distance d_{min} can detect up to:

a) d_{min} errors

b) $d_{min} - 1$ errors

c) $d_{min}/2$ errors

d) $d_{min} + 1$ errors

Answer: b) $d_{min} - 1$ errors

6.

If a code can correct up to ttt errors, then its minimum distance must be at least:

a) 2t2t2t

b) 2t+12t + 12t+1

c) ttt

d) t+1t + 1t+1

Answer: b) 2t+12t + 12t+1

Set 1

Match the following:

Left Side	Right Side
Single-bit Error	Only one bit flipped
Burst Error	Multiple consecutive bits flipped
Parity Bit	Simple error detection

Answer Set 1:

- Single-bit Error → Only one bit flipped (Common error)
- Burst Error → Multiple consecutive bits flipped (Typical in noisy channels)
- Parity Bit → Simple error detection (Even/odd parity)

Set 2

Match the following:

Left Side	Right Side

Linear Block Codes	Satisfy linearity property
Generator Matrix	Used to encode data
Parity Check Matrix	Used to detect errors

Answer Set 2:

- Linear Block Codes → Satisfy linearity property (Addition of codewords = codeword)
- Generator Matrix → Used to encode data (G matrix)
- Parity Check Matrix → Used to detect errors (H matrix)

Set 3

Match the following:

Left Side	**Right Side**
Syndrome Decoding	Uses parity check matrix

Error Syndrome	Non-zero when error exists
Minimum Distance	Minimum number of differing bits

Answer Set 3:

- Syndrome Decoding → Uses parity check matrix (Checks for errors)
- Error Syndrome → Non-zero when error exists (If syndrome = 0 → No error)
- Minimum Distance → Minimum number of differing bits (Important for error correction)

Module 4: Cyclic Code and Convolution Code (9 Hrs)

1.
Cyclic codes are a subset of:
a) Linear block codes
b) Convolution codes
c) Source codes
d) Prefix codes

Answer: a) Linear block codes

2.
The generator polynomial g(x)g(x)g(x) of a cyclic code must:
a) Divide xn−1x^n - 1xn−1 exactly
b) Be irreducible
c) Have degree 1
d) Always be primitive

Answer: a) Divide xn−1x^n - 1xn−1 exactly

3.
In cyclic redundancy check (CRC), the remainder obtained is known as:
a) Syndrome
b) Parity
c) Check bits
d) Redundancy bits

Answer: a) Syndrome

4.
The primary advantage of cyclic codes is:
a) Ease of encoding and decoding
b) Less hardware required
c) No need for error detection
d) Low memory usage

Answer: a) Ease of encoding and decoding

5.
BCH codes are a type of:
a) Block codes
b) Convolutional codes
c) Cyclic codes
d) Source codes

Answer: c) Cyclic codes

6.
Convolutional codes process:
a) Blocks of data at a time
b) Continuous data streams
c) Only error-free data
d) Random blocks

Answer: b) Continuous data streams

7.
In convolutional encoding, the constraint length refers to:
a) Length of input sequence
b) Memory of the encoder
c) Number of parity bits
d) Decoding delay

Answer: b) Memory of the encoder

8.
Which decoding technique is commonly used for convolutional codes?
a) Hamming decoding
b) Viterbi algorithm
c) Syndrome decoding
d) Turbo decoding

Answer: b) Viterbi algorithm

9.
Tree and trellis diagrams are used in convolutional coding mainly for:
a) Compression
b) Encryption
c) Error detection
d) Decoding paths

Answer: d) Decoding paths

Set 1

Match the following:

Left Side	Right Side
Cyclic Codes	Codewords are cyclic shifts
BCH Codes	Correct multiple errors

Generator Polynomial	Used to generate cyclic codes

Answer Set 1:

- Cyclic Codes → Codewords are cyclic shifts (Circular property)
- BCH Codes → Correct multiple errors (Designed for powerful correction)
- Generator Polynomial → Used to generate cyclic codes (G(x) defines the code)

Set 2

Match the following:

Left Side	**Right Side**
Syndrome Computation	Used for error detection in cyclic codes
Convolutional Encoder	Uses shift registers
Trellis Diagram	Visual representation of code sequences

Answer Set 2:

- Syndrome Computation → Used for error detection in cyclic codes (Calculates remainder)
- Convolutional Encoder → Uses shift registers (Sequential encoding)
- Trellis Diagram → Visual representation of code sequences (Paths and states)

Set 3

Match the following:

Left Side	Right Side
Convolution Codes	Encodes with memory
Tree Diagram	Shows all possible code paths
Viterbi Algorithm	Optimal decoding for convolution codes

Answer Set 3:

- Convolution Codes → Encodes with memory (Depends on previous bits)
- Tree Diagram → Shows all possible code paths (Branching structure)

- Viterbi Algorithm → Optimal decoding for convolution codes (Dynamic programming approach)

Module 5: Basics of Number Theory and Cryptography (10 Hrs)

1.
A prime number is a number that:
a) Has exactly two distinct positive divisors
b) Has only one divisor
c) Is divisible by all numbers
d) Has no divisors

Answer: a) Has exactly two distinct positive divisors

2.
Random number generation is important in cryptography for:
a) Faster encryption
b) Reducing errors
c) Increasing security
d) Data compression

Answer: c) Increasing security

3.
The solution to ax+by=dax + by = dax+by=d exists if and only if:
a) ddd divides aaa
b) ddd divides bbb
c) ddd divides gcd(a,b)gcd(a, b)gcd(a,b)
d) aaa and bbb are coprime

Answer: c) ddd divides gcd(a,b)gcd(a, b)gcd(a,b)

4.
The Chinese Remainder Theorem is applicable when moduli are:
a) Coprime
b) Equal
c) Prime numbers only
d) Divisible by each other

Answer: a) Coprime

5.
Which of the following statements is TRUE according to Fermat's Little Theorem?
a) $a^p \equiv 1 \pmod{p}$ for any prime p and integer a
b) $p^a \equiv 1 \pmod{a}$
c) $a^p \equiv p \pmod{a}$
d) $p^a \equiv a \pmod{p}$

Answer: a) $a^p \equiv 1 \pmod{p}$

6.
Euler's Theorem is a generalization of:
a) Fermat's Little Theorem
b) Chinese Remainder Theorem
c) Modular Inverse Theorem
d) Lagrange's Theorem

Answer: a) Fermat's Little Theorem

7.
According to Shannon, a good cipher should exhibit:
a) High confusion and low diffusion
b) High diffusion and low confusion
c) High confusion and high diffusion
d) Low confusion and low diffusion

Answer: c) High confusion and high diffusion

8.
Which cipher rearranges the order of characters without changing them?
a) Substitution cipher
b) Transposition cipher
c) Affine cipher
d) Vigenere cipher

Answer: b) Transposition cipher

9.
The Caesar cipher is an example of:
a) Substitution cipher
b) Transposition cipher
c) Block cipher
d) Stream cipher

Answer: a) Substitution cipher

10.
The Affine cipher uses which two mathematical operations?
a) Addition and Division
b) Multiplication and Division
c) Multiplication and Addition
d) Addition and Subtraction

Answer: c) Multiplication and Addition

11.
In the Vigenère cipher, the keyword is:
a) Numeric
b) Alphabetic
c) Alphanumeric
d) Random

Answer: b) Alphabetic

Set 1

Match the following:

Left Side	Right Side
Prime Number Generation	Fundamental for cryptography
Random Number Generation	Needed for keys and nonces
Linear Congruences	Equations in modular arithmetic

Answer Set 1:

- Prime Number Generation → Fundamental for cryptography (Used in RSA, etc.)
- Random Number Generation → Needed for keys and nonces (Secure randomness)
- Linear Congruences → Equations in modular arithmetic (e.g., $ax \equiv b \mod n$)

Set 2

Match the following:

Left Side	Right Side
Chinese Remainder Theorem	Solves multiple congruences simultaneously
Fermat's Little Theorem	Basis for primality testing
Euler's Theorem	Generalizes Fermat's Little Theorem

Answer Set 2:

- Chinese Remainder Theorem → Solves multiple congruences simultaneously (CRT technique)
- Fermat's Little Theorem → Basis for primality testing (If p is prime, then a^(p-1) ≡ 1 mod p)
- Euler's Theorem → Generalizes Fermat's Little Theorem (Uses Euler's totient function)

Set 3

Match the following:

Left Side	Right Side
Encryption	Converting plaintext to ciphertext
Decryption	Recovering original message
Confusion and Diffusion	Concepts for strong cipher design

Answer Set 3:

- Encryption → Converting plaintext to ciphertext (Scrambling information)
- Decryption → Recovering original message (Reverse process)
- Confusion and Diffusion → Concepts for strong cipher design (Confusion hides relation to key, diffusion spreads plaintext influence)

Set 4

Match the following:

Left Side	Right Side
Caesar Cipher	Simple additive cipher
Affine Cipher	Uses both multiplication and addition
Vigenère Cipher	Polyalphabetic cipher

Answer Set 4:

- Caesar Cipher → Simple additive cipher (Shift letters)
- Affine Cipher → Uses both multiplication and addition (ax + b mod 26)
- Vigenère Cipher → Polyalphabetic cipher (Keyword-based shifting)