AMIT SOLANKI

BRANCH - ITESM / 4th SEM

BTE ROLL NO. - 1812111006

BTE Roll no - 18121111006

Page No.
Date

NTM assignment-2

Q1. What is data encipherment?

Ans. Encipherment →
The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.

- Encipherment is the process of translating Plaintext into ciphertext.
The cryptographic transformation of data to produce ciphertext.

OR

"Encipherment is the process of making data unreadable to unauthorized entities by applying a cryptographic algorithm (an encryption algorithm).
Decipherment (decryption) is the reverse operation by which the ciphertext is transformed to the Plaintext.

Data Encipherment :-
It means that the key in the certificate is used to encrypt application data. That is This is not used in TLS.

- It is used when the public key is used for encrypting user data other than cryptographic keys.

Q2. Explain arithmetic coding with example?

Ans. Arithmetic coding is a form of entropy encoding used in lossless data compression.

BTE Roll no. - 1812...

Page No.
Date

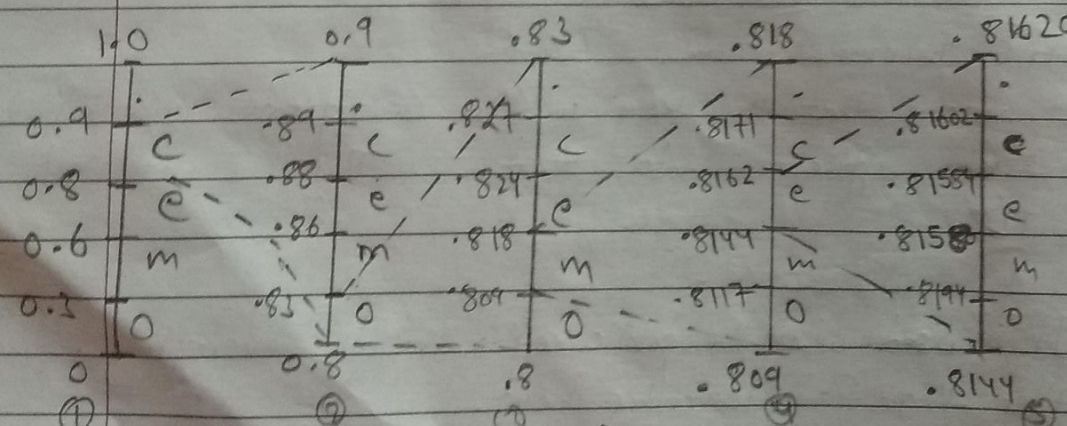
- It is useful when dealing with sources with small alphabet such binary sources.
- Generating variable length code.

- Arithmetic coding is a data compression technique that encodes data (the data string) by creating a code symbol which represents a fractional value on the number line between 0 and 1.
The coding algorithm is symbolwise recursive; i.e., it operates upon and encodes (decodes) one data symbol per iteration or recursion.

- It is used in PPM, JPEG / MPEG (as option), Bzip.

- More time costly than Huffman coding, but integer implementation is not too bad.

Example ● = 0.3 , m = 0.3 , e = 0.2 , C = 0.1 , • = 1



LL (lower limit) + d (difference) • (Probability)

① ⇒ 0.8 + 0.1(0.3) = .8 + .03 = .83

0.83 + 0.1 (0.3) = .83 + .03 = .86

.86 + 0.1(0.2) = .86 + .02 = .88

.88 + 0.1(0.1) = .88 + .01 = .89

Page No.
Date

Same step for 2, 3, 4 & 5.

.81602 < Codeword Range < .81620

$$\text{Tag} = \frac{.81602 + .81620}{2} = \frac{1.63222}{2} = 0.81611$$

Q3. Explain Ziv-lemple coding with example?

Ans. lempel-Ziv is a Universal lossless data compression algorithm Published by lemple & Ziv in 1978.

★ **Definition :-**

- It is a very common compression technique.
- It is basic of many PC utilities that claims to "double the capacity of your harddrive".
- It is lossless data. No data is loss.
- It Performs coding of Group of character of varying length.

★ **Uses:**

It is used in unix file compression, GIF, Pdf, TIFF

★ **How does it work?**

lemple Ziv coding works by reading a sequence of symbols.

↓

Grouping the symbol into string.

↓

Converting the string into codes

↓

Then finally we get a compression or compressed data.

ABBABBB → string

↓

code

BTE Roll no - 18121110006

Page No.
Date

★ Algorithm :-

Step1 → Source Sequence is sequencially passed into strings that have not appeared so far.

Step2 → After every seperation, look input sequence until new found shortest string which is not marked before.

Step3 → code this phase by giving the location of the Prefix value of last bit. to code. we have to assume A → "0", B → "1" and put this Binary number of Prefix.

Step4 → Getting the final compressed output.

Example.

BAABABBBAABBB

B	A	AB	ABB	BA	ABBB
1	2	3	4	5	6

B	A	2B	3B	1A	4B

100 → convert Binary

1	0	101	111	010	1001

o/p

Assume
A → "0"
B → "1"