COMPUTER ENGINEERING DEPARTMENT

SUBJECT: MULTIMEDIA SYSTEM

COURSE: T.E.	Year: 2020-2021	Semester: V

DEPT: Computer Engineering

SUBJECT CODE: CSDLO5011 EXAMINATION DATE: 16/01/2021

==

MULTIMEDIA SYSTEM ANSWER SHEET

Name :	AMEY MAHENDRA THAKUR
Seat No.:	51112146
Exam :	SEMESTER V
Subject :	MULTIMEDIA SYSTEM
Date :	16/01/2021
Day :	SATURDAY

Student Signature: Amey

Name: AMEY MAHENDRA THAKUR **Branch:** COMPUTER **Seat No.:** 51112146

Subject: MULTIMEDIA SYSTEM **Exam:** SEMESTER V

Q.3 A]

- A network company uses a compression technique to encode the message before transmitting over the network
- Suppose the message contains the following character with their frequency

A	B	C	D	E	F
7	16	19	45	13	6

Sol^n:

Total no.. of characters = 106

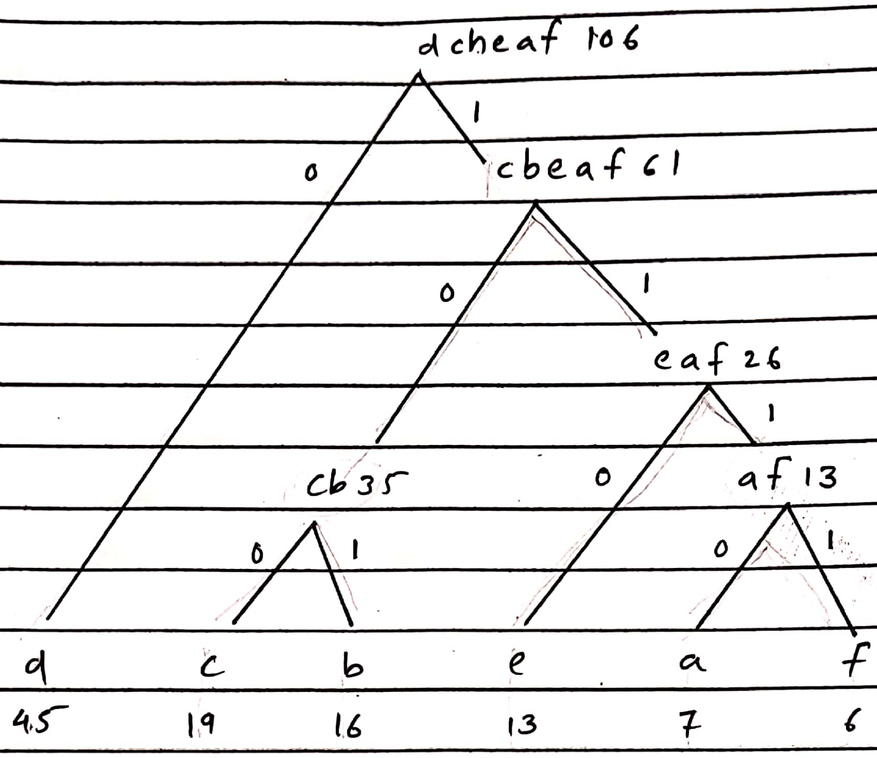
Each character takes 1 byte or 8 bits

so the no. of bits will be 848 bits

Compression Technique is Huffman coding.

16-01-2021

Student Signature: Amey



Characters	Code Word	Length of Code word
d	0	1
c	100	3
b	101	3
e	110	3
a	1110	4
f	1111	4
		18

Avg length $= \frac{18}{8} = 3$ bits. This is the average length of code word

166 × 3 = 318 bits

Normal compression technique will take 848 bits

Huffman Coding Technique = 318 bits

848 - 318 bits = 530 bits.

∴ If the compression technique used is huffman coding,
The no of bits saved will be 530 bits

Q.3. B]

Shannon - Fano Compression Algorithm

1) Examine all elements of the text to be compressed and counts their frequency in the source.

2) It then sorts the actual symbols contain in the source by descending frequency so that most common element will be at the left and the least common at right.

3) It then segments the list into 2 sections such that the sum of the number of ocerrance of elements to the left is as closed to the sum of the occurrances of elements to the right.

4) A zero is then assigned to left section and One to the right and algorithm recursively countinuous splitting and assigning a value until no further split is possible

5) In this way each input element will be assigned a sequence of 0/1 value and thus a binary encoding

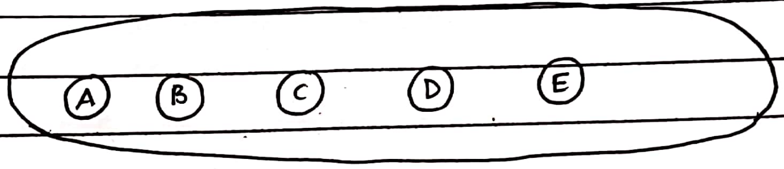
6) The source data is then compressed by replacing each element of the source with its binary encoding

7) In the generator the user can specify a string to the encoded, the default string to be encoded is Shannon-Fanon

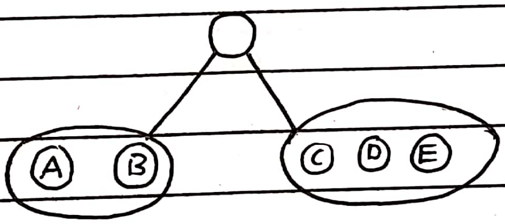
Symbol	A	B	C	D	E
Frequency (F)	12	8	7	6	5
Probability	12/38 =0.315789	8/38 = 0.210526	7/38 =0.184210	6/38 0.157895	5/38 0.131578

$\Sigma F = 12+8+7+6+5 = 38$

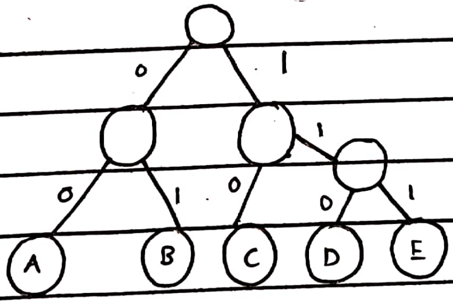
a.



b



c



A'	00
B	01
C	10
D	110
E	111

∴ These are the code for each symbols

Q.3. C] Steganographic Methods

Steganography

- Steganography is a technique of hiding communication by concealing the secret message into a fake message.
- The word steganography has greek influenence which means 'covered writing'
- The main idea behind the steganography is to prevent suspicion about the existence of the information.

⇒ Pure Seganography does not require the exchange of a cipher such as a stego key. It assumes that no other party is aware of the communication

⇒ Secret Key seganography where the secret (stego) key is exchanged prior to communication. This is most susceptible to interception. Secret key steganography takes a cover message and embeds the secret message inside of it by using a secret key (stego-key). Only the parties who know the secret key can reverse the process and read the secret message.

⇒ Public key Steganography where a public key and a private key is used for secure communication. The sender will use the public key during the encoding process and only the private key which has a direct mathematical relationship with the public key can decipher the secret message.

Student Signature: Amey

16-01-2021

Steganography Methods

Steganography Methods :

Techniques used in steganography are -
① Least Significant Bit
② Palette Based Technique
③ Secure Cover Selection

① Least Significant Bit
- In this steganography method, the attacker identifies the least significant bits of information in the carrier image and substitutes it with their secret message, in this case, malicious code.
When the target downloads the carrier file, they introduce the malware into their computer which allows the attacker access to this device and the hack begins.
Cybersecurity professionals commonly use sandboxes to detect these corrupt files.
However, black hat hackers have invented various methods of bypassing sandboxes like sleep patching.
Sleep patched malware is not easily detected by the sandbox since it poses as begins and Buys time while studying the timing artifacts of the sandbox and executes when the sandbox is vulnerable.

16-01-2021 **Student Signature:** Amey

Name: AMEY MAHENDRA THAKUR **Branch:** COMPUTER **Seat No.:** 51112146

Subject: MULTIMEDIA SYSTEM **Exam:** SEMESTER V **Page No.:** 8 / 8

② Palette Based Technique.

- The technique also uses digital images as malware carriers. Here, the attackers first encrypt the message and then hide it in a stretched palette of the cover image.
  Even though this technique can carry a limited amount of data, it frustrates threat hunters since the malware is encrypted and takes a lot of time to decrypt.

③ Secure Cover Selection

- This is a very complex technique where the cyber criminals compare the blocks of the carrier image to the blocks of their specific malware.
  If an image with the same blocks as the malware is found, it is chosen as the candidate to carry thee malware.
  The identical malware blocks are then carefully fitted into the carrier image.
  The resulting image is identical to the original and the worst part is that this image is not flagged as a threat by detection software and applications.

16-01-2021 **Student Signature:** Amey