Unit-V

PRESENTATION LAYER

The **primary goal** of this layer is to take care of the syntax and semantics of the information exchanged between two communicating systems.

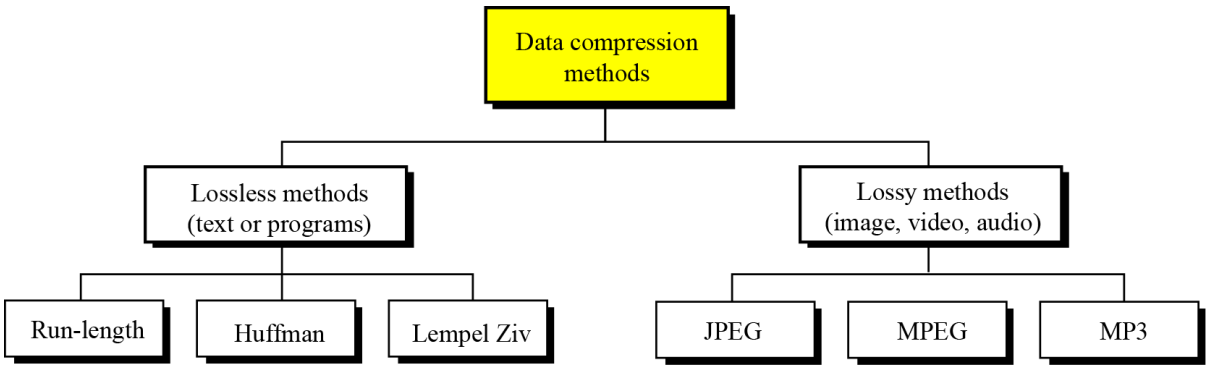
Languages(syntax) can be different of the two communicating systems. Under this condition presentation layer plays a role translator.

Functions of Presentation Layer:

1. **Translation:** Before being transmitted, information in the form of characters and numbers should be changed to bit streams. The presentation layer is responsible for interoperability between encoding methods as different computers use different encoding methods. It translates data between the formats the network requires and the format the computer.
2. **Encryption/Decryption:** It carries out encryption at the transmitter and decryption at the receiver. Encryption and decryption help protect the confidentiality of the data stored on computer systems or wired over the internet or other computer networks. Nowadays, modern-day encryption/decryption can provide not only confidentiality but also, authentication and integrity.
3. **Compression:** It carries out data compression to reduce the bandwidth of the data to be transmitted. The primary role of Data compression is to reduce the number of bits to be transmitted. It is important in transmitting multimedia such as audio, video, text etc. Compression is often used to maximize the use of bandwidth across a network or to optimize disk space when saving data.

DATA COMPRESSION

Data compression implies sending or storing a smaller number of bits. Although many methods are used for this purpose, in general these methods can be divided into two broad categories: **lossless** and **lossy** methods



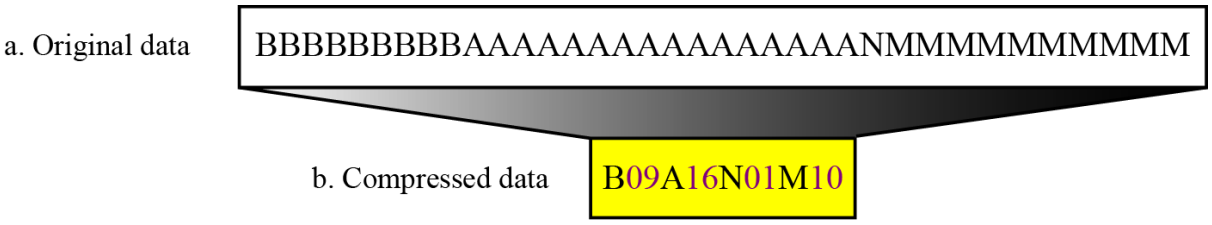
Lossless Compression:

In **lossless** data compression, the integrity of the data is preserved. The original data and the data after compression and decompression are exactly the same because, in these methods, the compression and decompression algorithms are exact inverses of each other: no part of the data is lost in the process. Redundant data is removed in compression and added during decompression. Lossless compression methods are normally used when we cannot afford to lose any data.

1. Run-length encoding

Run-length encoding is probably the simplest method of compression. It can be used to compress data made of any combination of symbols. It does not need to know the frequency of occurrence of symbols and can be very efficient if data is represented as 0s and 1s.

The general idea behind this method is to replace consecutive repeating occurrences of a symbol by one occurrence of the symbol followed by the number of occurrences. for example, 0 and 1

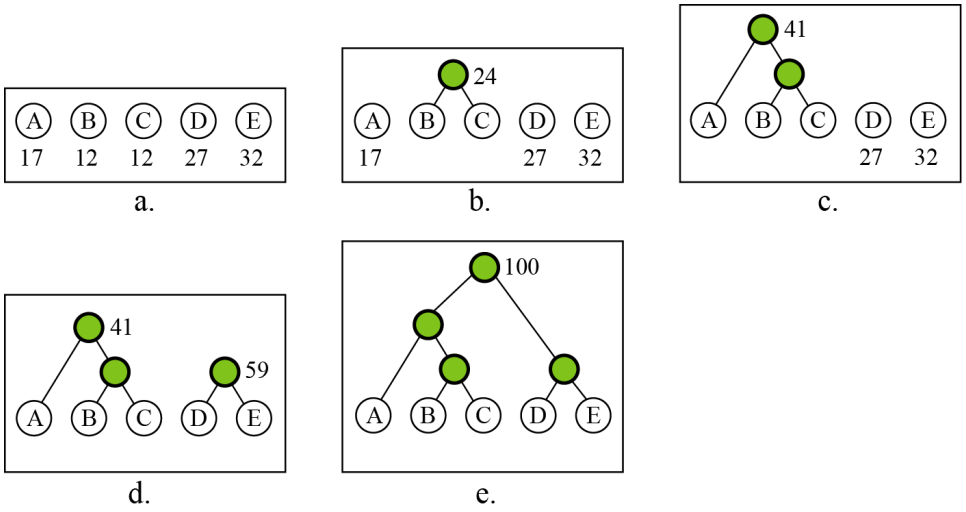


2. Huffman coding

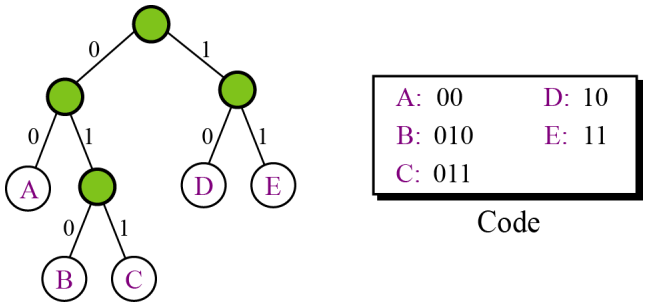
Huffman coding assigns shorter codes to symbols that occur more frequently and longer codes to those that occur less frequently. For example, imagine we have a text file that uses only five characters (A, B, C, D, E). Before we can assign bit patterns to each character, we assign each character a weight based on its frequency of use.

Table 15.1 Frequency of characters

Character	A	B	C	D	E
Frequency	17	12	12	27	32



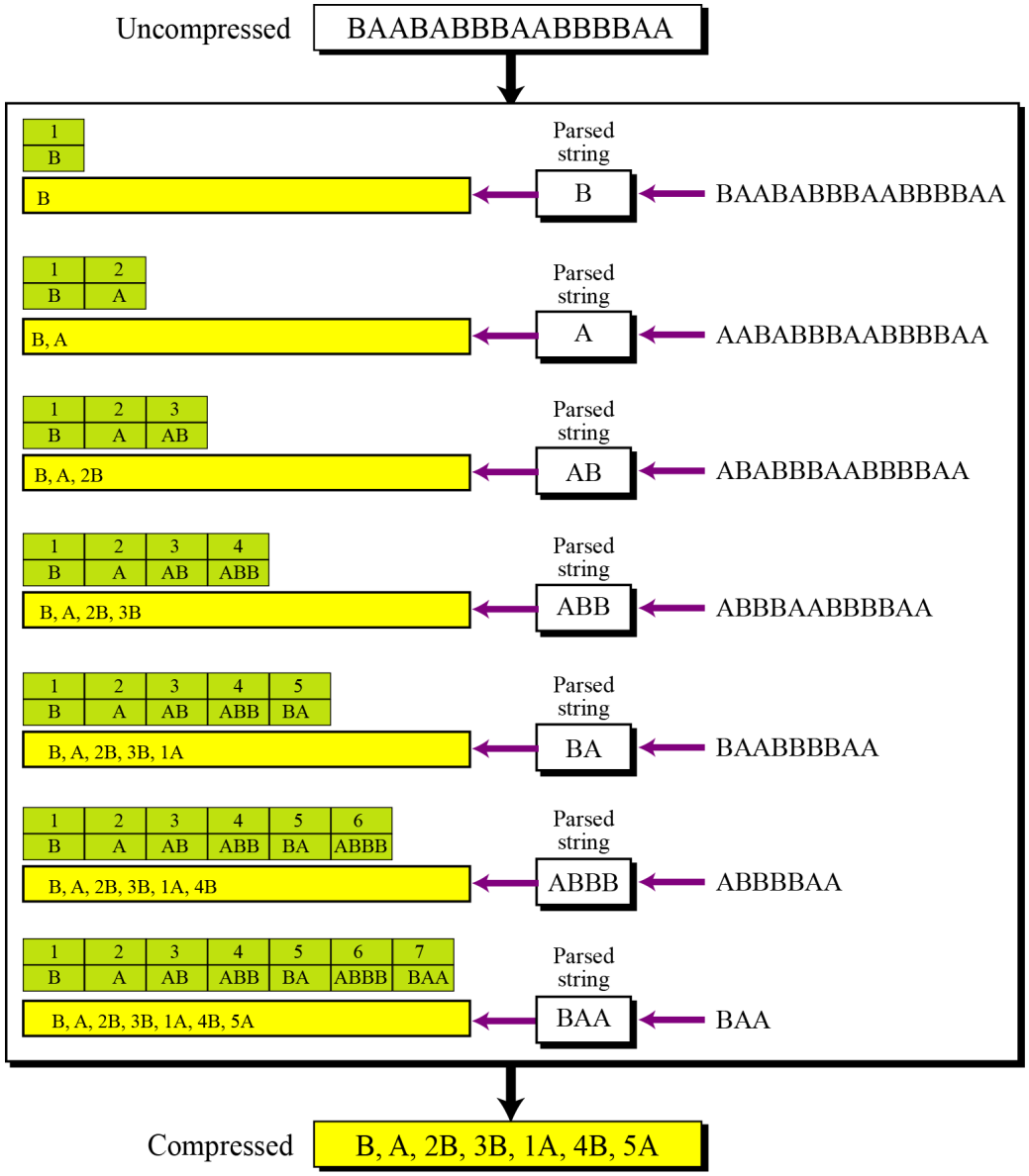
A character's code is found by starting at the root and following the branches that lead to that character. The code itself is the bit value of each branch on the path, taken in sequence.



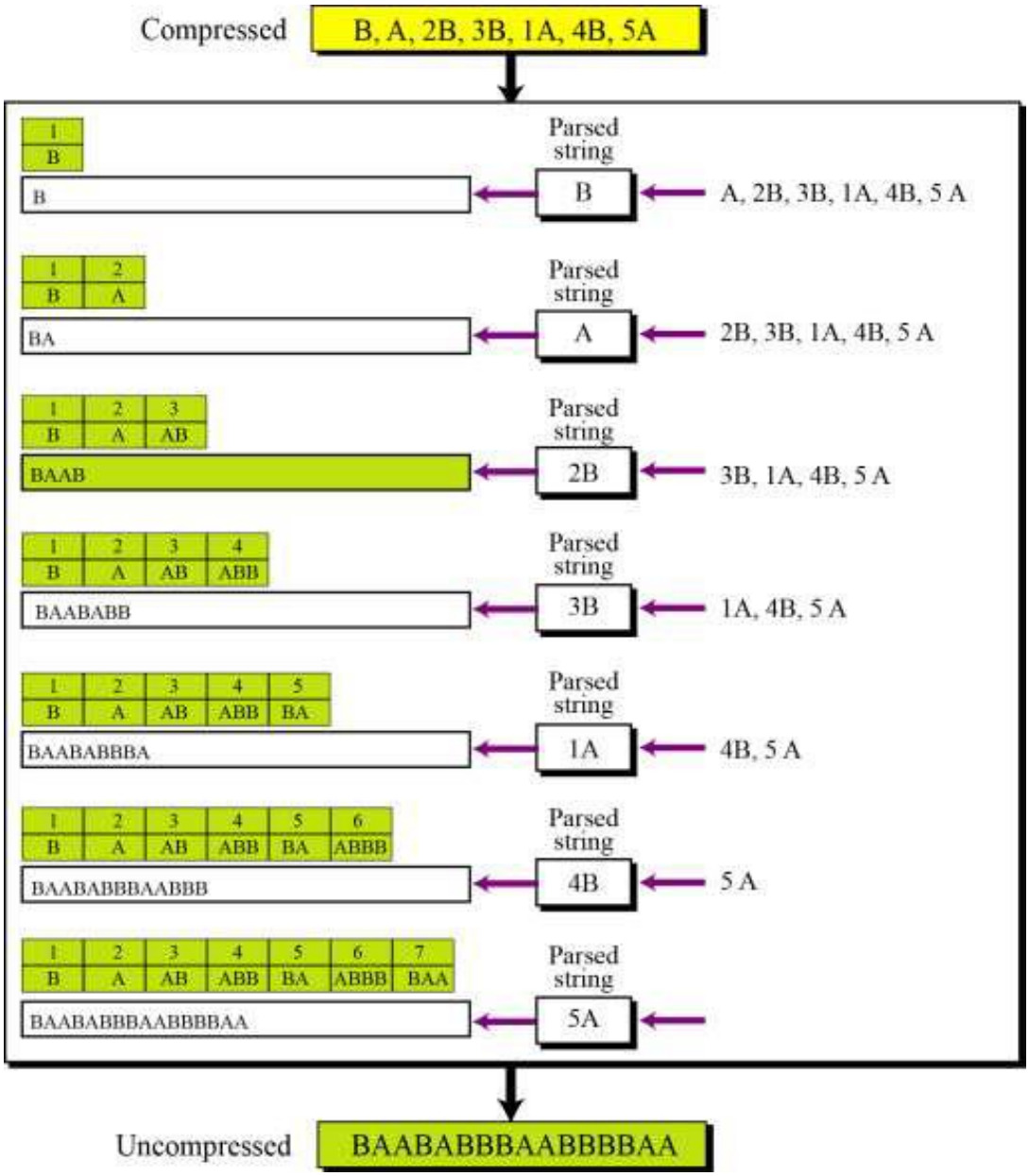
3. Lempel Ziv encoding

Lempel Ziv (LZ) encoding is an example of a category of algorithms called *dictionary-based* encoding. The idea is to create a dictionary (a table) of strings used during the communication session. If both the sender and the receiver have a copy of the dictionary, then previously-encountered strings can be substituted by their index in the dictionary to reduce the amount of information transmitted. In this phase there are two concurrent events: **building an indexed dictionary** and **compressing a string of symbols**.

Compression occurs when the substring, except for the last character, is replaced with the index found in the dictionary. The process then inserts the index and the last character of the substring into the compressed string.



Decompression is the inverse of the compression process. The process extracts the substrings from the compressed string and tries to replace the indexes with the corresponding entry in the dictionary, which is empty at first and built up gradually. The idea is that when an index is received, there is already an entry in the dictionary corresponding to that index.



LOSSY COMPRESSION METHODS:

Lossy compression reduces a file by permanently eliminating certain information, especially redundant information. When the file is uncompressed, only a part of the original information is still there (although the user may not notice it).

Lossy compression is generally used for video and sound, where a certain amount of information loss will not be detected by most users.

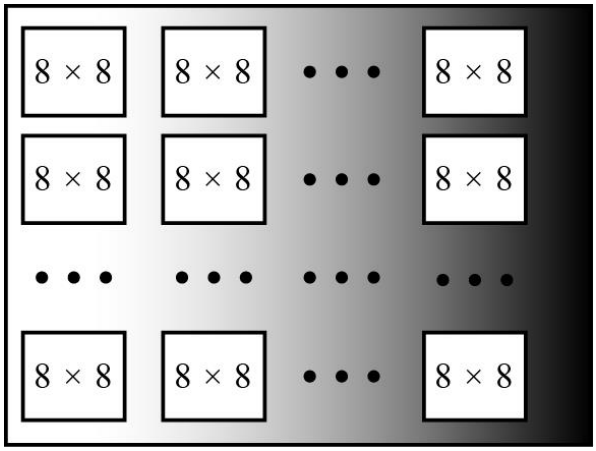
JPEG (Joint Photographic Experts Group) encoding is used to compress pictures and graphics, **MPEG (Moving Picture Experts Group)** encoding is used to compress video, and **MP3 (MPEG audio layer 3)** for audio compression.

1. JPEG: Image Compression

An image can be represented by a two-dimensional array (table) of picture elements (pixels).

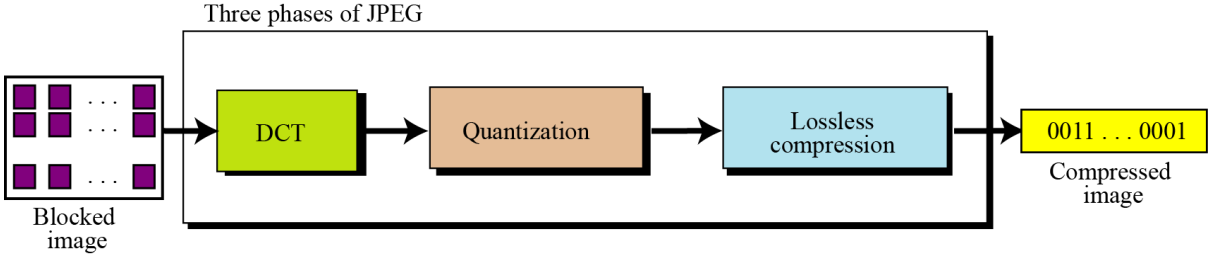
A grayscale picture of 307,200 pixels is represented by 2,457,600 bits, and a color picture is represented by 7,372,800 bits.

In JPEG, a grayscale picture is divided into blocks of 8 × 8-pixel blocks to decrease the number of calculations. (because, the number of mathematical operations for each picture is the square of the number of units)



JPEG grayscale example, 640 × 480 pixels

The whole idea of JPEG is to change the picture into a linear (vector) set of numbers that reveals the redundancies. The redundancies (lack of changes) can then be removed using one of the lossless compression methods.



The JPEG compression process

Discrete cosine transform (DCT)

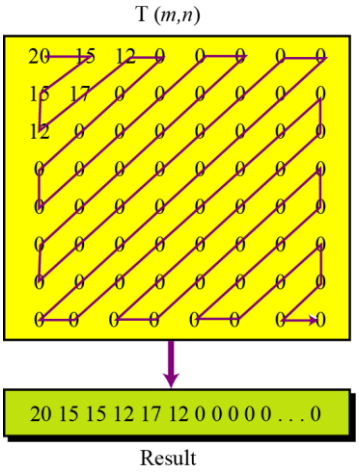
In this step, each block of 64 pixels goes through a transformation called the **discrete cosine transform (DCT)**. The transformation changes the 64 values so that the relative relationships between pixels are kept but the redundancies are revealed.

Quantization

After the transformation, table T is created, the values are quantized to reduce the number of bits needed for encoding. Quantization divides the number of bits by a constant and then drops the fraction. This reduces the required number of bits even more. In most implementations, a quantizing table (8 by 8) defines how to quantize each value. The divisor depends on the position of the value in the T table. This is done to optimize the number of bits and the number of 0s for each particular application.

Compression

After quantization the values are read from the table, and redundant 0s are removed. However, to cluster the 0s together, the process reads the table diagonally in a zigzag fashion rather than row by row or column by column. The reason is that if the picture does not have fine changes, the bottom right corner of the T table is all 0s.
JPEG usually uses run-length encoding at the compression phase to compress the bit pattern resulting from the zigzag linearization.



Reading the table

2. MPEG: Video Compression

The **Moving Picture Experts Group (MPEG)** method is used to compress video. In principle, a motion picture is a rapid sequence of a set of frames in which each frame is a picture. In other words, a frame is a spatial combination of pixels, and a video is a temporal combination of frames that are sent one after another. Compressing video, then, means spatially compressing each frame and temporally compressing a set of frames.

Spatial compression

The spatial compression of each frame is done with JPEG, or a modification of it. Each frame is a picture that can be independently compressed.

Temporal compression

In temporal compression, redundant frames are removed. When we watch television, for example, we receive 30 frames per second. However, most of the consecutive frames are almost the same. For example, in a static scene in which someone is talking, most frames are the same except for the segment around the speaker's lips, which changes from one frame to the next.

3. Audio Compression

Audio compression can be used for speech or music. For speech we need to compress a 64 kHz digitized signal, while for music we need to compress a 1.411 MHz signal. Two categories of techniques are used for audio compression: **predictive encoding** and **perceptual encoding**.

Predictive encoding

In predictive encoding, the differences between samples are encoded instead of encoding all the sampled values. This type of compression is normally used for speech. Several standards have been defined such as GSM (13 kbps), G.729 (8 kbps), and G.723.3 (6.4 or 5.3 kbps).

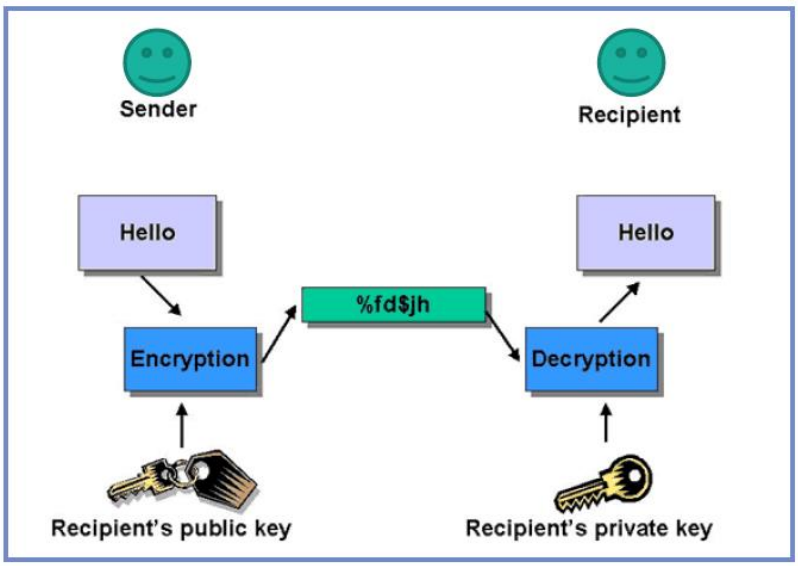
Perceptual encoding: MP3

The most common compression technique used to create CD-quality audio is based on the perceptual encoding technique. This type of audio needs at least 1.411 Mbps, which cannot be sent over the Internet without compression. MP3 (MPEG audio layer 3) uses this technique.

Encryption/ Decryption

Encryption – sender transform original information (plaintext) to another form (ciphertext) by a function that is parameterised by a key.

Decryption – reverses the original process to transform the message (ciphertext) back to its original form (plaintext).



- ***Key*** – a value that is used by an algorithm to encrypt and decrypt a message.

Encrytption/Decryption Keys

- **Symmetric Keys** – use same key to encrypt and decrypt a message.

Eg.: Data Encryption Standard (DES), Triple DES (3DES), Advanced Encryption Standard (AES)

- **Asymmetric Keys** -2 keys are needed (public key and private key); 1 key to encrypt, another key to decrypt and vice versa.

Eg.: RSA and Diffie-Hellman

How Encryption Protects

Because cryptography is concerned with the storage or transmission of information, five key security functions need to be fulfilled:

Protection	Description
Confidentiality	Allow only authorized users to access information.
Authentication	Verify who the sender was and trust the sender is who they claim to be.
Integrity	Trust the information has not been altered
Nonrepudiation	Ensure that the sender or receiver cannot deny that a message was sent or received.
Access Control	Restrict availability to information.