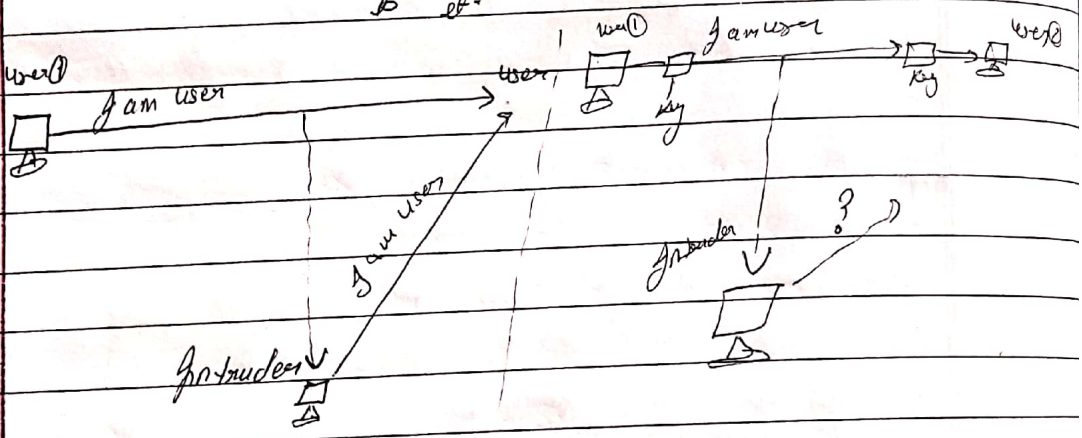
Assignment - 04

Q#1 What are the elements of Network security?

Ans Network security is required by the users to communication on the network.
If medium is insecure then an intruder may intercept. record and modify the transmitted - data from sender to reciver.

Elements of Network security

→ Confidentiality ⇒ Information should be available only to those who have rightful access to it.



* Authenticity and Integrity ⇒ The sender of a message and the message, itself should be verified at the receiving - point.

message content and sender identity falsified by Intruder. (b) method of applied security.

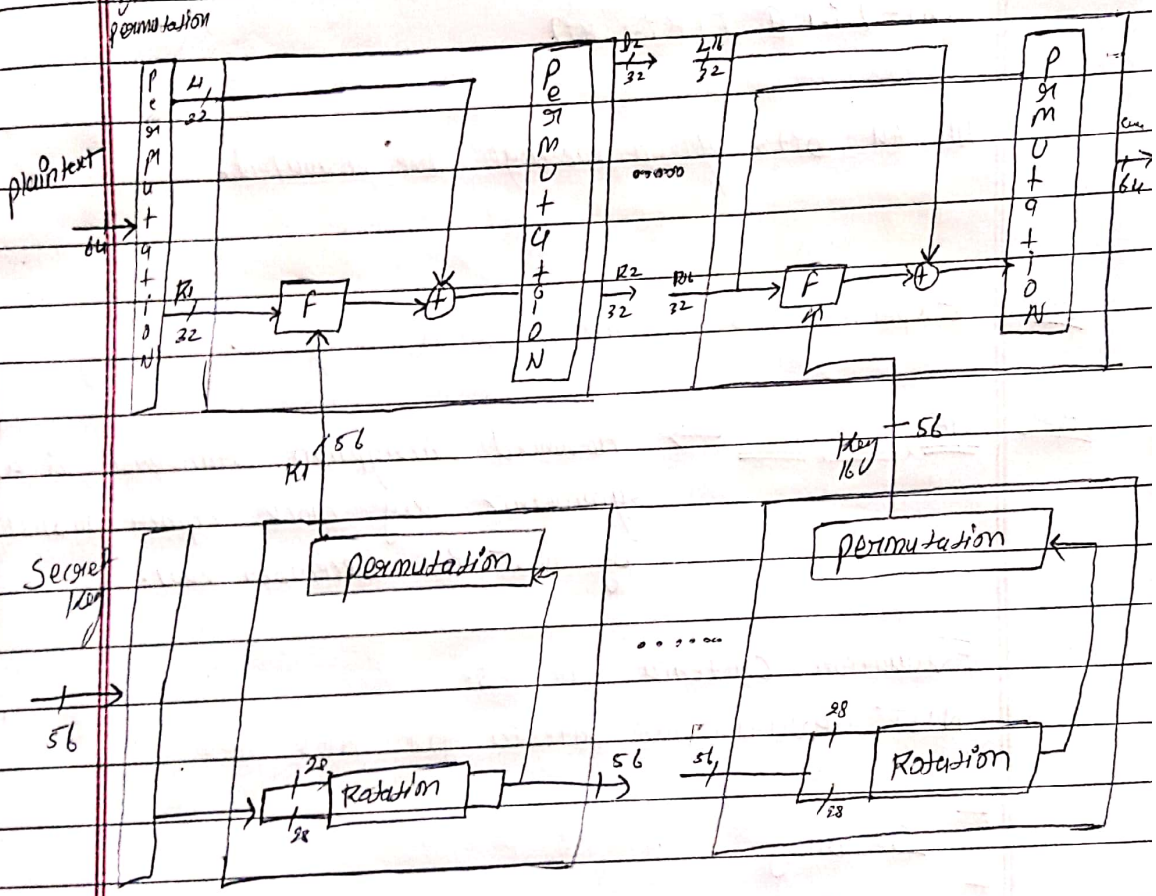
→ user 1 sends a message ("I am user") to user.
→ The Network lacks any security system. an Intruder can receive the message and change, its content to a different message.
→ a security block is added to each side of the communication

Q-12 Explain DES algorithm with diagrams.

Ans → plaintext message are converted into 64-bit blocks & each block is encrypted using a key.

* The key length is 56 bits.

* DES consist of 16 identical rounds of an operation



Begin DES algorithm.

* Initialize Before round 1 begins, all 64 bits of the message and all 56 bits of the secret keyare separately permuted.

* Each incoming 64-bit message is broken into two 32-bit halves denoted by Li and Ri respectively.

The 56 bits of the key are also broken into two 28 halves and each half is rotated one or two bit positions depending on the round.

* All 56 bits of the key are permuted, producing version Ki of the key on round i.

* Li and Ri are determined by $Li = Ri-1$

$Ri = Li-1 \oplus F(Ri-1, Ki)$

All 64 bits of a message are permuted.

Q>3 Explain AES algorithm with diagram.

Ans AES Algorithm ⟹ Advanced Encryption standard is a symmetric key block cipher published by NIST in December 2001.

Evaluation criteria for AES.
NIST evaluation criteria for AES are

* Security
* Cost
* Algorithm and implementation characteristics.

→ This refers to the effort required to cr algorithm following parameters are also consider for evaluation.

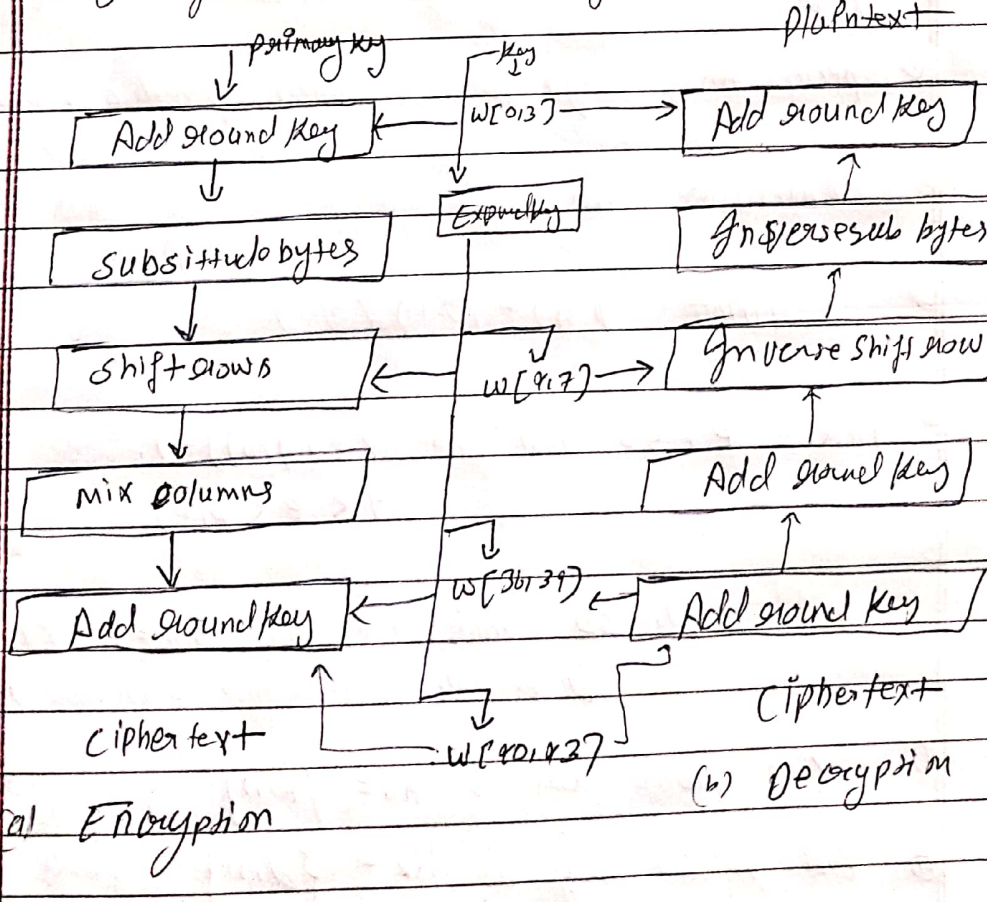
2⇒ Cost → Licensing requirements :→ When the AES is issued the algorithm specified in the AES shall be available on a worldwide.

Computational efficiency :→ The evaluation of computational efficiency will be applicable.

3⇒ Algorithm and implementation → This category includes a variety of considerations. Including flexibility.

* The input to the encryption and decryption algorithm is a single 128-bit block. The block is represented as a row of matrix of 16 bytes.

* Data block is referred to as state. Block is copied into state array which is modified at each stage of encription or decryption.



(a) Encryption

(b) Decryption

Q.x Explain RSA algorithm.

Ans → public key cryptography algorithms: RSA

* RSA is a block cipher in which the plaintext and ciphertext are integers between 0 and n-1 for some n.

* A typical size for n is 1024 bits.

* The RSA algorithm developed in 1977 by Rivest Shamir Adleman (RSA) at MIT RSA algorithm public key encription type algorithm.

* The RSA algorithm each station independently and randomly chooses two large prime p and q number.

Key generation

① pick two large prime number p and q, $p \neq q$

② calculate $n = p \times q$.

③ calculate $\phi(n) = (p-1)(q-1)$

④ Pick e, so that $\gcd(e, \phi(n)) = 1$.
$1 < e < \phi(n)$.

⑤ calculate d, so that $d \cdot e \bmod \phi(n) = 1$, i.e d is the multiplicative e in mod $\phi(n)$.

⑥ Get public key as $K_U = \{e, n\}$

⑦ Get private key as $K_R = \{d, n\}$

Encription → plaintext block $P < n$, it ciphertext

$$C = P^e \bmod n.$$

Decription → plaintext block $P < n$, it plaintext

$$P = C^d \bmod n$$

Ques Explain Diffie-Hellman key exchange protocol.

Ans Diffie-Hellman ⇒ The Diffie-Hellman key exchange protocol is a used in TLS.

The Logjam attack allows a man-in-the middle attacker to downgrade vulnerable TLS connections to 512-bit Export-grade cryptography.

This allows the attacker to read and modify any data passed over the connection.

The attack is reminiscent of the FREAK attack. but it due to a flaw in the TLS protocol rather than an implementation vulnerability and attacks.

* Diffie-Hellman key exchange rather than as RSA key exchange. The attack affects any server that supports DHE-EXPORT ciphers.

* The algorithm can not be used for any asymmetric key exchange. similarly it can not be used for signing digital signatures.

* it doesn't authenticate any parties in the transmission the Diffie Hellman key exchange.

1* Key generation algorithm

User - 1 selects a prime number 'a', random large number x_1 and a generator 'g'. 'g' such that

$$y' = g^{x'} \bmod a$$

user - 2 perform the same function and creates y_2 such that $y^2 = g^{x^2} \bmod a$

User - 1 then sends y_1 to user - 2 Now, user 1 forms its key K_1 using the information its partner sent as

$$K_1 = y_2^{x_1} \bmod a$$

User - 2 form its key K_a using the information its partner send it as

$$K_2 = y_1 x^2 \bmod a$$

The TWO keys K_1 and K_2 are qual, the two users can now encrypt their message, each using its own key -

*****

Assignment - OS

Q.1 Briefly explain three broad categories of multimedia Network application.

Ans Streaming stored audio/video
Conversational voice/video-over-IP and
Streaming live audio/video.

→ Streaming stored audio/video
The underling medium prerecorded video, for example → a movie
These prerecorded video are placed on servers.
The user send request to the server to view the video demand.

* Nowadays many internet companies provide streaming video
Example → youtube.

(1) Streaming
The client begins video playout within few seconds after it begins receiving the video from the server.

(2) Interactivity →
The media is prerecorded, so the user may pause, reposition or fast forward through video-content
* the response time should be less than a few seconds

(3) Continuous playout -
one playout of the video begins. it should proceed according to the original time. the data must receive from the server on time its playout at the

Conversational Voice and Video over-IP

* Real time conversational voice over the Internet is often referred to as Internet telephony.
* It is also commonly called Voice-over IP.
* Conversational Vedio Includes Vedio of the participants as well as there voices.
* Most today application allow user create conferences.

Streaming Live audio & video.

→ These application are similar to boardcast radio Accepted that transmission takes place over Internet.

→ These applicat allow user to receive a live radio transmitted from any corner of the world.

→ Example → live Cricket commentary.

Today thousands of radio stations around the world are boardcasting content over Internet.

live boardcast applications have many users who receive same audio program at the same time -

The network must provide an average throughput that is larger than the video consumption rate.

With a diagram, explain streaming stored video over HTTP/TCP

HTTP Streaming

The video is stored on an HTTP server as an ordinary file with a specific URL.

Here is works it work:

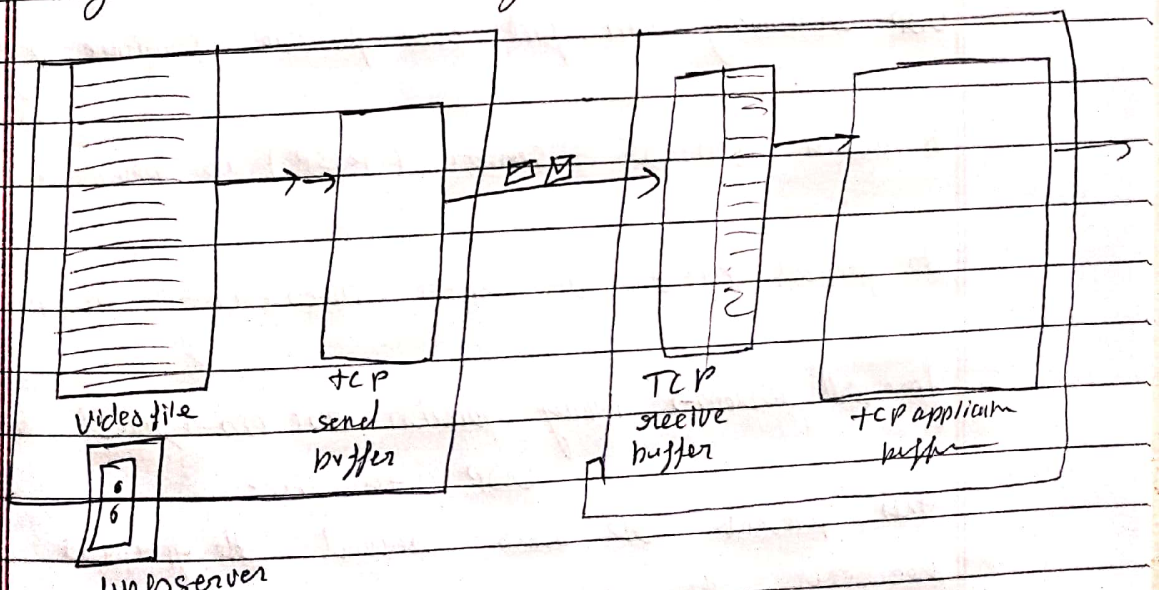
When a user want to see the media, the client establishes a TCP connection with the server and.

Issues an HTTP GET request URL.

Then the server responds with the video file.

With a HTTP response message on client side -

* This buffer exceeds a specific threshold, the client begin black on playback.



Streaming video over TCP/HTTP

Q-78 Explain UDP streaming and the challenges of UDP streaming.

Ans UDP streaming :->

The server streaming transmits video at rate that matches the client video consumption.

The server transmits the video chunks over UDP at a steady rate.

There the server can push packets into the network at the video consumption rate.

Using RTP, the server encapsulation the video chunks within transport packets.

Real time streaming protocol (RTSP) is a popular open control for connection.

Unreliability
UDP streaming can fail over provide continue playout.

A media control server (RTSP) is required.

to process client to server interactivity required.

fire wall problem-> many fireton are configured to block UDP traffic.
this prevents the user behind the firewall from receiving the video.

Q2) Support CDN operation with help of a neat diagram.

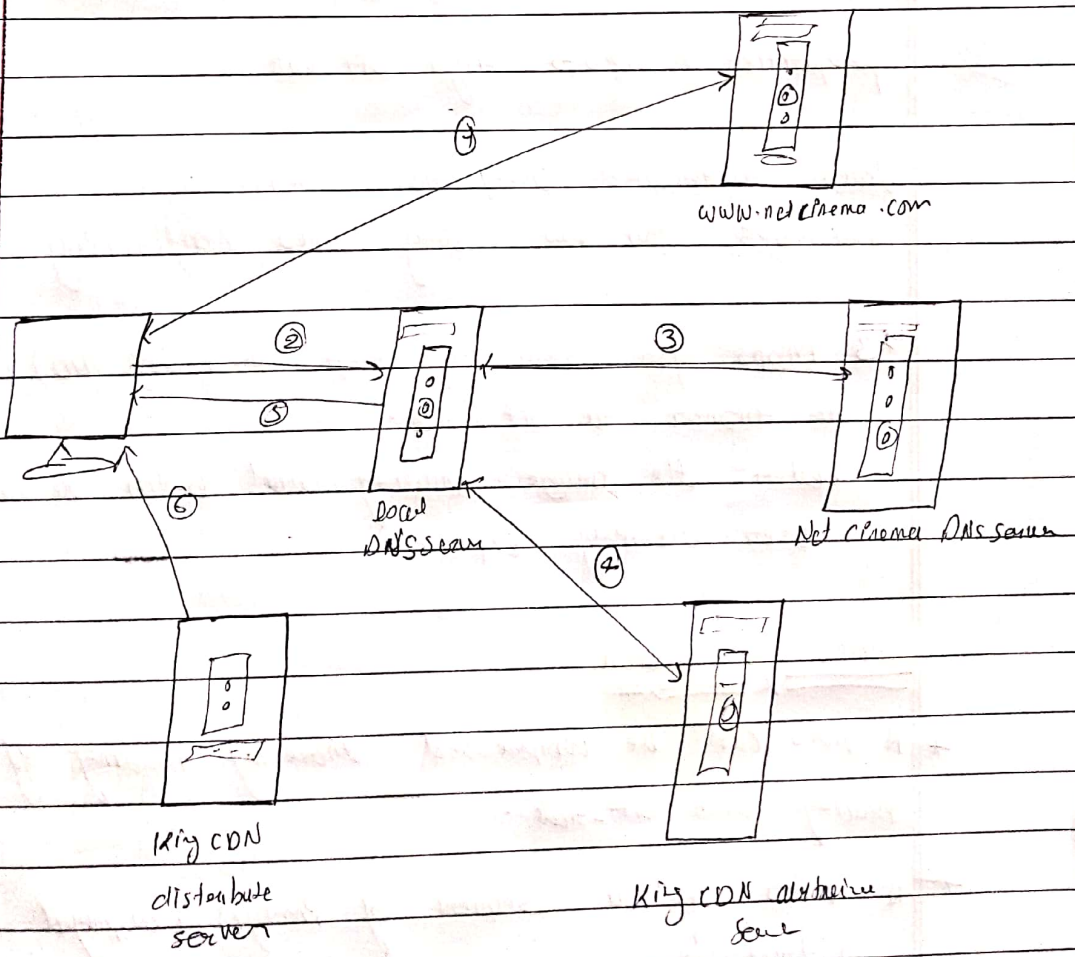
Ans CDN operation

When a browser wants to retrieve a specific video.
The CDN intercepts these request the CDN.

* determines a suitable server - cluster for the client redirects the client request to the server.

* Most CDN take advantage of DNS to intercept and redirect request.

* CDN operation is illustrated are below:



* The user host sends a DNS query for "video.netcinema"
* The server "NetCinema" returns LDNS a hostname for the kingcdn.com server.
* The user LDNS can then send a second query now for "a105.kingcdn.com".
* The LDNS forwards the IP address of the KingCDN server to the user's host.
* establishes a TCP connection with layer server.

Q->5 formulate properties of Audio and Video.

Ans properties of video -> High Bit Rate

Video distributed over the Internet use.
100 Kbps for low-quality video conferencing

-> 3 Mbps for streaming high definition (HD) movies.
the higher the bit-rate.
better the image quality and better the overall user viewing experience.

Video compression

* A video can be compressed there by trading off video quality with bit-rate.
* A video is a sequence of images, displayed at a constant rate.

Properites of Audio

* PCM pulse code modulation is a technique used to change an analog signal to digital data.

PCM Encoder

* Digital audio has lower bandwith requirements than video.
* consider how analoag audio is converted to a digital - signal.
* Example 800 samples per second.
* the value of each sample is an arbitrary real numbers.
* Each sample is then rounded to one of a finite numeer ivalues *

* * *