Scheme of Evaluation Internal Assessment Test 3 – January 2021

Sub:	Computer Networks and Security							**Code:**	18CS52
Date:	19/01/2023	Duration:	90mins	Max Marks:	50	**Sem:**	V	**Branch:**	ISE

Note: Answer Any five full questions.

Question #		Description	Marks Distribution		Max Marks
1		Discuss the working principles of Adaptive streaming and DASH. **Diagram** **Explanation**	2M 8M	10M	10M
2	a)	Perform encryption and decryption using RSA algorithm for the following: p=7, q=11,e=7, M=9. **Finding n, phi(n), d** **Encryption and Decryption** **Steps**	3M 2M 1M	6M	6M
2	b)	What do you mean by jitter and how to remove the jitter at the receiver for audio by fixed and adaptive playout delay? **Definition** **Explanation** **Example**	1 M 2 M 1 M	4M	

3	a)	Explain Diffie-Hellman key exchange algorithm in detail. **Stating Algorithm** **Explanation**	3M 2M	5M	
3	b)	Write the steps involved in Data Encryption Standard along with a diagram. **Stating Algorithm** **Explanation** **Diagram**	2M 2M 1M	5M	10M
4		Write a short notes on (i) Netflix video streaming platform (ii) VoIP with Skype **Explanation** **Diagram**	(3+3)M (2+2)M	10 M	10M
5	a)	Explain about CDN types, operations and cluster selection strategies. Types Operations Cluster selection strategies	5 M 2M 3M	10M	10M

6	a)	Describe the following protocols i)RTP ii)SIP Explanation of RTP Explanation of SIP	5M 5M	10 M	10M

Scheme Of Evaluation Internal Assessment Test 3 – Jan 2022

Sub:	Computer Networks and Security							**Code:**	18CS52
Date:	19/01/2023	Duration:	90mins	Max Marks:	50	**Sem:**	V	**Branch:**	ISE

Note: **Answer Any full five questions**

Q. 1 Discuss the working principles of Adaptive streaming and DASH.

Adaptive Streaming & DASH

• Problem with HTTP streaming:

All clients receive the same encoding of video, despite the large variati‹

bandwidth available to different clients.

Solution: Use DASH (Dynamic Adaptive Streaming over HTTP).

DASH

• The video is encoded into several different versions.

• Each version has a different bit-rate and a different quality level.

• Two main tasks:

1) The client dynamically requests video-chunks from the different versions: low & nigh.

i} When the available bandwidth is high, the client selects chunxs from a hign-rate version.

for ex: Fiber connections can receive a high-quality version.

ii) Wnen the available bandwidth is low, the client naturally selects from a tow-rate version.

for ex: 3G connections can receive a low-quality version.

2) The client adapts Lo the available bandwidth if end -to-end bandwidth cnanges during session.

This feature is particularly important for mobile-users.

The mobile-users see their bandwidth fluctuate as they move with respect to base-stations.

• HTTP server stores following files:

1) Each video version with a different URL.

2) Manifest file provides a URL for each version along with irs bit-rate.

• here is how it works:

1} First, tne client requests the manifest file and learns about the various versions.

2) Then, the client selects one chunk aF a time by specifying

URL and

—• byte range in an HTTP GET request message.

3) While downloading chunks, the client

—• measures the received bandwidth and runs a rate determination-algorithm.

i) If measured-bandwidth is high, client will choose cnun< from high-rate version.

ii) IN measured -band width is Iow, cllent will Choose chun< from low-rate v ersion

4) Therefore, DASH allows the client to freely switch among different quality-levels.

• Advantages:

1) DAShl can achieve continuous pJayout at the best possible quality level w/o frame freezing.

2) Server—side scala bility is improved : Because

—• the client maintains the intelligence to determine which cnunk to send next.

3) Client can use HTTP byte-rang e reque st to precisely control the amount of prefetched video.

Q.2a) Perform encryption and decryption using RSA algorithm for the following: p=7, q=11,e=7, M=9.

Clearly, n = p*q = 77.

We select x = 3, which is relatively prime to (p − 1)(q − 1) = 60.

Then, from xy mod (p − 1)(q − 1) = 3y mod 60 = 1, we can get y = 7.

Consequently, the public key and the private key should be {3, 77} and {7, 77}, respectively.
If we encrypt the message, we get c = mx mod n = 93 mod 60 = 3.
The decryption process is the reverse of this action, as m = c y mod n = 37 mod 60 = 9.

Q.2 b) What do you mean by jitter and how to remove the jitter at the receiver for audio by fixed and adaptive playout delay?

Packet Jitter
• fitter refers to va ryin g queui ng delays th at a packet experiences in the network's routers.
• If tfie receiver
ignores the presence of fitter and plays out audio-chunks,
then the resulting audio-quality can easily become unintelligible.
• fitter can often be removed by using seguence numbers, time stamps, and a play out delay
Removing Jitter at the Receiver for Audio
• for VoIP application, receiver must provide periodic playout of voice-chunKs ii jitter
• This is typically done by combining the following 2 mechanisms:
1) Prepending each Chunk with a Timestamp
The sender attaches each chunx with the time at which the chunk was generated.
2) Delaying Playout of Chunks at the Receiver
The playout delay of the received chunks must be long.
So, the most of the packets are received before their scheduled playout times.
This playout delay can either be
—• fixed throughout the duration of the session or
—• vary adaptively during the session-lifetime.

3A) Explain Diffie-Hellman key exchange algorithm in detail.HTTP Request Message:

- In the Diffie-Hillman key-exchange protocol, two end users can agree on a shared secret code without any information shared in advance.
- Thus, intruders would not be able to access the transmitted communication between the two users or discover the shared secret code.
- This protocol is normally used for virtual private networks (VPNs), The essence of this protocol for two users, 1 and 2, is as follows.
- Suppose that user 1 selects a prime a, a random integer number x1, and a generator g and creates y1 {1, 2, ..., a − 1} such that

$$y_1 = g^{x_1} \bmod a.$$

In practice, the two end users agree on a and g ahead of time. User 2 performs the same function and creates y2:

$$y_2 = g^{x_2} \bmod a.$$

User 1 then sends y1 to user 2. Now, user 1 forms its key, k1, using the information its partner sent as

$$k_1 = y_2^{x_1} \bmod a$$

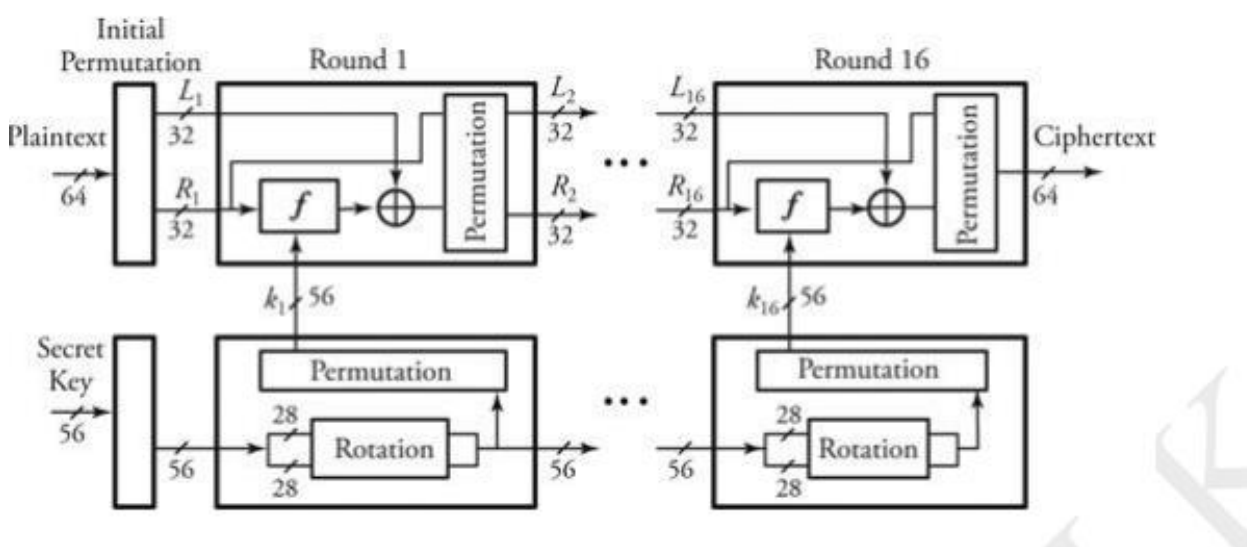
and user 2 forms its key, k2, using the information its partner sent it as

$$k_2 = y_1^{x_2} \bmod a$$

It can easily be proved that the two Keys k1 and k2 are equal. Therefore, the two users can now encrypt their messages

3 B) Write the steps involved in Data Encryption Standard along with a diagram.

- Plaintext messages are converted into 64-bit blocks,
- Each block is encrypted using a key.
- The key length is 64 bits but contains only 56 usable bits;
- The last bit of each byte in the key is a parity bit for the corresponding byte.
- DES consists of 16 identical rounds of an operation,



1. Initialize. Before round 1 begins, all 64 bits of an incoming message and all 56 bits of the secret key are separately permuted (shuffled).
2. Each incoming 64-bit message is broken into two 32-bit halves denoted by Li and Ri, respectively.
3. The 56 bits of the key are also broken into two 28-bit halves, and each half is rotated one or two bit positions, depending on the round.

4. All 56 bits of the key are permuted, producing version ki of the key on roundi.
5. In this step, is a logic Exclusive-OR, and the description of function F() appears next. Then, Li and Ri are determined by
6. All 64 bits of a message are permuted.

The operation of function F() at any round i of DES is as follows.

1. Out of 52 bits of ki, function F() chooses 48 bits
2. The 32-bit Ri−1 is expanded from 32 bits to 48 bits so that it can be combined with 48-bit ki.
3. The expansion of Ri−1 is carried out by first breaking Ri−1 into eight 4-bit chunks and then expanding each chunk by copying the leftmost bit and the rightmost bit from left and right adjacent chunks, respectively.
4. Function F() also partitions the 48 bits of ki into eight 6-bit chunks.

4. Write a short notes on (i) Netflix video streaming platform (ii) VoIP with Skype

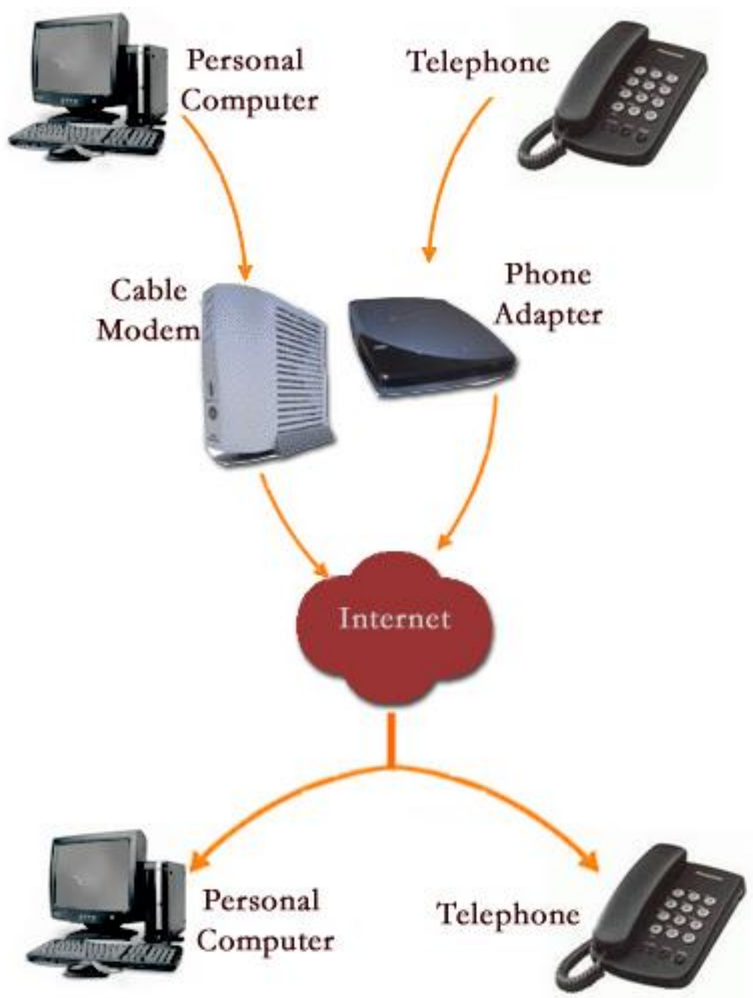
Netflix uses the internet to stream movies and TV shows from our servers to your screens, but we can't do it alone. From our servers to the world wide web to your ISP's (Internet Service Provider) network, our content travels across multiple touch points to get to your screen.

It starts when you hit ‘Play.’

First, Netflix has to decide where to send your TV show or movie from. Netflix has servers all over the world, and will send your video stream from as close to you as possible. The shorter the route, the higher the video quality.

When you hit play, Netflix uses the most efficient path possible to carry the video through our system to your ISP. Much like when traveling on a highway, Netflix tries to route your video around any traffic, accidents, or construction on the way.

Voice over Internet Protocol (VoIP), is a technology that allows you to make voice calls using a broadband Internet connection instead of a regular (or analog) phone line. Some VoIP services may only allow you to call other people using the same service, but others may allow you to call anyone who has a telephone number - including local, long distance, mobile, and international numbers. Also, while some VoIP services only work over your computer or a special VoIP phone, other services allow you to use a traditional phone connected to a VoIP adapter.



(i)

A broadband (high speed Internet) connection is required. This can be through a cable modem, or high speed services such as DSL or a local area network. **A computer, adaptor, or specialized phone is required.** Some VoIP services only work over your computer or a special VoIP phone, while other services allow you to use a traditional phone connected to a VoIP adapter. If you use your computer, you will need some software and an inexpensive microphone. Special VoIP phones plug directly into your broadband connection and operate largely like a traditional telephone. If you use a telephone with a VoIP adapter, you'll be able to dial just as you always have, and the service provider may also provide a dial tone.

5 Explain about CDN types, operations and cluster selection strategies.

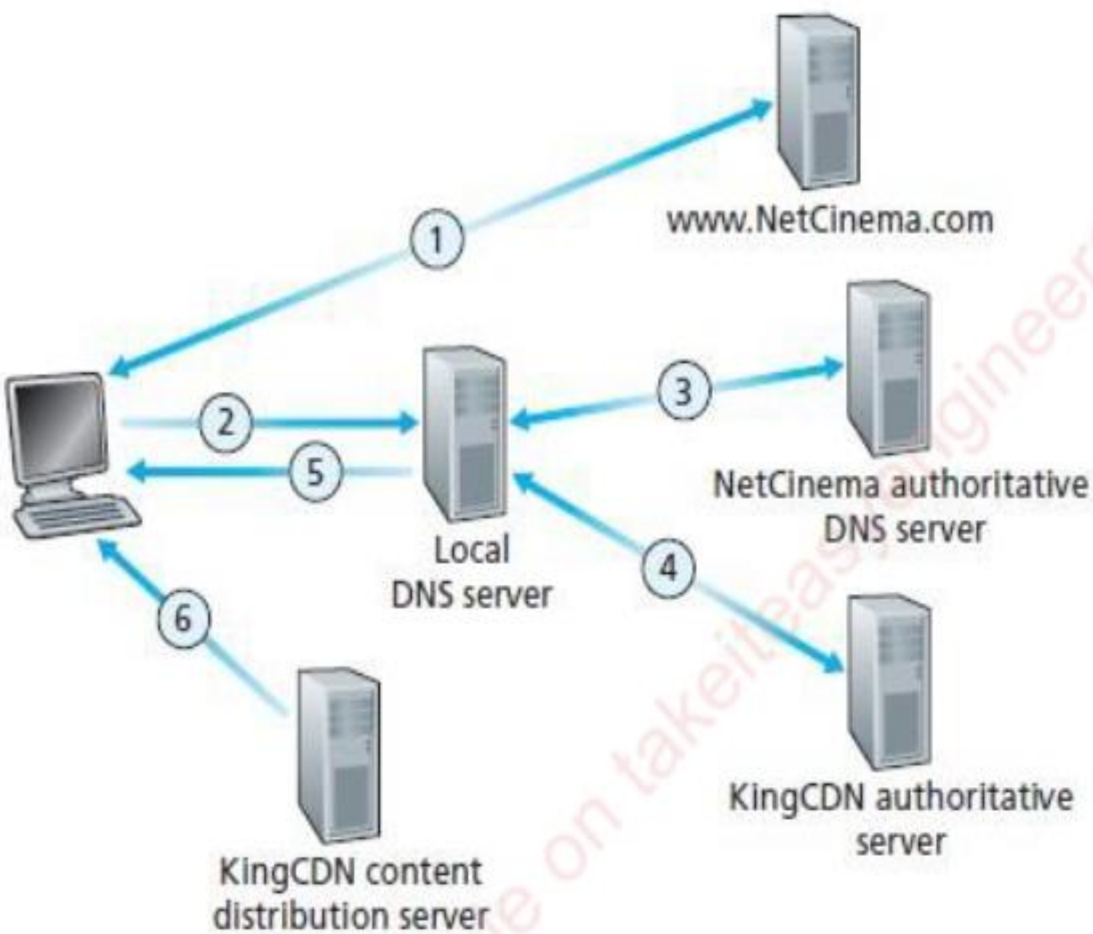
➔ CDN Operation

When a browser in a user's host is instructed to retrieve a specific video (identi

the CDN must intercept the request so that it can

(1) Determine a suitable CDN server cluster for that client at that time.

(2) Redirect the client's request to a server in that cluster.



➔ Cluster Selection Strategies

- Cluster Selection Strategies is a mechanism for dynamically
cluster or a data center within the CDN.
- The CDN learns the IP address of the client's LDNS server v
After learning this IP address, the CDN needs to select an appro
address.
- One simple strategy is to assign the client to the cluster that is g
commercial geo-location databases each LDNS IP address
location. When a DNS request is received from a particular L
geographically closest cluster.

6Describe the following protocols i)RTP ii)SIP

• RTP can be used for transporting common formats such as
→ MP3 for sound and
→ MPEG for video
• It can also be used for transporting proprietary sound and video formats.
• Today, RTP enjoys widespread implementation in many products and research
• It is also complementary to other important real-time interactive protocols, suc

5.4.1.1 RTP Basics

• RTP runs on top of UDP.
• The RTP packet is composed of i) RTP header & ii) audio chunk
• The header includes
i) Type of audio encoding
ii) Sequence number and
iii) Timestamp.
• The application appends each chunk of the audio-data with an RTP header.

SIP (Session Initiation Protocol) is an open and lightweight protocol.
Main functions of SIP:
1) It provides mechanisms for establishing calls b/w a caller and a callee over a
2) It allows the caller to notify the callee that it wants to start a call.
3) It allows the participants to agree on media encodings.
4) It also allows participants to end calls.
5) It provides mechanisms for the caller to determine the current IP address of
6) It provides mechanisms for call management, such as
→ adding new media streams during the call
→ changing the encoding during the call
→ inviting new participants during the call,
→ call transfer and
→ call holding.