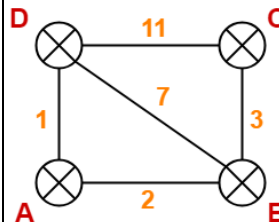


USN



Internal Assessment Test 3 – January 2022

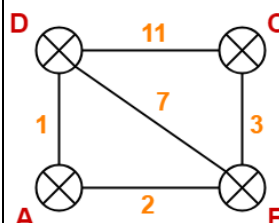
Sub:	Computer Networks and Security				Sub Code:	18CS52	Branch:	ISE		
Date:	24/01/2022	Duration:	90 min's	Max Marks:	50	Sem/Sec:	V A, B & C		OBE	
Answer any FIVE FULL Questions								MARKS	CO	RBT
1	Discuss the working principles of Adaptive streaming and DASH.						[10]	CO5	L2	
2	<p>Consider there is a network consisting of 4 routers. The weights are mentioned on the edges. Weights could be distances or costs or delays. Find out the final routing tables for all the routers using Distance Vector Routing algorithm.</p> 						[10]	CO3	L3	
3a)	Perform encryption and decryption using RSA algorithm for the following: $p=7$, $q=11$, $e=7$, $M=9$.						[6]	CO4	L3	
3b)	What do you mean by jitter and how to remove the jitter at the receiver for audio by fixed and adaptive playout delay?						[4]	CO5	L1	

P.T.O.

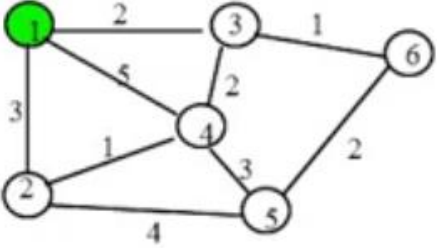
USN



Internal Assessment Test 3 – January 2022

Sub:	Computer Networks and Security				Sub Code:	18CS52	Branch:	ISE		
Date:	24/01/2022	Duration:	90 min's	Max Marks:	50	Sem/Sec:	V A, B & C		OBE	
Answer any FIVE FULL Questions								MARKS	CO	RBT
1	Discuss the working principles of Adaptive streaming and DASH.						[10]	CO5	L2	
2	<p>Consider there is a network consisting of 4 routers. The weights are mentioned on the edges. Weights could be distances or costs or delays. Find out the final routing tables for all the routers using Distance Vector Routing algorithm.</p> 						[10]	CO3	L3	
3a)	Perform encryption and decryption using RSA algorithm for the following: $p=7$, $q=11$, $e=7$, $M=9$.						[6]	CO4	L3	
3b)	What do you mean by jitter and how to remove the jitter at the receiver for audio by fixed and adaptive playout delay?						[4]	CO5	L1	

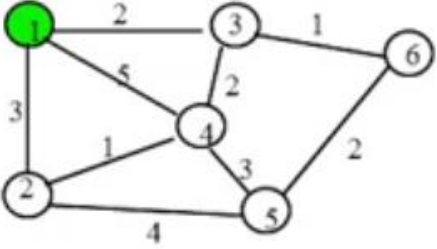
P.T.O.

4a)	Explain Diffie-Hellman key exchange algorithm in detail.	[5]	CO4	L2
4b)	Write the steps involved in Data Encryption Standard along with a diagram.	[5]	CO4	L2
5	Write a short notes on (i) Netflix video streaming platform (ii) VoIP with Skype	[10]	CO5	L1
6	Explain Link state algorithm and shows step by step process of link state for the following network. 	[10]	CO3	L3

Faculty Signature

CCI Signature

HOD Signature

4a)	Explain Diffie-Hellman key exchange algorithm in detail.	[5]	CO4	L2
4b)	Write the steps involved in Data Encryption Standard along with a diagram.	[5]	CO4	L2
5	Write a short notes on (i) Netflix video streaming platform (ii) VoIP with Skype	[10]	CO5	L1
6	Explain Link state algorithm and shows step by step process of link state for the following network. 	[10]	CO3	L3

Faculty Signature

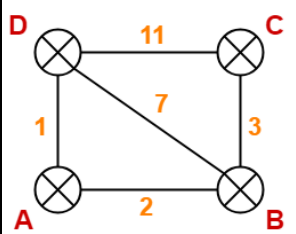
CCI Signature

HOD Signature

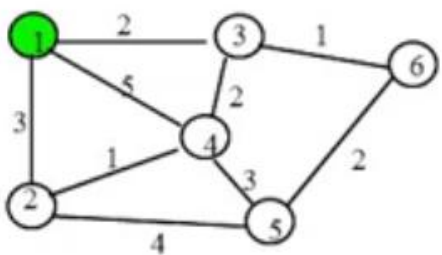
Scheme of Evaluation Internal
Assessment Test 3 – January 2021

Sub:	Computer Networks and Security					Code:	18CS52		
Date:	24/01/2022	Duration:	90mins	Max Marks:	50	Sem:	V	Branch:	ISE

Note: Answer Any five full questions.

Question #	Description	Marks Distribution	Max Marks
1	<p>Discuss the working principles of Adaptive streaming and DASH.</p> <p>Diagram Explanation</p>	<p>2M 8M</p>	10M
2	<p>Consider there is a network consisting of 4 routers. The weights are mentioned on the edges. Weights could be distances or costs or delays. Find out the final routing tables for all the routers using Distance Vector Routing algorithm.</p>  <p>Routing table at all routers Shortest path Least cost</p>	<p>8M 1M 1M</p>	10M
3	<p>a) Perform encryption and decryption using RSA algorithm for the following: $p=7, q=11, e=7, M=9$.</p> <p>Finding n, phi(n), d Encryption and Decryption Steps</p>	<p>3M 2M 1M</p>	10M

3	b)	<p>What do you mean by jitter and how to remove the jitter at the receiver for audio by fixed and adaptive playout delay?</p> <p>Definition Explanation Example</p>	<p>1M 2M 1M</p>	4M	
4		<p>Explain Diffie-Hellman key exchange algorithm in detail.</p> <p>Stating Algorithm Explanation</p>	<p>3M 2M</p>	5M	10M
4	b)	<p>Write the steps involved in Data Encryption Standard along with a diagram.</p> <p>Stating Algorithm Explanation Diagram</p>	<p>2M 2M 1M</p>	5M	
5	a)	<p>Write a short notes on (i) Netflix video streaming platform (ii) VoIP with Skype</p> <p>Explanation Diagram</p>	<p>(3+3)M (2+2)M</p>	10M	10M

6	a)	<p>Explain Link state algorithm and shows step by step process of link state for the following network.</p>  <p>Explanation Steps</p>	<p>5M 5M</p>	10M	10M
---	----	--	------------------	-----	-----

Scheme Of Evaluation Internal Assessment Test 3 – Jan 2022

Sub:	Computer Networks and Security						Code:	18CS52	
Date:	24/01/2022	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 variation in 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 & high.
 - i) When the available bandwidth is high, the client selects chunks from a high-rate version.
for ex: Fiber connections can receive a high-quality version.
 - ii) When the available bandwidth is low, the client naturally selects from a low-rate version.
for ex: 3G connections can receive a low-quality version.
 - 2) The client adapts to the available bandwidth if end-to-end bandwidth changes 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.

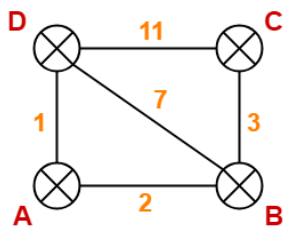
- HTTP server stores following files:

- 1) Each video version with a different URL.
- 2) Manifest file provides a URL for each version along with its bit-rate.

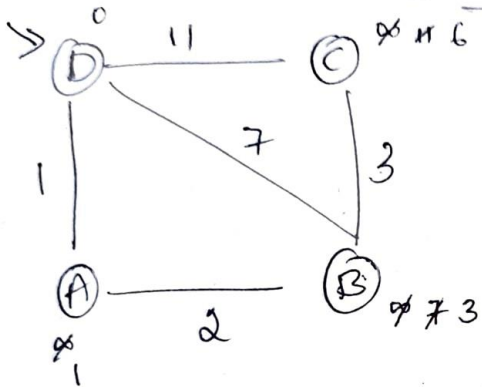
- here is how it works:

- 1) First, the client requests the manifest file and learns about the various versions.
- 2) Then, the client selects one chunk at 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 chunk from high-rate version.
 - ii) If measured-bandwidth is low, client will choose chunk from low-rate version.
- 4) Therefore, DASH allows the client to freely switch among different quality-levels.
 - Advantages:
 - 1) DASH can achieve continuous playback at the best possible quality level w/o frame freezing.
 - 2) Server-side scalability is improved : Because
 - the client maintains the intelligence to determine which chunk to send next.
 - 3) Client can use HTTP byte-range request to precisely control the amount of prefetched video.

Q2) Consider there is a network consisting of 4 routers. The weights are mentioned on the edges. Weights could be distances or costs or delays. Find out the final routing tables for all the routers using Distance Vector Routing algorithm.



Bellman Ford algorithm



Source = D

4 nodes so

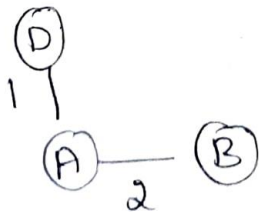
$4 - 1 = 3$ iterations

Edge List - (D,C) (D,B) (D,A) (C,B) (A,B)

Iteration	D	A	C	B
0	0	∞	∞	∞
1	0	1	11	7
2	0	1	11	3
3	0	1	6	3

Least Cost D - B = 3

Least path



Q.3 a) Perform encryption and decryption using RSA algorithm for the following: p=7, q=11,e=7, M=9.

Clearly, $n = p \cdot q = 77$.

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

Then, from $xy \bmod (p - 1)(q - 1) = 3y \bmod 60 = 1$, 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 $c = mx \bmod n = 93 \bmod 77 = 16$.

The decryption process is the reverse of this action, as $m = c y \bmod n = 16 \cdot 7 \bmod 77 = 9$.

Q.3 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

- jitter refers to varying queuing delays that a packet experiences in the network's routers.

- If the receiver

ignores the presence of jitter and plays out audio-chunks,

then the resulting audio-quality can easily become unintelligible.

- jitter can often be removed by using sequence numbers, time stamps, and a playout delay

Removing Jitter at the Receiver for Audio

- for VoIP application, receiver must provide periodic playout of voice-chunks to remove jitter

- This is typically done by combining the following 2 mechanisms:

- 1) Prepending each chunk with a Timestamp

The sender attaches each chunk 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.

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

- In the Diffie-Hellman 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 x_1 , and a generator g and creates $y_1 \in \{1, 2, \dots, a - 1\}$ 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 y_2 :

$$y_2 = g^{x_2} \text{ mod } a.$$

User 1 then sends y_1 to user 2. Now, user 1 forms its key, k_1 , using the information its partner sent as

$$k_1 = y_2^{x_1} \text{ mod } a.$$

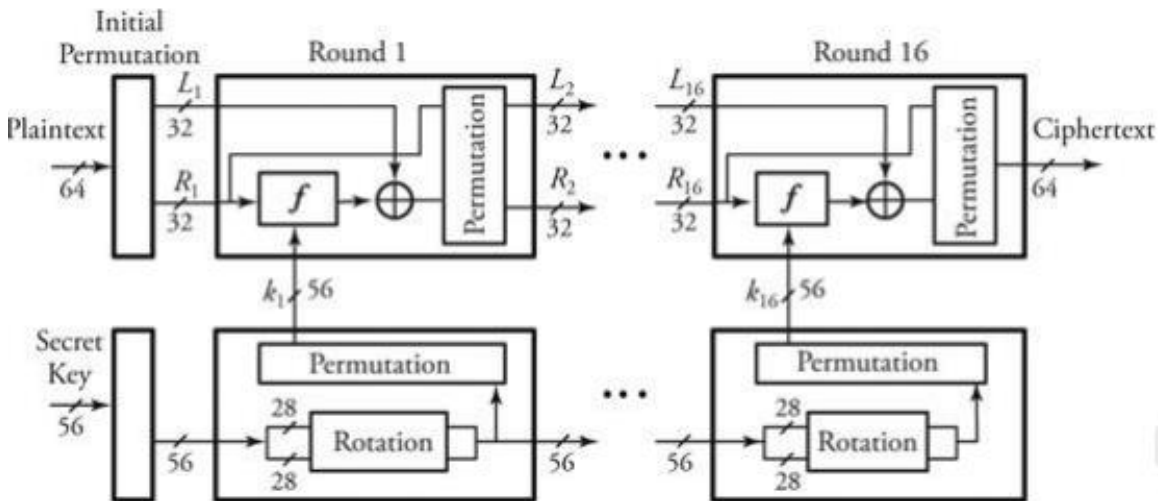
and user 2 forms its key, k_2 , using the information its partner sent it as

$$k_2 = y_1^{x_2} \text{ mod } a$$

It can easily be proved that the two Keys k_1 and k_2 are equal. Therefore, the two users can now encrypt their messages

4. 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 L_i and R_i , 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 k_i of the key on round i .
5. In this step, is a logic Exclusive-OR, and the description of function $F()$ appears next. Then, L_i and R_i 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 k_i , function $F()$ chooses 48 bits
2. The 32-bit R_{i-1} is expanded from 32 bits to 48 bits so that it can be combined with 48-bit k_i .
3. The expansion of R_{i-1} is carried out by first breaking R_{i-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 k_i into eight 6-bit chunks.

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

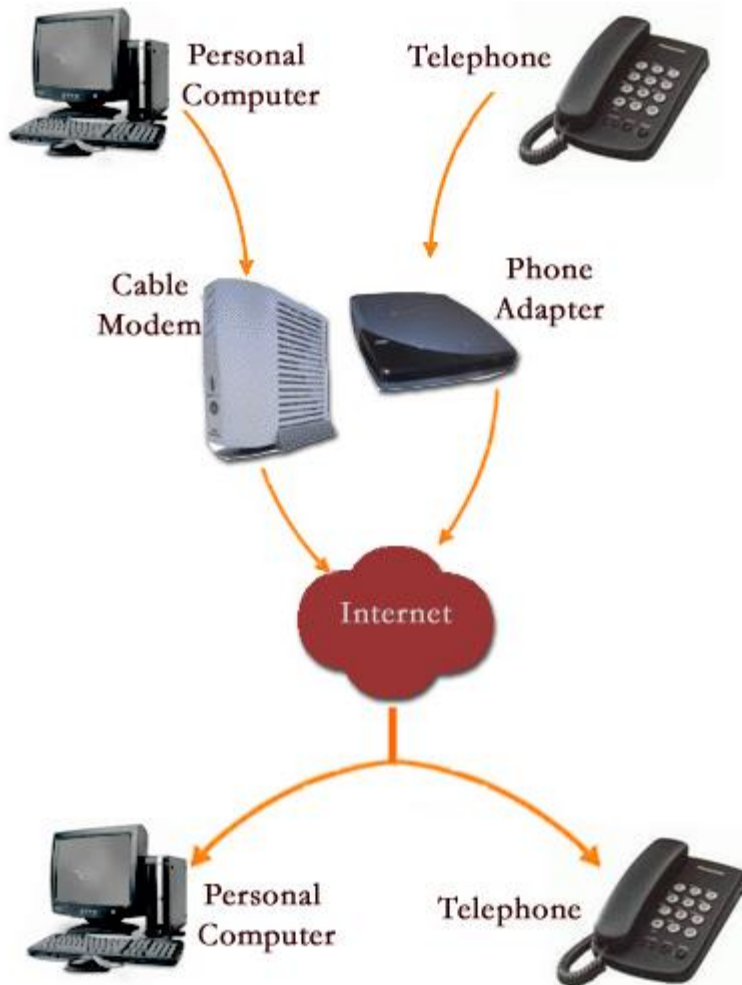
Netflix uses the internet to stream movies and TV shows from our servers to your screens, but we can't do it alone. From our servers to the world wide web to your ISP's (Internet Service Provider) network, our content travels across multiple touch points to get to your screen.

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.

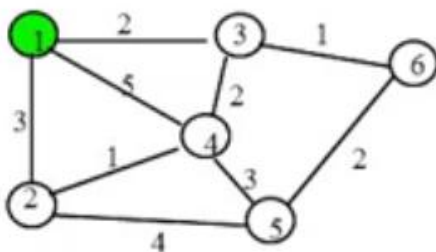
Voice over Internet Protocol (VoIP), is a technology that allows you to make voice calls using a broadband Internet connection instead of a regular (or analog) phone line. Some VoIP services may only allow you to call other people using the same service, but others may allow you to call anyone who has 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.



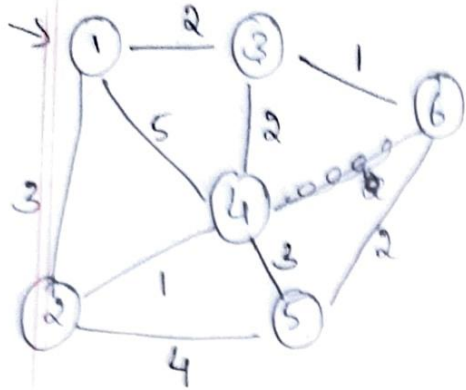
(i)

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.

6 Explain Link state algorithm and shows step by step process of link state for the following network.



Dijkstra's algorithm



	1	2	3	4	5	6
1	0	∞	∞	∞	∞	∞
3		3	2	5	∞	∞
6		3		5	∞	3
2		3		5	5	
4				4	5	
					5	

least cost 1-6 \rightarrow 3

shortest path $(1) \xrightarrow{2} (3) \xrightarrow{1} (6)$