

## Unit 9 - Week 07: P2P Mailing List Services, P2P Web, P2P Search Engine, On Being Anonymous and P2P in Blockchain

Course outline
How does an NPTEL online course work?
Week 0
Week 01: P2P Networks – Motivation, Basics – Cryptographic Hash, Public Key Cryptography Principles, Security Certificates, Structured and Unstructured P2P Networks, Inconsistent Hashing, Consistent Hashing, Rendezvous Hashing, Locality Preserving Hashing, Distributed Hash Tables
Week 02: Logarithmic Partitioning of Node ID Space and Index Entry Authenticity, Implementation of Voice Over Internet Telephony in P2P Way, Leaf node, Core node and Type of Messages in DHT Networks, Static and Dynamic Partitioning of Node ID Space: Fixed and floating partitioning
Week 03: DHT Routing Protocol : Pastry and Kademlia
Week 04: Tapestry Routing Protocol, Multi-dimensional Distributed Hash Table, and Multi-Layer DHT
Week 05: Keeping <Key, Value> Pairs at Correct Root Nodes, Abrupt and Graceful Exit of Root Node, Resilience of <Key, Value> Pairs, Distributed File System, Storage Space Problem and Incentives to Share Storage
Week 06: P2P Nodes Communications Challenges in Heterogeneous Network Environments, P2P Overlaid Multicast, and A Design of P2P Email System
Week 07: P2P Mailing List Services, P2P Web, P2P Search Engine, On Being Anonymous and P2P in Blockchain
<ul style="list-style-type: none"> <li>● Lecture 24: P2P Mailing List Services: A Basic Design</li> <li>○ Lecture 25: P2P Mailing List Services: An Alternate Design</li> <li>○ Lecture 26: P2P Web: A Basic Design</li> <li>● Lecture 27: P2P Web Search Engine: A Basic Design</li> <li>● Lecture 28: P2P Internet: On Being Anonymous</li> <li>● Lecture 29: P2P in Blockchain</li> <li>○ Quiz : Assignment_7</li> <li>○ Feedback For Week 7</li> <li>○ Solution: Assignment-07</li> </ul>
Week 08: P2P Anonymous Communication, The Anonymous Communication on the Internet through TOR Network, An Introduction to TOR Browser, Hidden Services on TOR Network, and Summary of the Course
DOWNLOAD VIDEOS
Live Session

### Assignment\_7

The due date for submitting this assignment has passed.  
As per our records you have not submitted this assignment.

**Due on 2020-11-04, 23:59 IST.**

- 1) Consider the following statements about the mailing list in the traditional networks. 1 point
- LISTSERV is an email list management software program. Email list management software makes it easy to administer email lists, performing most of the operations in seconds using developed functions.
  - LISTSERV allows list owners to control the character and behaviour of their list(s).
  - The list owner is the person formally in charge of the operation of a specific list. There cannot be more than one list owner for a list. The responsibility of the list owner is limited to the list itself.
  - A list moderator may or may not be the list owner as well. There can be more than one list moderator for a list, and some lists have none. Moderators receive incoming messages sent to a moderated list and determine whether they should be accepted for distribution or rejected.
- List moderators:
- Approve messages to be posted to the list.
  - Stop inappropriate messages from being sent to the list.
  - Cannot edit the content of messages before sending them to the list.
- v. The LISERVER maintainer is the technical person in charge of the LISERVER application on a particular server.
- Has the responsibility for creating new lists and assigning list ownership.
  - Ensures that LISERVER is up and functioning correctly, with a working connection to the Internet.

Which of the above statement/s is/are **NOT** true? Select the correct code.

- i, ii  
 iii, v  
 iv  
 None of the above

No, the answer is incorrect.  
Score: 0

Accepted Answers:  
iv

- 2) Consider the following statements about the mailing list (small and large) in the P2P environments. 1 point
- Only a list subscriber should be able to read the mail. The list owner generates the group key, and this is transported through a P2P email service. This mail must be encrypted and digitally signed to maintain privacy and non-repudiation property.
  - The list owner creates the list, and the message to it is encrypted by the group key.
  - The mailing list is available with the list server. If the mailing list (e.g., all@list.iitk.ac.in) is large, it must be partitioned. The list server picks some nodes and sends the message, which has the control information. This control information conveys the index information of the partitions in the whole mailing list. If this node can not handle the partition list, it can further sub-partition the list.
  - The responsible node fetches this partitioned list, and the list (shared) is signed by both the list server (i.e. node private key) and the list owner using their private key.
  - The partition list can be represented using a tree. If we are doing 'm' fork at every node, and the depth of the tree is D. In this way, we can manage  $(m-1)^D$  number of the mail IDs in the mailing list. The value of D should be small.

Which of the above statement/s is/are **NOT** true? Select the correct code.

- i, ii  
 iii  
 iv  
 v

No, the answer is incorrect.  
Score: 0

Accepted Answers:  
iv

- 3) Which of the following sentence/s is/are true about the Universal File System (UFS)? 1 point
- In UFS, a file fragment can be indexed by its hash value, and there is a low probability that fragments have the same hash value.
- If a file is replicated on various nodes in UFS, the presence of multiple copies and their locations should be hidden from the client.
- In UFS, a file is encrypted and digitally signed by the creator of the file. This can be used in peer to peer web.
- The files in UFS will always remain in the network even when they are not used for a long time.

No, the answer is incorrect.  
Score: 0

Accepted Answers:

*In UFS, a file fragment can be indexed by its hash value, and there is a low probability that fragments have the same hash value.  
If a file is replicated on various nodes in UFS, the presence of multiple copies and their locations should be hidden from the client.*

- 4) Yacy.net is one of the examples of a Peer-to-Peer Search Engine. Which of the following sentence/s is/are **NOT** true for Peer-to-Peer Search? 1 point
- The content in the Peer to Peer web is digitally signed by the users to maintain authenticity.
- If the content publisher machine is turned off, the content published is also unavailable.
- If a keyword is unused for a longer duration, it needs to be purged to accommodate new keywords.
- Yacy.net indexes the files only on the web.

No, the answer is incorrect.  
Score: 0

Accepted Answers:

*If the content publisher machine is turned off, the content published is also unavailable.*

- 5) Why are the multiple copies of a document maintained for Peer to Peer Web? Select the correct option/s. 1 point
- If a document publisher's machine is off, even then, the document is accessible to other peers as multiple copies of the same document are maintained at multiple root nodes.
- If a node does not keep multiple copies of a document at different root nodes, its reputation goes down.
- Multiple copies of a document are for the resilience of the network.
- Number of copies of a document keeps on varying all the time.

No, the answer is incorrect.  
Score: 0

Accepted Answers:

*If a document publisher's machine is off, even then, the document is accessible to other peers as multiple copies of the same document are maintained at multiple root nodes.  
Multiple copies of a document are for the resilience of the network.*

- 6) If a node 'X' wants to connect on a Peer-to-Peer basis but does not want to reveal its identity. Which of the following sentence/s is/are true for being anonymous? 1 point
- The node 'X' can use its private key as a node ID as well as a user ID, which is generated using the RSA algorithm.
- To maintain anonymity, Node 'X' has to keep on changing its symmetric key with the other end so that nobody can eavesdrop.
- There is nothing like completely anonymous; the node 'X' can be caught by its device's IP address.
- Even with DHT routing for transferring all the messages, one endpoint can find the IP address of the other endpoint.

No, the answer is incorrect.  
Score: 0

Accepted Answers:

*To maintain anonymity, Node 'X' has to keep on changing its symmetric key with the other end so that nobody can eavesdrop.  
There is nothing like completely anonymous; the node 'X' can be caught by its device's IP address.*

- 7) Match Set I with the sentences in Set II. 1 point
- Set I.
- Anonymous Peer to Peer Network
  - Identity-based Peer-to-Peer Network
- Set II.
- Mutual Authentication based on user ID is required at the beginning of the session.
  - Node ID can be used as an identity.
  - RSA algorithm can be used to generate public, private key pair
  - DHT routing algorithms can be used for query routing.
  - Brihaspati 4 is one of the examples.

- A (1,2,3,4,5) ; B(1,2,4,5)  
 A(1,2,3,4); B(2,3,4,5)  
 A(2,4); B(1,2,3,4)  
 A(3,4,5); B(1,2)

No, the answer is incorrect.  
Score: 0

Accepted Answers:

*A(1,2,3,4); B(2,3,4,5)*

- 8) Consider the following statements about search engines. 1 point
- Search engines have three primary functions:
    - Crawl: Scour the Internet for content and looking over the code/content for each URL they find.
    - Index: Store and organize the index to the content found during the crawling process.
    - Rank: Provide the pieces of content that will best answer a searcher's query.
  - Crawling is the discovery process in which search engines send out a team of robots known as a crawler. This crawler finds new and updated content. Content can vary; it could be a webpage, an image, a video, a PDF, etc. but regardless of the format, content is discovered by links.
  - Search engines process and store information present in an index.
    - When someone performs a search, search engines scour their index for highly relevant content. Then orders that content to solve the searcher's query. This ordering of search results by relevance is known as ranking.
    - When someone searches a website (e.g., site.iitk.ac.in) for a keyword. If this site is not showing up anywhere in the search results, there are a few possible reasons why:
      - Your site is brand new and hasn't been crawled yet.
      - Your site is NOT linked to, from any external websites.
      - Your site's navigation makes it hard for a robot to crawl it effectively.
      - Your site contains some basic code called crawler directives that are blocking search engines.

Which of the above statement/s is/are **NOT** true? Select the correct code.

- i, ii  
 iii  
 iv  
 v

No, the answer is incorrect.  
Score: 0

Accepted Answers:

i

iv

- 9) Consider the following statements about Peer to Peer search engines. 1 point
- P2P search engines for the Internet use structured and unstructured indexing mechanism both.
  - In the P2P Inverted Index, it keep on purging the old keyword not used for a longer duration and keep on adding the new keywords which have been searched for the first time.
  - If a new keyword is searched, there is no entry in the inverted index; the search will return no result. Now crawlers will learn the new keyword and then start populating the index with a new keyword.
  - The crawling rate for different keywords can not be modified as per the usage frequency of the keyword.

Which of the above statement/s is/are **NOT** true? Select the correct code.

- i  
 ii  
 iii  
 iv

No, the answer is incorrect.  
Score: 0

Accepted Answers:

i

iv

- 10) Consider the following statements about Blockchain. Which of the following sentence/s is/are **TRUE** for Blockchain? 1 point
- A Blockchain allows the peer-to-peer exchange of digital currencies without intermediaries such as banks like we do in the cash transaction.
- Miners in Blockchain are computers that initiate the transaction.
- The user ID is the public key of the node in any blockchain transaction.
- The person involved in the transaction can access all the records on Blockchain.

No, the answer is incorrect.  
Score: 0

Accepted Answers:

*A Blockchain allows the peer-to-peer exchange of digital currencies without intermediaries such as banks like we do in the cash transaction.  
The user ID is the public key of the node in any blockchain transaction.*