Roll No.: _____

Amrita Vishwa Vidyapeetham

Amrita School of Computing, Coimbatore

B.Tech Midterm Examinations – April 2023

Sixth Semester

Computer Science & Engineering

19CSE311 Computer Security

Duration:Two hours

Maximum: 50 Marks

CO	Course Outcomes (COs):
CO01	Understand the fundamental concepts of computer security and apply to different components of computing systems.
CO02	Understand basic cryptographic techniques.
CO03	Understand how malicious attacks, threats, security and protocol vulnerabilities impact a system's Infrastructure.
CO04	Demonstrate knowledge in terms of relevance and potential of computer security for a given application.

Answer all questions

1. a. Consider an automated cash deposit machine in which users provide a card or an account number to deposit cash. Give examples of confidentiality, integrity, and availability requirements associated with the system, and, in each case, indicate the degree of importance of the requirements. **[CO01][BTL2][4 Marks]**

b. For each of the following assets, assign a low, moderate, or high impact level for the loss of confidentiality, availability, and integrity, respectively. Justify your answers. **[CO01][BTL3][4 Marks]**

i. An organization managing public information on its Web server.

ii. A law enforcement organization managing extremely sensitive investigative information.

iii. A financial organization managing routine administrative information (not privacy-related information).

iv. An information system used for large acquisitions in a contracting organization contains both sensitive, pre-solicitation phase contract information and routine administrative information. Assess the impact for the two data sets separately and the information system.

2. Network security is a broad term that covers the security of the communications as well as device security. As the lead security advisor of a fortune 500 company, you have realized that one of your employees is unhappy with your company and is attempting to tamper your network from within the company. Assuming that the employee still has low level physical access to the machine answer the following questions: **[CO03][BTL3][8 Marks]**

a. Mention the intrusion technique used by the attacker and justify your answer alongside a brief description of the intrusion type. **[2 Marks]**

b. Assume that you have attempted to mitigate the issue by revoking the credentials of the user. However, they are now attempting to bypass their lack of access by getting another users password. Explain three different methods that this malicious user can use to gain access to another password. **[6 Marks]**

3. a. Analyze the key distribution method given in Figure 1 for performing online banking transactions and answer the following questions.

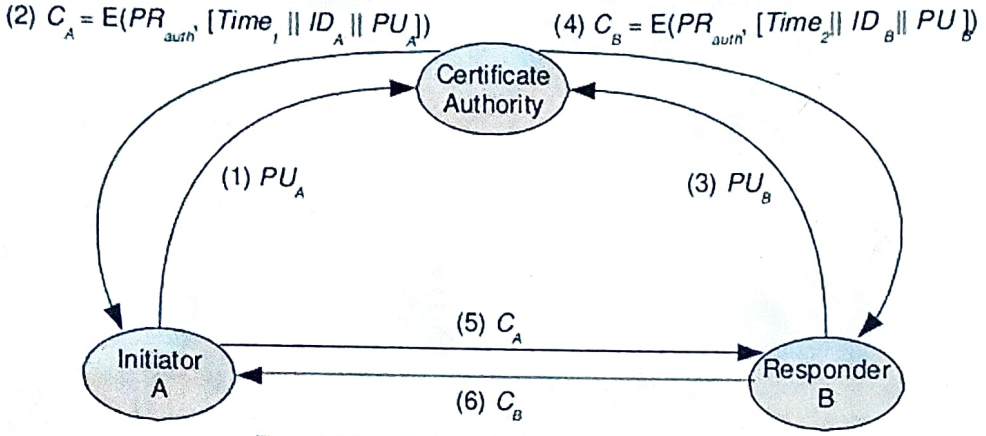


Figure 1: Certificate Authority Key Distribution Scheme

i. The procedure in Figure 1 assumes each node already has (or knows) some keys. List those keys for each node: **[CO04][BTL4][3 Marks]**

i. Certificate Authority (Auth)
ii. User A
iii. User B

ii. Is it required that message 1 (and 2) be sent before message 3 (and 4)? Justify. **[CO04][BTL4][2 Marks]**

b. i. Alice and Bob select p = 61 and g = 55 for a Diffie-Hellman key exchange. Alice sends 32 to Bob, and Bob sends 54 to Alice. What is their shared secret? **[CO02][BTL3][1 Mark]**

ii. How many primitive roots are there in total for 61? **[CO02][BTL3][1 Mark]**

iii. Considering computational Diffie-Hellman problem and decisional Diffie-Hellman problem which of these is more difficult? Justify. **[CO02][BTL3][1 Mark]**

4. a. Given are two protocols in which the sender's party performs the respective operations. mentioned in the table given below: Analyze these protocols and fill the table entries for each of the protocol given. Justify your answer in every case.

[CO02][BTL 4][4 Marks]

S. No	Protocol	Security Service	Provided – Yes or No	Justification
i)	$y = e_{k1}[x \| H(k_2 \| x)]$ where x is the message, H is a hash function such as SHA-1, e is a symmetric-key encryption algorithm, E is a public key encryption, "‖" denotes simple concatenation, and k_1, k_2 are secret keys which are only known to the sender and the receiver.	Integrity		
		Non-repudiation		
ii)	$y = x, E_{Kpub}(H(x))$ where x is the message, and k_{pr} is a private key of the sender and k_{pub} is a public key of the receiver, H is a hash function	Integrity		
		Non-repudiation		

b. Mr. X sends a signature value $sig(w) = 6292$ for a text $w = 123$ with an RSA signature scheme. The public key chosen is ($n = 9797$, $e = 131$). Mr. Y must analyze the signature sent by Mr. X. Verify the correctness of the signature to help Mr. Y.

[CO02][BTL4][4 Marks]

5. a. Given the input state of AES after shift rows, compute the missing values (marked with ?) after mix column operation. **[CO02][BTL3][4 Marks]**

Matrix after Shift Rows :

$$\begin{bmatrix} C4 & DE & F7 & 9E \\ 4C & 95 & C0 & 35 \\ FD & 7B & 69 & C7 \\ 59 & E3 & 1E & BA \end{bmatrix}$$

Matrix after Mix Column

$$\begin{bmatrix} \square & ? & \square & \square \\ \square & \square & \square & \square \\ \square & \square & ? & \square \\ \square & \square & \square & \square \end{bmatrix}$$

b. Assume that there are two parties (A and B) trying to communicate over untrusted network. There is a requirement that the communication needs to be secure and error-free. Suppose that the data " 1100 1101 0110 1011"was sent by Alice to Bob, using CRC verify whether the data was received without any errors. Show the computation on both the sender and receiver side with $G(x) = x^8 + x^2 + x + 1$.

[CO01][BTL3][4 Marks]

6. a. Assume that amrita.edu is more or less the only major University web site that doesn't support, multi-factor authentication. The reason it doesn't use MFA is that due to an old platform incompatibility. It requires utmost security, since submission of marks and grades by professors is done through UI provided by this site. Partially to compensate, there is auditing, email confirmation of major actions, etc. Tabulate the pros and cons of this approach as compared with multifactor authentication system.

[CO04][BTL4][5 Marks]

b. Given that Alice and Bob have decided to use RSA for secure e-mail communication and public key of Alice is 11, 65. Assume that Eve has intercepted the cipher text(22 mod 65) communicated by Bob to Alice. Eve claims that she has figured out the original message. Is her claim right?If yes what is the original message? **[CO02][BTL3][4 Marks]**

c. "One might assume that larger, faster computers will enable "hackers" to break codes more easily and thus make public key cryptosystems less secure". Is this statement True/False? Justify your answer. **[CO04][BTL4][1 Mark]**

****

Course Outcome /Bloom's Taxonomy Level (BTL) Mark Distribution Table

CO	Marks	BTL	Marks
CO01	12	2	4
CO02	21	3	27
CO03	8	4	19
CO04	9		

AG 19945

Roll No.: CB.EC.U20196

Amrita Vishwa Vidyapeetham
Amrita School of Computing, Coimbatore
B.Tech Mid Term Examinations – April 2023

Sixth Semester
Computer Science and Engineering

19CSE312 Distributed Systems

Duration: Two hours

Maximum: 50 Marks

CO	Course Outcomes
CO1	Understand the design principles in distributed systems and the architectures for distributed systems.
CO2	Apply various distributed algorithms related to clock synchronization, concurrency control, deadlock detection, load balancing, voting etc.
CO3	Analyze fault tolerance and recovery in distributed systems and algorithms for the same.
CO4	Analyze the design and functioning of existing distributed systems and file systems.
CO5	Design and implement a simple distributed system and implement different distributed algorithms over it.

Answer all the questions

1. "It is not always a good idea to aim at implementing the full distribution transparency." Is this statement True? Justify your answer. [3] [CO1] [BTL2]

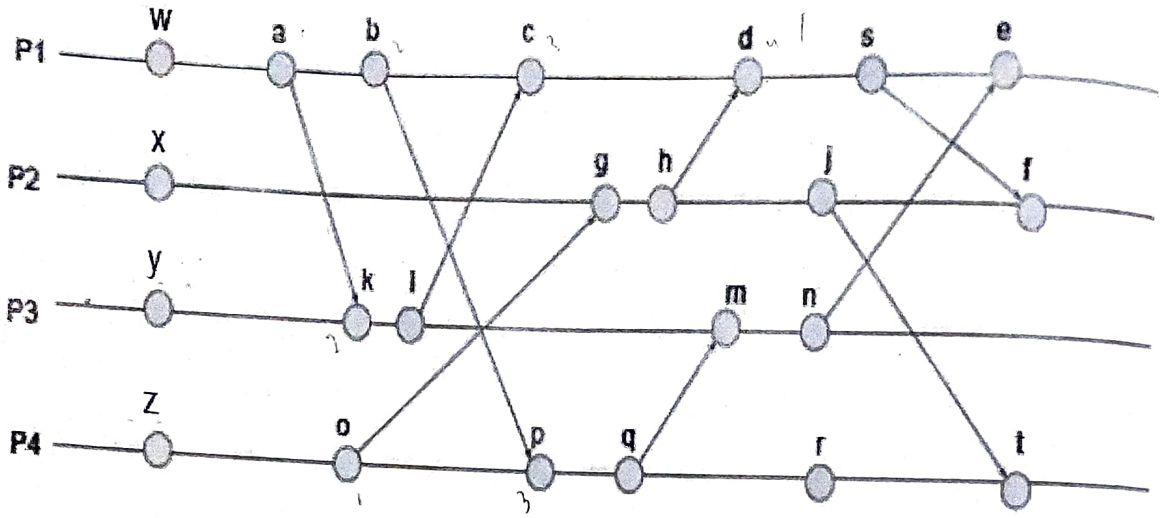
2. a) Scaling with replication in a distributed system leads to inconsistencies. Substantiate the statement with an example. [2] [CO1] [BTL2]

   b) Applications can often be constructed from three different layers, interface layer, processing layer and data layer. With the help of a figure, explain the simplified organization of an Internet search engine into these three different layers. [5][CO1] [BTL2]

3. a) For any two events e_i e_j, with the scalar timestamp of $C(e_i)$ and $C(e_j)$ respectively, prove the following property.

   i. Scalar timestamps are consistent but not strongly consistent.
   ii. $C(e_1)$ represents the height of the event e_i

   b) A distributed computation spanning four processes (P1, P2, P3, P4) is depicted in the diagram below with initial vector timestamp values of events: w(1,0,0,0), x(0,1,0,0) , y(0,0,1,0) and z(0,0,0,1) recorded in the respective processes. [3][CO2] [BTL3]



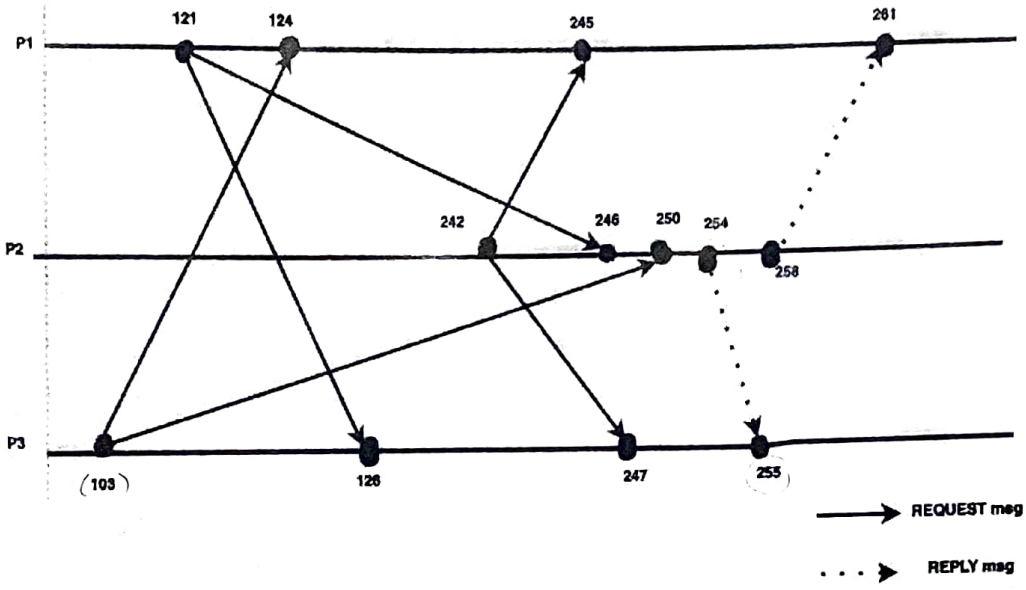
i. List all the events that happened-before (→) event 'p' and 'd'. [2]
ii. Determine the vector timestamp of events 'p', 'g' and 'd'. [2]
iii. List all the events that are concurrent with event d. [3] [CO2] [BTL3]

4. a) Visualize the following types of communications in distributed system and differentiate their functionalities.
   a. asynchronous blocking send. [2]
   b. asynchronous non-blocking send. [2]
   c. synchronous blocking send with blocking receive. [3] [CO1] [BTL2]

   b) How is Message Passing emulated on a Shared Memory system? [3][CO1] [BTL1]

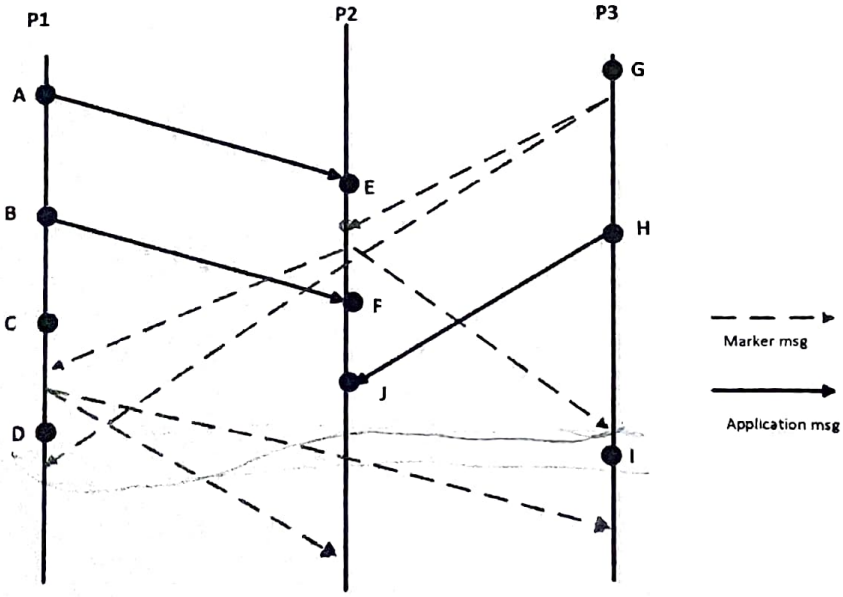
5. Consider three processes in a distributed environment. The system has totally ordered clocks by breaking ties by process ID. It uses the Ricart - Agrawala algorithm to ensure the mutual exclusion of critical sections. Each message takes 2 real-time steps to get delivered. The critical section takes 2 real-time steps. The Lamport clock-based timestamp for each process of id i is T(p) = Ci + time taken for the event execution + i .
   For Example, in process, P1 first event is of time stamp = 121 Event 2 = max(121,103) + 2 + 1 = 124

   a) Complete the process-time diagram for the process(P1, P2, P3) with the messages that are being REQUEST(it is basically broadcast) and REPLY (it is basically sent or receive event) with proper timestamp computation for sent and receive events. Depict the tracing of the algorithm with the help of a neat diagram. [6]
   b) The status of the Data structure(Deferred Request array) involved in the Ricart - Agrawala Algorithm at different timestamps of execution with proper annotation of message (For Eg, Is it Request, Reply, Execution of Critical Section). [3]
   c) Give the final order in which Processes enter the critical section. [1]
   Assume that if a process receives messages from the other two processes at the same time, the message that comes from the lower process ID will be received first. [CO2][BTL3]



6. a) Given below is the state diagram of a distributed system with three processes P1, P2 and P3. Application messages and marker messages are exchanged between the three processes and each process after receiving the marker messages records the local state of the system. Process P3 starts the global recording in the distributed system using Chandy Lamport's global state recording algorithm. Trace the algorithmic steps when each process takes its snapshot. What are the events captured in each snapshot by a process and what is the state of the channels when the algorithm terminates?

[7][CO2] [BTL3]



b) What are the conditions to be satisfied by a distributed system to be in a consistent global state? Justify your answer

[3] [CO2] [BTL2]

SE

Roll No.: 20236

Amrita Vishwa Vidyapeetham
Amrita School of Computing, Coimbatore
B.Tech. Mid Term Exam– April 2023
Sixth Semester
Computer Science and Engineering
19CSE313 Principles of Programming Languages (Lab Based)

Duration: Two hours Maximum: 40 Marks

Course Outcomes (COs):

CO	Course Outcomes
CO01	Understand and write pure functional programs (especially in Haskell and Scala).
CO02	Understand and write concurrent programs in Java.
CO03	Formulate abstractions with higher order procedures.
CO04	Formulate abstractions with data.

Instructions: Part A to be completed in Lab Duration :1 hr.15 mins

Part B to be written in the Answerbook Duration : 45 mins.

PART A

1. Write a Haskell function for the following:
   A. Define a function called "Distance", It should take four arguments (x1,y1) and (x2,y2) of type Double. Compute the Euclidean distance between the points. (x1,y1) and (x2,y2). [COO1] [BTL 3] [2 marks]

   Example
   > distance 3 4 5 6
   2.8284271247461903

   B. A postal service prices the package the following way.
   - Packages that weigh up to 500 grams cost 250 credits
   - Packages that weigh over 500 grams cost 300 credits + 1 credits per gram
   - Packages that weigh over 5000 grams costs a constant 6000 credits

   Write a Haskell function postage Price that takes the weight of the package (in grams ,Int) and returns the cost in credits (Int) [COO1] [BTL 3] [4 marks]

2. Write a Haskell higher order function "map_list" which generates a list of Int values starting from a, with an increment of next until it reaches b. The first argument is a function fn that takes an Int argument and returns a value of some type a. The second and third argument a and b are the lower limit and upper limit of the integer range to generate the list. The fourth argument next is the increment value to use when generating the list. example usage of the map_list function: [COO3][BTL 3] [7 marks]

   map_list square 1 10 2
   Output: [1, 9, 25, 49, 81]

3. Write a Haskell program only using recursion without higher-order function and list comprehension with the function largeTuples whose arguments are max and list of tuples which produces a list of the tuples whose sum is larger than max, i.e., for a tuple (a,b), a + b > max.

[COO3] [BTL 4] [7 marks]

PART B

4. A. Predict the output of the following expression: COO1][BTL 3][4 marks]

   i. ("hello" ++" world") ==" hello world"
   ii. map (+1) [0..9]
   iii. (==)((**) 2 2) ((^) 2 2)
   iv. map (take 2) ["Hello","Haskell"]

   B. Write the equivalent Haskell expressions:

```
int foo (int bar) {
    return bar * 10 + 4;
}
```

5. Explain the term "Side Effect". What is meant by "Pure" and "Impure" functions in Haskell? Mention the default nature of Haskell with respect to the same. Explain How Impure Functions can be identified in Haskell. [COO1] [BTL 2] [4 marks]

6. A. It may also be useful to write generic functions such as /= that could be implemented in terms of ==, and valid for almost anything. By having a generic function that can compare anything, we can also make our code generic: if a piece of code only needs to compare things, then it ought to be able to accept any data type that the compiler knows how to compare. How to define such generic functions in Haskell. [COO1] [BTL 4] [4 marks]

   B. Identify errors in the following code and correct it and predict the output

```
myCompare:: a->a->Ordering
a `myCompare` b
 |a>b = GT
 |a==b = EQ
 |otherwise=LT
main = do
 print(5`myCompare`4)
```

7. Fill in the missing portions (indicated by <<?>>) of the following code which finds more than one occurrence of an number in a list: [COO3][BTL 3][4 marks]

```
twoSame :: [Int] -> Bool
twoSame [] = <<?>>
twoSame ( x : xs ) = <<?>> x xs <<?>> twoSame <<?>>
```

8. Higher order function is one of the important features of Haskell. Define higher order function. What is the type of higher order functions foldr and foldl.

[COO4][BTL 2][4 marks]

Roll No.: 20236

Amrita Vishwa Vidyapeetham

Amrita School of Computing, Coimbatore

B.Tech MID TERM EXAMINATION– April 2023

Sixth Semester

Computer Science and Engineering

19CSE314 Software Engineering – Set 3

Duration: Two hours

Maximum: 50 Marks

Course Outcomes (COs):

CO	Course Outcomes
CO01	Understand and apply the principles of software engineering
CO02	Understand various software process models
CO03	Apply the appropriate software design methodology for a given scenario
CO04	Evaluate a system developed for real-world applications in Agile Mode
CO05	Understand and implement various industry standard

Answer all questions

Part-A

1) Outline the major Objects and services for smart home automation system for fire alarm, unauthorized entry and smoke/gas detection. [4] [CO03][BTL 4]
2) Illustrate how the elements of analysis model are translated into design model. [4][CO01][BTL 3]
3) Elucidate the steps that make up requirement engineering pertaining to on-line Shopping for electronic goods based on product review and brand. [4][CO03][BTL 3]
4) Identify the human factors considered for an agile software development [4][CO01][BTL 3]
5) What are the major shortcomings of the waterfall model?. How have those shortcomings been overcome by the agile model? [4][CO02][BTL 2]

Part-B

6) To effectively manage courses and classes offered by a training organization, we need to design a courseware management system that provides control and visibility over the management of courses. The system should support a variety of courses in different areas such as learning management techniques and software languages and technologies. Each course will be made up of a set of topics that can be customized based on the needs of the organization. Tutors in the organization will be assigned courses to teach based on their area of specialization and availability. The organization will publish and maintain a calendar of different courses and assign tutors to teach them each year. The courseware management system will be used by a group of Course Administrators within the

organization to manage course content, assign courses to tutors, and define course schedules. The primary goal of the courseware management system is to provide better control and visibility over the management of courses and to streamline the process of generating and managing the schedule of different courses. To achieve this, the system should include features such as:

- A centralized database to store course information, including course content, tutors, and schedules.
- An intuitive user interface to manage courses and classes, including the ability to assign tutors to courses and define course schedules.
- Automated scheduling and notifications to help Course Administrators keep track of course schedules and tutor assignments.
- Reporting and analytics capabilities to provide insights into course performance and tutor effectiveness.
- Integration with other systems used by the organization, such as HR(Human Resoures), and payroll systems, to facilitate seamless management of courses and tutors.

Overall, the courseware management system will help the training organization to efficiently manage courses and classes and provide better visibility and control over the entire process. This will enable the organization to deliver high-quality training programs and achieve its goal of providing effective and comprehensive training to its clients.

A) Draw Use case diagram pertaining to the above framework [10][CO03][BTL 4]

B) Draw an activity diagram pertaining to the above framework. [10][CO03][BTL 4]

Part-C

Viva [10][C001,C002,C003][BTL-2]

****

CO	Marks	BTL	Marks
CO01	8	BTL 1	
CO02	4	BTL 2	14
CO03	38	BTL 3	12
CO04		BTL 4	24
CO05		BTL 5	

R