Reg. No: ...., Model Question Paper
Name : ....

Second Semester M.Tech. Degree Examination, Sept 2014
Branch: Computer Science and Engineering (CS)
RCE 2007: ADVANCED GRAPH THEORY

(2013 Scheme)

Instruction: Answer **any two out of three** questions
from each module

Time: 3 Hours

Max. Marks: 60

MODULE -1

1. a. Prove that the number of vertices in a simple connected graph with odd degrees is even. 3

b. If a graph G(n,m) has degree k or k+1 for each vertex, show that the number of vertices of degree k is (k+1)n – 2m. 3

c. Prove that a simple graph with n vertices must be connected if it has more that [(n-1)(n-2)]/2 edges. 4

2. a. State and prove the sufficient conditions for a graph to be hamiltonian. 4

b. Explain the following graph operations,
i. union ii. intersection
iii. join iv. cartesian product and
v. square of a graph. 4

c. Draw a simple graph that is eulerian but not hamiltonian. 2

3. a. Prove that $\delta(G) \leq \kappa(G) \leq \lambda(G)$ 2

b. State and prove menger's theorem (vertex or edge version) 5

c. What is a circulant graph. Explain its properties with an example. 3

- MODULE -2

4. a. Draw a nontrivial graph(not a tree) with 12 vertices and 15 edges and find its radius, diameter, center(s) , median and girth. 3

b. Prove that a nontrivial graph G is radius-minimal if and only if G is a tree. 4

c. Show that the Pertersen graph on 10 vertices is a moore graph. 3

5. a. Describe the construction of an extremal graph for radius $r \geq 3$with p nodes. 3

b. Prove that the sequence $D = (d_1,d_2,\ldots,d_p)$ with $p\text{-}1 \geq d_1 \geq d_2 \geq \ldots \geq d_p$ is a graphical sequence if and only if the modified sequence $D' = (d_2\text{-}1, d_3\text{-}1, \ldots , d_{d1+1}\text{-}1, d_{d1+2},\ldots, d_p)$ is a graphical sequence. 4

c. Show how a status sequence ss(G) is derivable from ddsG). 3

6. a. What is meant by geodetic iteration number gin(G) and geodetic number gn(G). 3

b. What is a symmetric graph? 3

c. What is adjacency matrix? What properties of a graph can be derived by taking the nth power of an adjacency matrix? 4

MODULE -3

7. a Describe any one algorithm for finding the spanning tree of a nontrivial graph(p,q). 4

b. Give the Ford-Fulkerson algorithm for finding the maximum flow in a network flow graph. 4

c. What is a perfect matching. 2

8. a. Describe the Kruskal's algorithm or Prim's algorithm for finding an MST of a weighted graph. 4

b. Give an algorithm for finding the maximum matching in a bipartite graph. 4

c. Differentiate between strong, unilateral and weak connectivity in a digraph D. 2

9. a. What is a tournament? 3

b. Explain the branch and bound method for solving the TSP. 5

c. What is an activity digraph and a critical path. 2

Department of Computer Science & Engineering
College of Engineering,Trivandrum

List of subjects for M2 Computer Science & Information Security

Code	Subject	Stream
RCC 2001	OPERATING SYSTEM DESIGN	CS
RCC 2002	ADVANCED COMPUTER NETWORKS	CS
RID 2002	ADVANCED TOPICS IN DISTRIBUTED SYSTEMS(Departmental Elective)	CS&IS
RCD 2004	DATA COMPRESSION(Departmental Elective)	CS&IS
RCE 2001	PARALLEL ALGORITHMS(Stream Elective 1)	CS
RCE 2007	ADVANCED GRAPH THEORY (Stream Elective 2)	CS
RIC 2002	NETWORKS SECURITY	IS
RIC2001	FORMAL METHODS IN SECURE COMPUTING	IS
RIE 2001	DATABASE SECURITY(Stream Elective 1)	IS
RIE 2004	WEB SECURITY TESTING(Stream Elective 2)	IS

[illegible]

Department of Computer Science and Engineering

College of Engineering, Trivandrum

M2 Computer Science and Engineering (2013 scheme)

RCC 2001 Operating System Design

Time: 3 Hrs **Max.Marks: 60**

Answer any two questions from each module

Module I

1. (a) Multithreading is a commonly used programming technique. Describe three different ways that threads could be implemented. Explain how these ways compare to the Linux clone mechanism. (5)

   (b) Explain forking in Linux. (5)

2. (a) Explain the differences in the degree to which the following scheduling algorithms discriminate:

   (i) Traditional Unix scheduling

   (ii) Fair scheduling (7)

   (b) Consider a system with two runnable tasks: a text editor and video encoder.

   Describe the scheduling policy in action. (3)

3. (a) Implement a system call that uses methods copy_to_user and copy_from_user.Describe the implementation of the system call getpid( ). (6)

   (b) Describe the system call's arguments,return value and error codes with example. (4)

Module II

4. (a) Consider the following snapshot of a system:

	Allocation	Max	Available
	A B CD	A B C D	A B C D
P0	0 0 1 2	0 0 1 2	1 5 2 0
P1	1 0 0 0	1 7 5 0	
P2	1 3 5 4	2 3 5 6	
P3	0 6 3 2	0 6 5 2	
P4	0 0 1 4	0 6 5 6	

Answer the following questions using the banker's algorithm:

a. What is the content of the matrix Need ?

b. Is the system in a safe state?

c. If a request from process P1 arrives for (0,4,2,0), can the request be granted immediately? (7)

(b) List three options for breaking an existing deadlock. (3)

5. (a) Describe the implementation of softirqs and tasklets . (7)

(b) Describe registering an interrupt handler in Linux OS. (3)

6. Explain spin lock methods in Linux. (10)

Module III

7. Explain design of the slab layer. (10)

8. (a)How to allocate and destroy a memory descriptor in Linux OS. (6)

(b)Given memory partitions of 100K, 500K, 200K, 300K, and 600K (in order), how would each of the First-fit, Best-fit, and Worst-fit algorithms place processes of 212K, 417K, 112K, and 426K (in order)? Which algorithm makes the most efficient use of memory? (4)

9. Describe the Superblock object,Inode object ,Dentry object and File object. (10)

Department of Computer Science & Engineering
College of Engineering,Trivandrum
M2 Computer Science and Engg (2013 Scheme)

RCC 2002 ADVANCED COMPUTER NETWORKS

Time:3*Hrs* Max Marks: 60

Answer Any Two From each module

Module I

1. a. With an example explain the criterion to select router (5)
b.Explain with an example code division multiple acccess (5)

2. a. Explain charateristic of FDDI (5)
b. Compare Fast Ethernet and Gigabit Ethernet (3)
c.What are the drawbacks of a geostationary satellite? (2)

3. a.Suggest a set of characteristics that you would like to include into a SLA ,provided that you need to transmit the traffic of an real time live streaming of video through the network (7)
b.Is it possible to transmit traffic with long delays but without jitter? (3)

Module II

4. a. How many subnets and hosts per subnet can you get from the network 192.161.204.0/30? Also give the broadcast address for subnet zero and all-ones subnet. (5)
b.Compare AH protocol and ESP protocol (3)
c.How does an ICMP message improve the reliability of data transmission in an IP network? (2)

5. a.What is NAT?What is the main goal of NAT?Which packet attribute are used in NAT for mapping the set of internal addresses to a single global address? (3)
b. A classless address is given as 167.199.170.82/27
(i) Find the number of addresses in the block
(ii) Find the first and last addresses
(iii) If a mask of 255.255.255.224 is used then
a. Find the number of addresses in the block
b. Find first and last addresses using mask (7)

6. a.List all main stages of establishing a virtual circuit (4)
b.An organization has a class B network and wishes to form subnets for 64 departments. What would be the subnet mask? (4)

c.What is Label Distribution Protocol? (2)

Module III

7. a. Evaluate the link utilization coefficient if the data are transmitted in it using the protocol based on the idle source algorithm. The transmission rate is equal to 100 Mbps, the Round Trip Time (RTT) is 10 ms, and packets are not lost and do not get corrupted. Packet size is fixed and is equal to 1,500 bytes. Acknowledgment size can be neglected. (5)
b. Explain TCP/IP and Sketch the TCP connection initiation and connection termination packet flows using a timing diagram. (5)

8. Explain RSVP with an example for reservation style (10)

9. a.Consider the use of 1000 bit frames on a $1Mbps$ satellite channel with $270ms$ delay .What is the maximium link ultilization for

i.Stop and wait flow control

ii.Continuous flow control with window size of 7? (5)

b.A TCP entity open a connection and uses slow start.Approximately how many round trip time are required before TCP can send N segment (5)

****

Model Question Paper

Second Semester M. Tech Degree Examination(2013 scheme)

Stream: COMPUTER SCIENCE & ENGINEERING

Subject: RID2002 ADVANCED TOPICS IN DISTRIBUTED SYSTEMS

(Departmental Elective)

Time : 3 hours Marks : 60

Answer any two questions from each module.
All questions carry equal marks.

MODULE-I

1. a) Explain the goals of distributed systems.
   b) Write a note on replica management.
2. a) Explain synchronization mechanisms.
   b) What is meant by virtualization? Explain the architecture of virtual machines.
3. a) Explain data centric and client centric consistency models.
   b) Write notes on server clusters and distributed clusters.

MODULE-II

4. a) Write a note on failures in a distributed system.
   b) Show that the version of *SynchGHS* that uses edge identifiers in place of edge weights in fact produces an MST.
5. a) Write the code for *SynchBFS* algorithm and analyse its complexity. Explain its applications.
   b) What is meant by distributed snapshots? Explain.
6. a) Write the code for *OptFloodMax* algorithm.
   b) Describe in detail an algorithm that extends *SynchBFS* to allow the source process i_0 to broadcast a message to all other processes and obtain an acknowledgement that all processes have received it. Your algorithm should use $O(|E|)$ messages and $O(diam)$ time.

MODULE-III

7. a) What is meant by scaling out? Explain.
   b) Write a note on sorting and joins in MapReduce.
8. a) Explain MapReduce output formats.
   b) Explain data flow in HDFS.
9. a) Explain administration procedure in Hadoop.
   b) Explain the design and features of HDFS. What are the limitations?

(6 x 10 = 60 marks)

Model Question Paper.

Second Semester M.Tech Degree Examination

Elective-3 (Deparmental Elective) (2013 Scheme)

RCD 2004 : DATA COMPRESSION

(Specialisation : Computer Science & Engineering, Information Security)

Time : 3 Hrs. Max. Marks : 60

(Answer 2 questions from each module)

Module 1

1. (a) Write the Huffman codes for the following data [5]
   P(a)=P(c)=0.2, P(b)=0.4, P(d)=P(e)=0.1

   (b) Generate a **ternary Huffman code** for a source with 6 letter alphabet and a probability model
   P(a1)=P(a3)=P(a4)=0.2, P(a5)=0.25, P(a2)=0.05, P(a6)=0.1 [5]

2. (a) Using **LZ78** approach encode the following sequence : [5]
   wabba**b**wabba**b**wabba**b**wabba

   (b) Given alphabet A={**b**,e,h,i,s,t}. Decode the following using **move to front** method [5]
   40350135015

3. (a) Illustrate the encoding process in arithmetic coding with proper illustration. [5]

   (b) Describe the decoding procedure in Adaptive Huffman coding [5]

Module 2

4. Explain the MPEG audio coding with Layer-1, Layer-2 and Layer-3 [10]

5. (a) How silence compression is implemented in audio processing [5]

   (b) Explain the wavelet transform method for image compression. [5]

6. Describe in detail the process involved in JPEG compression. [10]

Module 3

7. (a) Explain the block based motion compression method. [5]

   (b) Write the steps in the two dimensional logarithmic search used in video compression. [5]

8. (a) Eplain one compression algorithm for packet video. [5]

   (b) Explain the fractal compression method. [5]

9. Describe the MPEG-1 video compression scheme in detail. [10]

======

Kerala University

Model Question Paper

End Semester Examination (2013 scheme)

IInd Semester M-Tech Computer Science and Engineering

RCE2001 Parallel Algorithms

3Hours 60 Marks

Answer two questions from each module

Module 1

1. A) The parallel computers of concurrent access model with very large number of processors are technologically impossible to build due to known reasons. Hence concurrent access to memory by an arbitrary number of processors may not be realizable in practice. Suggest a solution to the problem of implementing m out of N multiple access where N is the number of processors and m<N. (5 Marks)

   B) Explain the following interconnection networks of SIMD computers with neat diagrams.

   a) Perfect Shuffle Connection b) Cube Connection

   (5 Marks)

2. Given a set of numbers $\{s_1, s2,...s_N\}$. All sums of the form s_1+s_2, $s1+s_2+s_3...$ $s1+s_2+s_3+....+S_N$ are to be computed. Design an algorithm for solving this problem using N processors in an EREW SM SMID model. Explain its time complexity in terms of number of processors.

   (10 Marks)

3. A sequence of integers S = $\{s_1, s2... s_n\}$ and an integer k, $1 \leq k \leq n$ are given. It is required to determine the kth smallest element of S. A cost optimal parallel algorithm is to be designed. Suggest your choice. Why it is cost optimal? (10 Marks)

Module 2

4. Give a parallel algorithm for finding the transpose of an NXN matrix by using an NXN mesh of processors. Explain its time and cost analysis. (10 Marks)
5. A cube connected SIMD parallel computer is given. Explain the algorithm for finding the product of two matrices and its time complexity analysis. (10 Marks)
6. It is required to multiply a matrix by a vector on a tree connected SIMD parallel computer. Explain an algorithm, its time and cost analysis. (10 Marks)

Module 3

7. Explain the working of the parallel version of Gauss-Jordan algorithm for solving the following system of linear equations on an SIMD multi-processor system.

$$2x_1 + x_2 = 3$$

$$x_1 + 2x_2 = 4$$

(10 Marks)

8. Given a system of non linear equations. It is required to find the roots of the system. Suggest an SIMD algorithm for this problem. Explain its time and cost analysis. (10 Marks)

9. A cube connected SIMD parallel computer is given. Suggest an algorithm for finding Eigen values of a given nXn matrix and an nX1 vector. Explain its running time and cost analysis. (10 Marks)

Second Semester M. Tech. Degree Examination (2013 Scheme)
Branch : Computer Science
Specialization : Information Security
Subject: RIC2002 Network Security

Max Marks : 60 Duration: 3 hours

Answer two questions from each module. Each question carries 10 marks

Module 1

1. a) Find the value of d as a process of breaking security of RSA, assume that e =17 and n=187 are other parameters of RSA algorithm
   b) Define weak and strong collision resistance of a Hash Function
2. a) Explain how ESP operates in Tunnel mode
   b) What is a Clogging attack
3. What do you mean by Kerberos? Write the sequence of messages exchanged in Kerberos V4

Module II

4. With the help of a neat block diagram explain the sequence of steps for providing 'Authentication and confidentiality' with PGP
5. How SSL Record protocol provide confidentiality and message integrity? What are Security Associations?
6. Explain Secure Electronic Transactions

Module III

7. Explain the basic features of SNMP v1 and SNMP v3
8. Discuss about the security issues faced by WLAN? Describe the services offered by WEP
9. What are firewalls? What are the different types of firewall?

SECOND SEMESTER M.TECH INFORMATION SECURITY

RIC 2001 FORMAL METHODS IN SECURE COMPUTING

Model Question (2013 Scheme)

Time: 3 hrs Max Marks: 60

Answer any two questions from each module.

Module 1

1. a) Suppose an intruder picks up the following message from a protocol

Sq.<encrypt(ServerKey(b), Sq<A,k>),encrypt(k,nb)>

He would make use of deduction rules to deduce the valuable information. Illustrate. (5)

b) What is the significance of maintaining fairness, anonymity and availability in security protocol? (5)

2. a) Is the formal methods scale to "real life" applications? Justify your answer. (3)

b) How reflection leads to an attack? (4)

c) What is the significance of data types for protocol models (3)

3. a) Briefly describe the random oracle model. (5)

b) What are the limits of formal analysis? (5)

Module 2

4. Consider the following Otway-Rees protocol :

Msg1: a → b : $m.\ a.\ b.\{n_a .m.\ a.\ b\}_{ServerKey(a)}$

Msg2: b → s : $m.\ a.\ b.\{n_a.m.\ a.\ b\}_{ServerKey(a)} \cdot \{n_b .m.a.b\}_{ServerKey(b)}$

Msg3: s → b : $m.\{n_a \cdot k_{ab}\}_{ServerKey(a)} \cdot \{n_b \cdot k_{ab}\}_{ServerKey(b)}$

Msg4: b → a : $m.\{n_a \cdot k_{ab}\}_{ServerKey(a)}$

a) Give the message sequence chart for the correct run of this protocol. (5)

b) Use the message sequence chart to identify the points at which signals need to be inserted for authenticating the responder to the initiator. What information particular to the run can be included in the signals? Express the CSP description for the same. (5)

5. a) How would you change the system model to enable the distinction between initiator and responder claims of secrecy? (5)

b) If one of the coins is double-headed, but cryptographers do not know which, does the system still provide anonymity? How about if one of the coins is double-headed or double-tailed, but the cryptographers do not know which? (5)

6. a)

Msg1:	$a \rightarrow b$:	n_a
Msg2:	$b \rightarrow s$:	$\{a. n_a . n_b\}_{ServerKey(b)}$
Msg3a:	$s \rightarrow a$:	$\{b. k_{ab.} n_a . n_b\}_{ServerKey(a)}$
Msg3b:	$s \rightarrow b$:	$\{a . k_{ab}\}_{ServerKey(b)}$
Msg4:	$a \rightarrow b$:	$\{n_b\}_{kab}$

Investigate the effect of moving b's identity outside of the encrypted component of Msg3a. Compare the above protocol with Yahalom protocol. (5)

b) Specify that b should not have the message m until a has the required evidence that b has received the message m. (5)

Module 3

7. a) Can we use BAN logic for security analysis of a protocol? Illustrate. (5)

b) What are the salient features of Dolev-Yao model (5)

8. a)How Spi calculus is being used for modeling and reasoning of security protocol?(5)

b) Write a short note on NRL analyser (5)

9. a) What is strand spaces model? (5)

b) Briefly describe Spi Calculus. (5)

Model Question Paper

Second Semester M.Tech Degree Examination (2013 Scheme)

Branch : Computer Science and Engineering – Information Security

RIE 2001 – Database Security (Elective)

Time : 3 Hours Max. Marks : 60

*Answer any **two** questions from each module. All questions carry equal marks*

Module I

1. Explain the concept of a multi level relational model. Describe the various granularities of classifying data in a DBMS based on security levels. Give suitable examples. (10)

2. Explain the modified Bell and LaPadula security model used to provide mandatory security in databases. Describe (a) integrity lock architecture and (b) distributed architecture for implementing multi level security in databases. (10)

3. Describe the various methods to ensure discretionary security in database systems. (10)

Module II

4. Describe the various architectures for providing security in heterogeneous and federated database systems. What are the issues that arise when performing schema integration and security policy integration in such systems? (10)

5. Write notes on secure multimedia data management systems. (10)

6. Discuss the various multi level security architectures for distributed databases. (10)

Module III

7. Discuss the process of designing a secure data warehouse. (10)

8. Write detailed notes on the various aspects of ensuring security for digital libraries. (10)

9. What are the various threats faced by web databases? Discuss some solutions for the same. (10)

Kerala University

Model Question Paper, End Semester Examination

IInd Semester M-Tech Information Security(2013 Scheme)

Stream Elective 2 RIE 2004 Web Security Testing

3Hours **60 Marks**

Answer two questions from each module

Module 1

1.

a) Explain with an example, how hidden form fields can be used to inject attacks. (5)

b) Identify the encoding/ hash function used.

i. b076be7758111786470391ec5081dcc9

ii. YjA3NmJlNzc1ODExMTc4NjQ3MDM5MWVjNTA4MWRjYzk= (5)

2.

a) What are hashes? What properties should a good hash function satisfy? (5)

b) Explain how URL headers can be modified to inject an attack. (5)

3. You are given a website to test. Explain with a flow chart, how will you obtain a local copy of the unique URLs of the wesite for offline testing. Also name the tools/commands used in each step.

(10)

Module 2

4. Consider the following URL. http://example.com/users/personalData/getDoc?readOnly=True. Write an algorithm for a cURL script to modify the URL to check for cross site scripting and directory traversal. Clearly mention the input to the algorithm. (10)

5. Write the algorithm for a Perl script to check if the application validates expired cookies. The script should modify the expiration date of the cookies that your application sends. (10)

6.

a) How can you impersonate a web browser or device for sending an HTTP request? (5)

b)
```
<form name="loginForm" action="loginCheck.php" method="post">
User Name: <input type="text" name="username"><br><br>
Password :  <input type="password" name="pwd"><br>
             <input type="submit" name="Submit" value="Login"> </form>.
```
Write a Perl script to submit the form content using 'Post' method. (5)

Module 3

7.

a) Explain with an example how out of order navigation can result in unwanted behavior of a web application. (5)

b) Give an example of how a predictable identifier can be modified to impersonate another person. (5)

P.T.O.

8. What is Ajax? Explain how to observe live Ajax requests, and modify them to send malicious requests. (10)

9.

a) Which are the different ways of storing/sending session information to a server? (4)

b) How all can the session expire and what are the security implications for each of these methods? (6)