Tribhuvan University
Institute of Science and Technology
2067
✡

Bachelor Level/ Third Year/ Fifth Semester/ Science
Computer Science and Information Technology (CSc. 301)
(Computer Networks)

Full Marks: 60
Pass Marks: 24
Time: 3 hours.

Candidates are required to give their answer in their own words as for as practicable.
Attempt all the questions.

Group 'A'

Long answer questions

Attempt all questions. **(2 x 10 = 20)**

1. Explain the principles of application layer protocols. What do you mean by file transfer?

OR

What are the main relationship between transport layer and network layer? What are the transport layer uses in Internet?

2. Explain the congestion control principle and its approaches.

Group 'B'

Short Answer Questions

Attempt any eight questions. **(8 x 5 =40)**

3. Explain the connection oriented and connectionless service.
4. Explain the working principle of DNS.
5. What do you mean by pipelined reliable data transfer protocol?
6. What do you mean by hierarchical routing?
7. Explain the multicasting routine and its applications.
8. Define Data link layer and its services.
9. Mention the types of multimedia networking applications.
10. What are the key components of network management architecture?
11. Explain the Asynchronous transfer mode (ATM).

Tribhuvan University
Institute of Science and Technology
2068
✡

Bachelor Level/ Third Year/ Fifth Semester/ Science — Full Marks: 60
Computer Science and Information Technology (CSc. 301) — Pass Marks: 24
(Computer Networks) — Time: 3 hours.

Candidates are required to give their answer in their own words as for as practicable.
Attempt all the questions.

Group 'A'

Long answer questions

Attempt all questions. **(2 x 10 = 20)**

1. Explain the OSI reference model.

OR

What do you mean by TCP? Explain the TCP structure.

2. Define DNS. Explain the DNS records and DNS messages.

Group 'B'

Short Answer Questions

Attempt any eight questions. **(8 x 5 =40)**

3. What do you mean by Internet Protocol stack?
4. Differentiate between transport layer and network layer.
5. Explain the principle of congestion control.
6. What do you mean by IP datagram fragmentation?
7. Explain the point to point protocol (PPP).
8. What do you mean by multicasting routing?
9. Explain the Internet Control Message Protocol (ICMP).
10. What are the various types of multimedia networking application?
11. What types of intra structure is needed for network management?

Tribhuvan University
Institute of Science and Technology
2069
✡

Bachelor Level/ Third Year/ Fifth Semester/ Science — Full Marks: 60
Computer Science and Information Technology (CSc. 301) — Pass Marks: 24
(Computer Networks) — Time: 3 hours.

Candidates are required to give their answer in their own words as for as practicable.
Attempt all the questions.

Group 'A'

Long answer questions

Attempt all questions. **(2 x 10 = 20)**

1. What are the seven layers of OSI model? Comparison between these seven layers.

OR

What do you mean by routing? Differentiate between Non-adaptive algorithm and adaptive algorithm.

2. Explain the congestion control algorithm with example.

Group 'B'

Short Answer Questions

Attempt any eight questions. **(8 x 5 =40)**

3. What do you mean by internet protocol stack?
4. Differentiate between DNS records and DNS messages.
5. Explain the pipelined reliable data transfer protocol.
6. Explain network service model.
7. Explain IPV4 addressing.
8. What do you mean by network address translator?
9. Explain on ALOHA and slotted ALOHA protocols.
10. What are the various applications of multimedia networking?
11. Explain the network management architecture with suitable diagram.

Tribhuwan University

Institute Of Science and Technology

Computer Networks

2070

Full Marks : 60

Pass Marks : 24

Time : 3 Hours

Group A

Attempt all questions : (2*10=20)

1.) Explain the functioning of 7 layers of OST model. What is the necessity of using 7 layers concept in OST Model?

OR

Explain the various layers of TCP/IP. Also, lists the protocols used in each layer.

2.) Explain how does CRC detect the errors with multiple bits? Given message is M(x) = x2+x4+x3=x2+1 and the generator is G(x) = x3+1. Show the actual bit string transmitted, suppose the third bit from the left is inverted during the transmission. Show how the error is detected at the receiver's end.

Group B

Attempt any eight questions : (8*5=40)

3.) What are sliding window protocol? Explain one-bit sliding window protocol with an appropriate diagram.

4.) Explain how slatted Aloha improves the performance of system over pure Aloha.

5.) Describe multimedia networking and its various applications.

6.) Why routing is important in a computer network? Differentiate between adaptive and non-adaptive routing algorithms.

7.) Differentiate between broadband and base band services.

8.) How does ATM differ from frame relay? List and briefly define the ATM service classes.

9.) Compare and contrast the IPV4 and the IPV6 header files. Do they have any fields in common?

10.) Define multiplexing. Discuss the need for multiplexing in network system.

11.) What is meant by "domain name"? How is a domain name translated to an equivalent IP address? Explain with the help of an example.

Tribhuwan University

Institute Of Science and Technology

Computer Networks

2071

Full Marks : 60

Pass Marks : 24

Time : 3 Hours

Group A

Attempt all questions : (2*10=20)

1.) Define protocol. Why do we need layered protocol architecture? Discuss each layer of TCP/IP protocol architecture in detail.

OR

Define transmission media. Differentiate between guided and unguided transmission media. Discuss each guided transmission in detail.

2.) What is routing? Discuss link state routing algorithm in detail.

Group B

Attempt any eight questions : (8*5=40)

3.) Explain client server system. How is it different from peer to peer system?
4.) Discuss HTTP in detail.
5.) Discuss the importance of multiplexing in data communication.
6.) Assume a class B network and divide it into four subnets. What is the value of new subnet mask.
7.) Discuss CRC as an error detection mechanism.
8.) Explain the importance of multimedia network.
9.) Why is network management an important task?
10.) What is congestion control? Why do we need it?
11.) Write short notes on :
    a.) DNS
    b.) Streaming audio and video

CSc.301-2072 ✡

Tribhuvan University
Institute of Science and Technology
2072
✡

Bachelor Level / Third Year /Fifth Semester/Science
Computer Science and Information Technology (CSc.301)
(Computer Networks)

Full Marks: 60
Pass Marks: 24
Time: 3 hours

Candidates are required to give their answers in their own words as for as practicable.
The figures in the margin indicate full marks.

Group A

Long Answer Questions:

Attempt all questions. (2×10=20)

1. Discuss the relationship between transport layer and network layer. Discuss TCP as a transport layer protocol along with its segment structure.

OR

What is transmission media? Discuss each transmission media in detail.

2. Why do we need routing algorithm? Discuss distance vector routing algorithm in detail.

Group B

Short Answer Questions:

Attempt any eight questions. (8×5=40)

3. What is connection oriented service? Differentiate it with connectionless service.
4. Discuss the working principle of DNS.
5. Why do we need multiplexing in data communication? Discuss.
6. What is subnetting? Assume a class C network and divide it into four subnets. What is the value of new subnet mask?
7. How does the system corrects error after error detection?
8. Discuss multimedia networking application.
9. Why is network management a challenging task?
10. Discuss the importance of congestion control in data communication.
11. Write short notes on:
    a) HTTP
    b) Backbone

CSc. 301-2073/74

Tribhuvan University
Institute of Science and Technology
2073

Bachelor Level / Third Year / Fifth Semester/Science
Computer Science and Information Technology (CSc.301)
(Computer Networks)

Full Marks: 60
Pass Marks: 24
Time: 3 hours

Candidates are required to give their answers in their own words as far as practicable.
The figures in the margin indicate full marks.

Group A

Long Answer Questions:

Attempt all questions. (2×10=20)

1. Explain the seven layers of OST model and compare between them.

OR

What do you mean by link state routing algorithm? Differentiate between IPv4 and IPv6.

2. Explain the purpose of subnet ting and also explain the subnet mark.

Group B

Short Answer Questions:

Attempt any eight questions. (8×5=40)

3. Explain the responsibilities of data link layer is the internet model.
4. What do you mean by TCP push operation?
5. Explain the Internet Control Message Protocol (ICMP).
6. Explain the point to point protocol (PPP) with example.
7. What down the techniques used in the 802.12 protocol for wireless networks?
8. Differentiate between ALOHA and slotted ALOHA protocols.
9. Discuss the idea used in public key encryption system.
10. What are the applications of multimedia networking?
11. Mention the intra structure for network management.

Tribhuvan University
Institute of Science and Technology
2067
✡

Bachelor Level/ Third Year/ Fifth Semester/ Science — Full Marks: 80
Computer Science and Information Technology (CSc. 303) — Pass Marks: 34
(Design and Analysis of Algorithm) — Time: 3 hours.

Candidates are required to give their answer in their own words as for as practicable.
The figures in the margin indicate full marks.

Attempt all the questions.

1. Explain Worst case, best case and average case of algorithm analysis with an example. (8)

2. What is recurrence relation? Find big-O of following recurrence using recurrence tree method.
   $T(n) = T(n/2) + 1 \quad n > 1$
   $= 1 \quad n = 1$ (2+6)

3. Make a tight big-O analysis of following code.

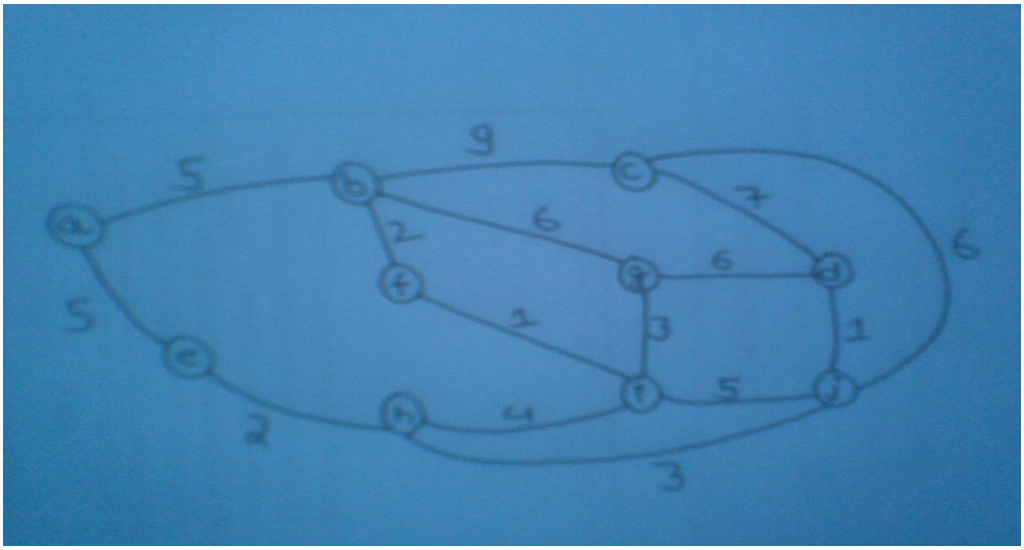
```
void main( )
{
        int m,n,i,j,a[ ], b[ ], c[ ];
        printf("Enter value of m and n");
        scanf("%d %d",&m, &n);
        for (i = 0; I < n; i++)
        {
                a[i] = i;
                b[i] = i*i;
                c[i]= -i;
        }
        for (j = 0; j < m; j++)
        {
                printf("%d\t %d\t %d\n", a(j), b(j), c(j);
        }
}
```
(8)

4. What is order statistics? How can you devise an algorithm that guarantee the selection of i^{th} order statistics in linear time? Write the algorithm of it and analyze it. (1+3+4)

5. What is the main idea of randomized algorithm? Write an algorithm quick sort and analyze it. (2+6)

6. Define greedy paradigm. How can you define Huffman algorithm is greedy algorithm? Explain. (2+6)

7. What is minimum spanning tree? Write the execution trace of the following graph to construct minimum spanning tree by prime algorithm.



(2+6)

8. Explain Graham's Scan algorithm to compute convex hull. (8)

9. Define the terms "Class P", "Class NP" and "NP - Completeness". (8)

10. What is the concept of dynamic programming? Find the longest common subsequence (LCS) between "XMJYAUZ" and "MZJAWXU". (2+6)

Tribhuvan University
Institute of Science and Technology
2068
✡

Bachelor Level/ Third Year/ Fifth Semester/ Science — Full Marks: 80
Computer Science and Information Technology (CSc. 303) — Pass Marks: 34
(Design and Analysis of Algorithm) — Time: 3 hours.

Candidates are required to give their answer in their own words as for as practicable.
The figures in the margin indicate full marks.

Attempt all the questions.

1. Write down the formal definition of big-oh, big-omega and big-thita notation with examples. (8)

2. What is recurrence relation? Find the big-O of following recurrence by using recurrence tree method.

   $T(n) = 2T(n/2) + n \quad n>1$
   $=1 \quad n=1$ (2+6)

3. Make a tight big-O analysis of following code segment.

```
void main( )
{
   int m, n, i, j, a[ ], b[ ];
   printf("Enter value of m and n");
   scanf("%d %d', &m, &n);
   for (i = 1,I <= m, i++)
        a[i] = i*i;
   for (j=1, j<=n; j++)
        b[j] = -j;
   for (i = 1,I <= m, i++)
        printf("%d", a[i]);
   for (j=1, j<=n; j++)
        printf("%d", b[j]);
}
```
(8)

4. What is linear data structure? Write down the algorithm of heap sort and find its complexity analysis. (2+6)

5. What is divide and conquer technique? Using this technique. Write an algorithm of quick sort then analyze it. (2+6)

6. What are the advantages of dynamic programming? Find Longest Common Subsequence (LCS) between "abbaab" and "aabaabb". (2+6)

7. What is shortest path problem? Explain Dijkstra's algorithm for shortest path problem. (2+6)

8. What is left turn and right turn? Give an algorithm for finding two lines segments intersect or not by using left turn and right turn. Does this algorithm works for all cases? Justify with example. (2+6)

9. Define the terms "Class P", "Class NP" and "NP Completeness". (8)

10. What is the concept of randomized algorithm? Write an algorithm of approx-vertex-cover problem and analyze it. (2+6)

Tribhuvan University
Institute of Science and Technology
2069
✡

Bachelor Level/ Third Year/ Fifth Semester/ Science — Full Marks: 80
Computer Science and Information Technology (CSc. 303) — Pass Marks: 34
(Design and Analysis of Algorithm) — Time: 3 hours.

Candidates are required to give their answer in their own words as for as practicable.
The figures in the margin indicate full marks.

Attempt all the questions.

1. Use RAM model to estimate the big-oh of the running time for following code segment for

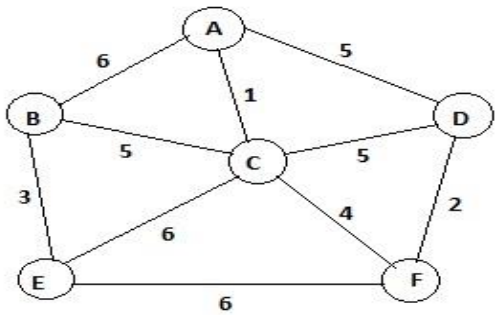
```
(i=1 ; i<n ; i++){
                small pos = i ;
                smallest = Array [small pos] ;
                for (j=i+1 ; j<=n ; j++) {
                        if (Array [j] < smallest){
                                small pos = j;
                                smallest = Array [small pos];
                        }
                }
                Array [small pos] = Array[i]
                Array [i] = smallest;
}
```
(8)

2. What do you mean by recurrence relation? Estimate the running time of algorithm given by following recurrence relations using master method.
   a. $T(n) = 4\,T(n/2) + n^3$
   b. $T(n) = 2\,T(n/2) + n$
   c. $T(n) = 3\,T(n/4) + n \log n$ (8)

3. Explain the quick sort algorithm with its complexity analysis. How randomized quick sort works efficiently even for worst case. (6+2)

4. Define order statistics. Write an algorithm that is able to select i^{th} largest element from an un-ordered list in linear time and analyze for its complexity. (2+6)

5. Sketch the Prim's algorithm for computing MST of a graph and analyze its complexity. Also trace the algorithm for the following graph. (2+6)

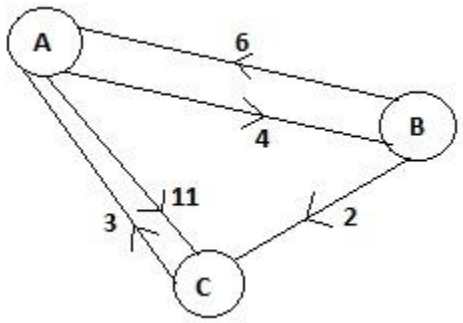


6. Give the job sequencing algorithm with deadlines. You have given 5 jobs with profit pi and deadline di as

   job i = { 1, 2, 3, 4, 5 }
   pi = { 20, 10, 5, 15, 1 }
   di = { 2, 1, 3, 2, 3 }

   Find the optimal job lists that can be executed in sequence with in their deadlines so as to maximize the profits. (4+4)

7. Explain and analyze the Floyd's warshall algorithm for all pair shortest path problem. Trace the algorithm for the following graph. (4+4)



8. What do you mean by left turn and right turn for given three points in 2D? Explain the method for computing the intersection of two line segment efficiently. (2+6)

9. Explain about class P, class NP and NP complete with suitable examples. (8)

10. Explain the Gram's scan algorithm with example to compute the convex hull of the set of points in 2D. (8)

Tribhuwan University

Institute Of Science and Technology

Design and Analysis of Algorithm

2070

Full Marks : 80

Pass Marks : 32

Time : 3 Hours

Attempt all questions :

1.) Explain the term Big-oh, Big-omega and Big-theta. Show that a function $f=3n^2+4n+7$ is big theta of n^2. (8)

2.) What do you mean by a recurrence relation? Solve the following recurrence relation using iterative expansion method (2+6)

a.) $$T(n) = \begin{cases} 2T(n/2)+1, & n>1 \\ 2, & n=1 \end{cases}$$

b.) $$T(n) = \begin{cases} 2T(n/2)+Kn, & n>1 \\ 1 & n=1 \end{cases}$$

3.) write an algorithm for quick-sort and trace out the algorithm for the following array A[ ] = { 16,7,15,14,18,25,55,32 }. (4+4)

4.) How can you solve the selection problem in linear time? Write the algorithm and analyze for its time complexity. (8)

5.) What is prefix code? You have given a message text having seven distinct characters {p,q,r,s,t,u,v} with frequency {40,20,15,12,8,3,2}. Trace the Huffman algorithm to build the free and obtain the optimum prefix codes for each characters. (2+6)

6.) Explain Prim's algorithm for computing the MST of a given graph and analyze it. Also verify the correctness of this algorithm. (5+3)

7.) Distinguish the main idea for divide and conquer approach with dynamic programming approach. Find the longest common subsequence between two sequences <A,B,C,B,D,A,B> and <B,D,C,A,B,A>. (2+6)

8.) Define convex hull in 2D. Explain the gram's scan algorithm for computing convex hull and analyze it. (2+6)

9.) Explain about the complexity classes P, NP and NP complete with suitable examples. (8)

10.) Explain Dijkstra's algorithm for computing the single source shortest path in a graph with suitable example. (8)

Tribhuwan University

Institute Of Science and Technology

Design and Analysis of Algorithm

2071

Full Marks : 80

Pass Marks : 32

Time : 3 Hours

Attempt all questions :

1.) Why do you need the algorithm analysis? Explain the best, worst and average case complexities with suitable example. (2+6)

2.) Explain the master method for solving the recurrence relations. Solve the following recurrence relations using this method. (2+3+3)

a.) T(n) = 3T(n/2) + n

b.) T(n) = 2T(n/4) + √n

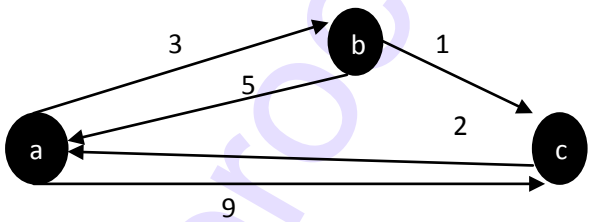
3.) Explain the divide and conquer approach for algorithm design. Design the binary search algorithm and analyze it's time complexity. (2+6)

4.) Explain the merge-sort algorithm with example and analyze its time complexity. (8)

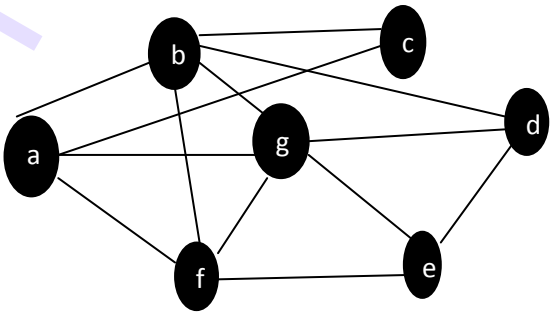
5.) What do you mean by a prefix code? How Huffman algorithm generates prefix codes? Explain with an example. (2+3+3)

6.) Discuss the 0/1 knapsack problem and how this problem can be solved? Explain the algorithm. (4+4)

7.) Explain the algorithm to find the all pair shortest path of a weighted connected graph. Trace the algorithm for the following graph. (3+5)



8.) Write an algorithm for depth first search. Use depth first search to find a spanning tree of the following graph. (3+5)



9.) Define the convex hull in 2D. Write the Grahm's scan algorithm for computing the convex hull of points in 2D and analyze its time complexity. (2+6)

10.) What do you mean by approximation algorithm? Write the algorithm for approximate the vertex cover of a connected graph with example. (2+6)

Tribhuvan University
Institute of Science and Technology
2072
✡

Bachelor Level / Third Year/ Fifth Semester/ Science
Computer Science and Information Technology (CSc.303)
(Design and Analysis of Algorithm)

Full Marks: 80
Pass Marks: 32
Time: 3 hours.

Candidates are required to give their answers in their own words as for as practicable.
The figures in the margin indicate full marks.

Attempt all questions.

1. Describe the best case and worst case complexity of an algorithm. Write algorithm for insertion sort and estimate the best and worst case complexity. [2+6]

2. Estimate the big Oh of the following recurrence relations using the iterative expansion method [4+4]

a) $T(n) = 2T(n/2) + k \quad , n>1$
$= 1 \quad , n = 1$

b) $T(n) = T(n/2) + kn \quad , n>1$
$= 1 \quad , n = 1$

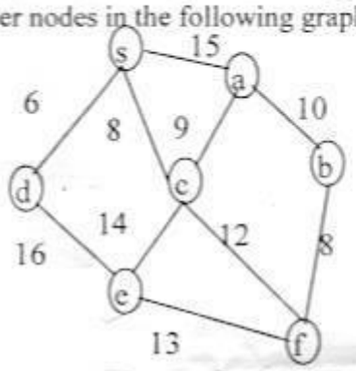
3. What is the worst-case of quick sort? Show that how quick sort can be made to run in optimal time in the worst case. [1+7]

4. Trace the heap-sort algorithm for the following data: *{16 ,41,18,99,74,20,17,25,10}.* [8]

5. What is prefix code? How Huffman algorithm generates the optimal prefix codes? Explain with suitable example. [1+3+4]

6. What do you mean by dynamic programming approach for design of algorithm? Write the algorithm for matrix chain multiplication and estimate its time complexity. [2+6]

7. Write the Dijkstra's algorithm for single source shortest path in a weighted connected graph. Find the shortest path from the node **s** to other nodes in the following graph. [4+4]



8. Write algorithm to compute the LCS of given two sequences. Trace the running of the algorithm to find the LCS of the sequences "XMJYAUZ" and be "MZJAWXU" [4+4]

9. Define the term diagonal, ear and mouth of a simple polygon. How can you determine the intersection of two line segment efficiently? Explain in detail. [3+5]

10. Discuss NP completeness. What is the role of approximation algorithms? Explain the algorithm for vertex cover of a graph with running example. [2+6]

CSc. 303-2073

Tribhuvan University
Institute of Science and Technology
2073

Bachelor Level / Third Year/ Fifth Semester/ Science
Computer Science and Information Technology (CSc.303)
(Design and Analysis of Algorithm)

Full Marks: 80
Pass Marks: 32
Time: 3 hours.

Candidates are required to give their answers in their own words as for as practicable.
The figures in the margin indicate full marks.

Attempt all questions.

1. Explain big-oh, big-omega and big-theta notations for computing analysis of algorithm with example. [8]

2. What do you mean by recurrence relation? Solve the following recurrence relation using master method. [2+3+3]

   a) $T(n) = 4T(n/2) + n^2$ $n>1$

   b) $T(n) = 9T(n/3) + n$ $n>1$

3. What is quick sort? Trace the following data using quick sort algorithm.
   A[]={99, 50, 60, 8, 5, 6, 20, 25, 40} [2+6]

4. What is Greedy paradigm? Write down the Greedy job sequencing algorithm. [2+6]

5. Write algorithm to computer Longest Common Subsequence of given two sequences. Compute the LCS of "COMPANY" and "COLONY". [4+4]

6. What is Flyod's algorithm? Write the details of Flyod's algorithm to find shortest path in a graph. [2+6]

7. What is convex hull? Describe the Graham's scan algorithm to compute convex hull. [4+4]

8. Describe the terms class-P, class-NP and NP-completeness. [8]

9. What is directed acyclic graph? How to find the shortest path from a vertex of directed acyclic graph? [2+6]

10. What is BST? Write the algorithm of insertion and deletion operation of BST. [2+6]

Tribhuvan University
Institute of Science and Technology
2067
✡

Bachelor Level/ Third Year/ Fifth Semester/ Science
Computer Science and Information Technology (CSc. 304)
(Artificial Intelligence)

Full Marks: 60
Pass Marks: 24
Time: 3 hours.

Candidates are required to give their answer in their own words as for as practicable.

Attempt all the questions. **(6 x 10 = 60)**

1. Define Artificial Intelligence (AI). Explain the behaviors of the AI. What do you mean by Turing Test? Explain it.

2. Why disjunctive normal form is required? Explain all the steps with examples.

3. "A person born in Nepal, each of whose parents is a Nepali citizen by birth, is a Nepali citizen by birth. A person born outside Nepal, one of whose parents is a Nepali citizen by birth, is a Nepali citizen by decent. Several developed countries have dual citizenship provision, but Nepal doesn't have that provision." Represent the above sentences in first-order logic and explain each step.

4. Differentiate between inference and reasoning. Why probabilistic reasoning is important in the AI? Explain with an example.

5. Justify that searching is one of the important part of AI. Explain in detail about depth first search and breadth first search techniques with an example.

6. Define Learning. Why learning frame work is required? Explain about learning frame with block diagram and examples.

7. What is Bayes' theorem? Explain its applications.

8. What is back propagation? Explain all the steps involved in the back propagation with an example.

9. How can you construct expert system? Explain knowledge engineering with a block diagram.

10. Define natural language processing. Explain the different issues involved in the natural language processing.

Tribhuvan University
Institute of Science and Technology
2068
✡

Bachelor Level/ Third Year/ Fifth Semester/ Science — Full Marks: 60
Computer Science and Information Technology (CSc. 304) — Pass Marks: 24
(Artificial Intelligence) — Time: 3 hours.

Candidates are required to give their answer in their own words as for as practicable.

Attempt all the questions. **(6 x 10 = 60)**

1. What is Artificial Intelligence (AI)? Describe your own criteria for computer program to be considered intelligent.

2. For each of the following agents, determine what type of agent architecture is most appropriate (i.e. table lookup, simple reflex, goal-based or utility based).

   a. Medical diagnosis system
   b. Satellite image analysis system
   c. Part-pricking robot
   d. Refinery controller

3. What is state space representation of problem? Represent the root finding problem having four cities in to state representation (you can choose any ordering of cities and links) and devise the complete problem formulation.

4. What is heuristic information? Suppose that we run a greedy search algorithm with h(n) – g(n) and h(n) = g(n). What sort of search will the greedy search follow in each case?

5. State whether the following sentences are valid, unsatisfiable, or neither.

   a. Smoke = > Smoke
   b. Smoke = > Fire
   c. (Smoke = > Fire) = > (~Smoke = > ~Fire)
   d. Smoke V Fire V ~Fire

6. Consider the knowledge base:

   "If it is hot and humid, then it is raining. If it is humid, then it is hot. It is humid"

   a. Describe a set of propositional letters which can be used to represent the knowledge base.
   b. Translate the KB into propositional letters using your propositional letters from part a.
   c. Is it raining? Answer this question by using logical inference rule with KB.

7. What do you mean by knowledge representation? Explain the characteristics of representation.

8. Define the Model-Based and Cased Based system. Discuss which system is suitable for the following problems.

    a. Electronic Circuit Testing
    b. Legal Reasoning
    c. Disease Recognition

9. What is Bayes' rule? Discuss the use of Bayes' rule for uncertain reasoning.

10. After your yearly checkup, the doctor has bad news and good news. The bad news is that you tested positive for a serious disease, and the test is 99% accurate (i.e. the probability of testing positive given that you have the disease is 0.99, as is the probability of testing negative if you don't have the disease). The good news is that this is a rare disease, striking only one in 10,000 people.

    a. Why is it good news that the disease is rare?
    b. What are the chances that you actually have the disease?

Tribhuvan University
Institute of Science and Technology
2069
✡

Bachelor Level/ Third Year/ Fifth Semester/ Science
Computer Science and Information Technology (CSc. 304)
(Artificial Intelligence)

Full Marks: 60
Pass Marks: 24
Time: 3 hours.

Candidates are required to give their answer in their own words as for as practicable.

Attempt all the questions. **(6 x 10 = 60)**

1. What do you mean by forward chaining? Why it is required? Explain it with two practical examples.

2. "System that think like humans" and "System that act like humans" are the part of artificial intelligence. Justify that statement with practical examples.

3. Why normal forms are required in AI? How do you convert to the disjunctive normal form? Explain all the steps with practical examples.

4. "A deductive system is sound if any formula that can be derived in the system is logically valid. Conversely, a deductive system is complete if every logically valid formula is derivable. All of the system discussed in this article are both sound and complete. They also share the property that it is possible to effectively verify that a purportedly valid deduction is actually a deduction; such deduction systems are called effective". Represent the above sentences in first-order logic and explain each step.

5. Justify that AI can't exist without searching. Explain in detail about any two types of informed search with practical examples.

6. Why do we require learning? Explain about learning framework with suitable block diagram and examples.

7. What do you mean by casual network? Explain it with practical application.

8. What is a Neural Network? Explain any one type of neural network with practical example.

9. Knowledge consists of facts, beliefs, and heuristics, justify it. Explain the advantages and disadvantages of an expert system.

10. Differentiate between natural language understanding (NLU) and natural language generating (NLG). Why we have to study natural language processing? Explain it.

Tribhuwan University

Institute Of Science and Technology

Artificial Intelligence

2070

Full Marks : 60

Pass Marks : 24

Time : 3 Hours

Attempt all questions :

1.) What is 'Turing Test' in Artificial Intelligence (AI)? Criticize the performance of the 'Turing Test' to measure the intelligence of the machine.
2.) Explain the uninformed search techniques with example.
3.) If we set the heuristic function h(n)=g(n) for both greedy as well A*. what will be effect in the algorithms? Explain.
4.) The minimax algorithm returns the best move for MAX under the assumption that MIN play optimally. What happens when MIN plays suboptimally?
5.) Translate the following sentence into first order logic :
    i.) "Everyone's DNA is unique and is derived from their parents' DNA".
    ii.) "No dog bites a child of it's owner".
    iii.) "Every gardener likes the sun".
    iv.) "All purple mushrooms are poisonous".
6.) Represent the following sentences into a semantic network .
    Birds are animals.
    Birds have feathers, fly and lay eggs.
    Albatross is a bird.
    Donald is a bird.
    Tracy is an albatross.

7.) What is an expert system? Explain the architecture and feature of rule-based expert system.
8.) What are conceptual graphs? Represent the following statements into conceptual graph.
    "King Ram marry Sita, the daughter of king Janak".
9.) What is machine learning? Explain the learning from analogy and instance based learning?
10.) What is Bayesian Network? Explain how Bayesian Network represents and inference the uncertain knowledge.

Tribhuwan University

Institute Of Science and Technology

Artificial Intelligence

2071

Full Marks : 60

Pass Marks : 24

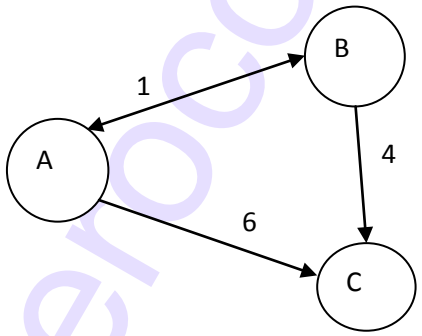
Time : 3 Hours

Attempt all questions :

1.) Define with suitable supporting statements and examples, "Artificial Intelligence is the system that act like humans".

2.) For each of the following agents, determine what type of agent architecture is most appropriate (i.e., table lookup, simple reflex, goal-based or utility-based).
   a.) Medical diagnosis system
   b.) Satellite imagine analysis system
   c.) Part-picking robot
   d.) Refinery controller

3.) Consider the following graph, steps cost is given on the arrow. Assume that the successors of a state are generated in alphabetical order, and that there is no repeated state checking. A is the starting node and C is goal node.



   a.) Of the four algorithms breadth-first, depth-first and iterative-deepening, which find a solution in this case?
   b.) Write sequence of node expanding by algorithm if finds solution.

4.) Define learning. Why learning frame work is required? Explain about learning frame work with block diagram and examples.

5.) Briefly describe the approaches of knowledge representation with example.

6.) Consider the following sentence :

[(food=>party) V (drinks=>party)] =>[(food^drinks) => party]

a.) Convert the right hand and left hand sides of main implication into CNF.

b.) Prove the validity of sentence using resolution.

7.) Convert the following sentence into predicate logic .

a.) “No dog bites a child of its owner”?

b.) “No two adjacent countries have the same color”?

8.) Why disjunctive normal form is required? Explain all the steps with examples.

9.) What is the difference between symbolic and non-symbolic AI? Represent the following knowledge in semantic network.

Robin is bird

Clyde is a Robin

Clyde owns a nest from spring 2014 to fall 2014

10.) Explain the steps of Natural Language Processing.

Tribhuvan University
Institute of Science and Technology
2072

✡

Bachelor Level / Third Year/ Fifth Semester/ Science
Computer Science and Information Technology (CSc.304)
(Artificial Intelligence)

Full Marks: 60
Pass Marks: 24
Time: 3 hours

Candidates are required to give their answers in their own words as for as practicable.
The questions are of equal marks.

Attempt all questions.

1. Define backward chaining. Explain the importance of backward chaining with two practical examples.

2. Justify that "System that think rationally" and "System that act rationally" are the part of artificial intelligence. Explain it with practical examples.

3. How do you convert to conjunctive normal form? Explain all the steps with examples.

4. "A key property of deductive systems is that the are purely syntactic, so that derivations can be verified without considering. any interpretation. Thus a sound argument is correct in every possible interpretation of the language, regardless whether that interpretation is about mathematics, economics, or some other area. The artificial intelligence deals with deductive system soundly". Represent the above sentences in first-order logic and explain each step.

5. Searching is an important part of AI, justify it. Explain any two types of blind search with suitable examples. How can you expand it to informed search?

6. What is learning by induction? Explain inductive learning process with example.

7. What do you mean by reasoning in belief network? Explain it with example.

8. Derive the mathematical model of neural network. Explain any one type of neural network with its algorithm.

9. Why do we require expert system structure? Draw the block diagram and explain it with practical example.

10. Explain the different steps involved in the natural language processing (NLP) with block diagram and examples.

CSc. 304-2073 ✡

Tribhuvan University
Institute of Science and Technology
2073

✡

Bachelor Level / Third Year/ Fifth Semester/ Science
Computer Science and Information Technology (CSc.304)
(Artificial Intelligence)

Full Marks: 60
Pass Marks: 24
Time: 3 hours

Candidates are required to give their answers in their own words as for as practicable.
The questions are of equal marks.

Attempt all questions.

1. Do you agree "the development of Artificial Intelligence has had some negative effect on the society"? If you agree list some of them and put your opinion in the support of development of Artificial Intelligence.
2. What is 'Turing Test' in AI? Criticize the performance of the 'Turing Test' to measure the intelligent of the machine.
3. Justify that searching is one of the important part of AI. Explain in detail about depth first search and breadth first search techniques with an example.
4. What is meant by admissible heuristic? What improvement is done in A* search than Greedy Search? Prove that A* search gives us optimal solution if the heuristic function is admissible.
5. Define a natural language processing. Explain the different issues involved in the natural language processing.
6. Differentiate between inference and reasoning. Why probabilistic reasoning in important in the AI? Explain with an example.
7. What is Bayesian network? Explain how Bayesian network represent and inference the uncertain knowledge.
8. Consider the following statements:

   Rabin likes only easy courses. Science courses are hard. All courses in the CSIT are easy. CSC 101 is a CSIT course.

   a) Translate the sentences into predicate logic.

   b) Convert your sentences into clausal normal form (CNF).
9. What are conceptual graphs? Represent the following statements into conceptual graph.

   King Ram marry Sita, the daughter of king Janak.
10. Define the Model-Based and Cased Based system. Discuss which system is suitable for the following problems

    i) Electronic circuit testing

    ii) Legal Reasoning

Tribhuvan University
Institute of Science and Technology
2067
✡

Bachelor Level/ Third Year/ Fifth Semester/ Science — Full Marks: 60
Computer Science and Information Technology (CSc. 302) — Pass Marks: 24
(Simulation and Modeling) — Time: 3 hours.

Candidates are required to give their answer in their own words as for as practicable.
The figures in the margin indicate full marks

Group A

Long Answer Questions:
Attempt any two questions. **(2×10=20)**

1. What is model? What are the different types of models? Give example for each.

2. What do you mean by Queuing system? Explain the characteristics of Queuing system with example.

3. Explain the independence test. A sequence of 1000 four digit numbers has been generated and an analysis indicates the following combinations and frequencies.

Combination (i)	Observed frequency (Oi)
Four different digits	560
One pair	394
Two pairs	32
Three digits of a kind	13
Four digits of a kind	1
	1000

Based on poker test, test whether these numbers are independent. Use $\alpha = 0.05$ and N = 4 is 9.49.

Group B

Short Answer Questions:
Attempt any eight questions. **(8×5=40)**

4. What are the advantages and disadvantages of simulation?

5. What do you mean by Pseudo random numbers?

6. Explain non-uniform random number generation.

7. Define a Markov chains and its application.

8. Use the linear congruential method to generate a sequence of three two-digit random integers.
   Let $X_0 = 29$, a = 9, c = 49 and m = 100

9. Why do we use verification and validation in simulation?

10. Explain the data and control statement in CSMP.

11. Explain the iterative process of calibrating a model.

12. Write short notes on:
    a) GPSS
    b) Server Utilization

Tribhuvan University
Institute of Science and Technology
2068
✡

Bachelor Level/ Third Year/ Fifth Semester/ Science — Full Marks: 60
Computer Science and Information Technology (CSc. 302) — Pass Marks: 24
(Simulation and Modeling) — Time: 3 hours.

Candidates are required to give their answer in their own words as for as practicable.
The figures in the margin indicate full marks

Group A

Long Answer Questions:
Attempt any two questions. **(2×10=20)**

1. Differentiate between dynamic physical models and static physical models with example.
2. Define the queuing system. Explain the elements of queuing system with example.
3. What is the main objective of gap test? Explain gap test algorithm with example.

Group B

Short Answer Questions:
Attempt any eight questions. **(8×5=40)**

4. Differentiate between discrete and continuous system.
5. What do you mean by Multi Server Queues?
6. What are the key features of Markov Chains?
7. Explain the congruence method of generating random numbers.
8. What do you mean by calibration and validation of models?
9. What are the Kendall notation of Queuing System?
10. What do you mean by Hybrid Simulation?
11. Use the mixed congruential method to generate a sequence of three two digit random numbers with Xo = 37, a = 7, c = 29 and m = 100.
12. Explain GPSS with example.
13. Write short notes on:
    a) Replication of Runs
    b) Simulation tools.

Tribhuvan University
Institute of Science and Technology
2069
✡

Bachelor Level/ Third Year/ Fifth Semester/ Science — Full Marks: 60
Computer Science and Information Technology (CSc. 302) — Pass Marks: 24
(Simulation and Modeling) — Time: 3 hours.

Candidates are required to give their answer in their own words as for as practicable.
The figures in the margin indicate full marks

Group A

Long Answer Questions:
Attempt any two questions. **(2×10=20)**

1. Define simulation. What are the various steps in simulation study? Explain.

2. Explain Markov Chains with example.

3. What are the properties of random number? The sequence of numbers 0.54, 0.73, 0.98, 0.11 and 0.68 has been generated. Use the Kolmogorov – Smirnov test $\alpha = 0.05$ to determine if the hypothesis that the numbers are uniformly distributed on the interval 0 to 1 can be rejected. (Note that the critical value of D for $\alpha = 0.05$ and $N = 5$ is 0.565).

Group B

Short Answer Questions:
Attempt any eight questions. **(8×5=40)**

4. When is simulation appropriate and when it is not?

5. What do you mean by server utilization?

6. What do you mean by non-uniform random number?

7. Why an auto-correlation test is needed in random number?

8. What do you mean by calibration and validation?

9. When is estimation method appropriate? Explain.

10. Explain Hybrid simulation with example.

11. Use the multiplicative congruential method to generate a sequence of four three-digit random numbers. Let $r_0 = 118$, $a = 4$ and $m = 1000$.

12. Explain the distributed lag model.

13. Write short notes on:
    a) Queuing discipline
    b) CSMP

Tribhuwan University

Institute Of Science and Technology

Simulation and Modeling

2070

Full Marks : 60

Pass Marks : 24

Time : 3 Hours

Group A

Attempt any two questions : (2*10=20)

1.) Why do we perform the analysis of simulation output? Explain how do you use simulation run statistics in the output analysis. (4+6)

2.) Describe the linear congruential method for random number generation. Use the Multiplicative congruential method to generate a sequence of four-three digit random integers, with seed=117, constant multiplier=43 and modulus=1000. (4+6)

3.) Consider that a machine tool in a manufacturing shop is turning out parts at the rate of one every 5 minutes. As they are finished , the parts go to an inspector, who takes 4±3 minutes to examine each one and rejects about 10% of the parts. Now, develop a block diagram and write the code for simulating the above problem using GPSS, and also explain the function of each block used in the block diagram in detail. (3+3+4)

Group B

Attempt any eight questions : (8*5=40)

4.) Differentiate between analytical models and numerical models. (5)

5.) Define congestion in a queuing system, and describe its major characteristics. (1+4)

6.) Describe the process of model building, verification, and validation in brief. (5)

7.) Explain, how do you update the clock time in system simulation. (5)

8.) What are the different phases that are employed in system simulation study? Explain in brief.(5)

9.) The sequence of numbers 0.54, 0.73, 0.97, 0.10, and 0.67 has been generated. Use the kolmogorov – smirnov test α=0.05 to determine if the hypothesis that the numbers are uniformly distributed on the interval [0,1] can be rejected. (Note that critical value of D for α=0.05 and μ=5 is 0.565). (5)

10.) Describe different types of statements, used in CSMP, with suitable examples. (5)

11.) "To simulate is to experiment". Justify it.

12.) Name the entities, attributes, activities, events, and state variables for the following systems :

- a.) Cafeteria
- b.) Inventory
- c.) Banking
- d.) A hospital emergency room
- e.) Communication

13.) Write short notes on :

a.) System, boundary and system environment
b.) Real time simulstion

Tribhuwan University

Institute Of Science and Technology

Simulation and Modeling

2071

Full Marks : 60

Pass Marks : 24

Time : 3 Hours

Group A

Attempt any two questions : (2*10=20)

1.) Explain the steps in simulation study. What are the limitations of simulation?
2.) Explain the Markovchains with examples and its applications.
3.) What do you mean by uniformity test? Explain the poker test with example.

Group B

Attempt any eight questions : (8*5=40)

4.) What are the types of simulation models?
5.) What are the elements of queuing system?
6.) What do you mean by pseudo random numbers?
7.) Explain the process of testing for auto-correlation test.
8.) Explain with example of calibration and validation of model.
9.) Explain the replication of runs.
10.) Use the multiplicative congruential method to generate of five digit random integers. X_0=118, a=45 and m=1000.
11.) What do you mean by simulation tool?
12.) Explain with example verification of simulation models.
13.) Write short notes on :
    a.) Discrete systems modeling
    b.) Feedback systems

Tribhuvan University
Institute of Science and Technology
2072

✡

Bachelor Level / Third Year/ Fifth Semester/ Science
Computer Science and Information Technology (CSc.302)
(Simulation and Modeling)

Full Marks: 60
Pass Marks: 24
Time: 3 hours

Candidates are required to give their answers in their own words as for as practicable.
The figures in the margin indicate full marks.

Group A

Long Answer Questions:

Attempt any two questions. (2×10=20)

1. What do you understand by analog method of system simulation? Explain it with suitable example. (3+7)

2. Define physical model. Explain the dynamic physical model with the help of suitable diagrams and expressions. (2+8)

3. Define frequency test for random numbers. Develop the Poker test for tour digit numbers, and use it to test whether a sequence of following 1000-four digit numbers are independent. (2+4+4)

(Use $\alpha = 0.05$ and $N = 4$ is 9.49)

Combination i	Observed frequency 0_i
Four different digits	565
One pair	392
Two pairs	17
Three like digits	24
Four like digits	2
	1000

Group B

Short Answer Questions:

Attempt any eight questions. (8×5=40)

4. Verification is concerned with building the "model right" and validation is concerned with building the "right model". Justify it with suitable reasons. (5)

5. How do you use estimation method in the analysis of simulation output? Explain in brief. (5)

6. Explain any four program control statements that are used in GPSS. (5)

7. Describe the rejection method of generating the random numbers. (5)

8. Define queuing discipline. Describe different types of queuing disciplines with example. (5)

9. How do you eliminate the effect of transient and initial bias in simulation output? (5)

10. Differentiate between clock time and simulation time used in system simulation. (5)

11. Describe the distributed lag model with the help of any practical example. (5)

12. Identify, with reasons, four different problems from your own experience that you think should be solved using digital simulation rather than analytically. (5)

13. Write short notes on: (2.5+2.5)
    a) Markov Chain
    b) Feedback systems

Tribhuvan University
Institute of Science and Technology
2073

Bachelor Level / Third Year/ Fifth Semester/ Science
Computer Science and Information Technology (CSc.302)
(Simulation and Modeling)

Full Marks: 60
Pass Marks: 24
Time: 3 hours

Candidates are required to give their answers in their own words as far as practicable.
The figures in the margin indicate full marks.

Group A

Long Answer Questions:

Attempt any two questions. (2×10=20)

1. Define and describe Markov chain in detail with the help of suitable examples. Also describe at least three areas of application of Markov chain.

2. Define and develop a Poker test for four-digit random numbers. A sequence of 10,000 random numbers, each of four digits has been generated. The analysis of the numbers reveals that in 5120 numbers all four digits are different, 4230 contain exactly one pair of like digits, 560 contain two pairs, 75 have three digits of a kind and 15 contain all like digits. Use Poker test to determine whether these numbers are independent> (Critical value of chi-square for α=0.05 and N=4 is 9.49).

3. Define congestion. Describe different types of components, characteristics and queueing disciplines of a queueing system.

Group B

Short Answer Questions:

Attempt any eight questions. (8×5=40)

4. Define model. Describe different types of simulation models in brief.

5. Describe the importance of differential/partial differential equations in simulation.

6. What do you understand by interactive system? Explain.

7. Define activity, event and state variables. List out the activities and events for the following systems; A. Super mark B. Inventory control C. Hospital.

8. Describe the process of calibration and validation in detail with example.

9. Draw and describe the different types of GPSS blocks that are used to gather statistics?

10. Differentiate between fixed time step and event to event model with the help of suitable examples.

11. Why do we need the analysis of simulation output? How do you use simulation run statistics in output analysis? Explain.

12. Write a computer program in C that will generate four digit random numbers using the multiplicative congruential method. Allow the user to input values of X_0, a, c and m.

13. Describe the basic nature of simulation in brief.

Tribhuvan University
Institute of Science and Technology
2067
✡

Bachelor Level/ Third Year/ Fifth Semester/ Science — Full Marks: 60
Computer Science and Information Technology (CSc. 313) — Pass Marks: 24
(Cryptography) — Time: 3 hours.

Candidates are required to give their answer in their own words as for as practicable.
The figures in the margin indicate full marks.

Attempt all the questions.

1. Answer the following questions in short **(Any Five)**. (5 × 2 = 10)

   a. List and briefly define types of cryptanalytic attacks based on what is known to the attacker.
   b. The larger the size of the key space, the more secure a cipher? Justify your answer.
   c. Explain the concepts of diffusion and confusion as used in DES.
   d. What are the characteristics of a stream cipher?
   e. How afraid should you be of viruses and worms?
   f. What do you mean when we say that a pseudorandom number generator is cryptographically secure?
   g. How many rounds are used in AES and what does the number of rounds depend on?

2.a) The notation $\mathbf{Z_n}$ stands for the set of residues. What does that mean? Why is $\mathbf{Z_n}$ not a finite field? Explain. (5)

2.b) Find the multiplicative inverse of each nonzero element in $\mathbf{Z_n}$. (5)

OR

Complete the following equalities for the numbers in GG(2):

1+1 = ?
1-1 = ?
-1 = ?
1*1 = ?
1*-1 = ? (5)

3.a) What are the steps that go into the construction of the 16 × 16 S-box lookup table for AES algorithm? (5)

3.b) In RSA algorithm, what is necessary condition that must be satisfied by the modulus n chosen for the generation of the public and private key pair? Also, is the modulus made public? (5)

OR

How is the sender authentication carried out in PGP? (5)

4.a) What sort of secure communication applications is the Kerberos protocol intended for? Explain. (5)

4.b) What is Fermat's Little Theorem? What is the totient of a number? (5)

5.a) Miller-Robin test for primality is based on the fact that there are only two numbers in $\mathbf{Z_p}$ that when squared give us 1. What are those two numbers? (5)

OR

What is discrete logarithm and when can we define it for a set of numbers? (5)

5.b) What is the Diffie-Hellman algorithm for exchanging a secret session key? (5)

6.a) We say that SSL/TLS is not really a single protocol, but a stack of protocols. Explain. What are the different protocols in the SSL\TLS stack? (5)

6.b) What is the relationship between "hash" as in "hash code" or "hashing function" and "hash" as in a "hash table" ? (5)

Tribhuvan University
Institute of Science and Technology
2068
✡

Bachelor Level/ Third Year/ Fifth Semester/ Science — Full Marks: 60
Computer Science and Information Technology (CSc. 313) — Pass Marks: 24
(Cryptography) — Time: 3 hours.

Candidates are required to give their answer in their own words as for as practicable.
The figures in the margin indicate full marks.

Attempt all the questions.

1. Answer the following questions in short **(Any Five)**. (5 X 2 = 10)

   a. All classical ciphers are based on symmetric key encryption. What does that mean?
   b. What makes Vigenere cipher more secure than say, the Playfair cipher?
   c. AES is a block cipher. What sized blocks are used by AES?
   d. When does a set become a group?
   e. What is the difference between the notation a mod n and the notation a ≡ b (mod n)?
   f. What is the difference between a virus and a worm?
   g. How do you define a prime number? When are two numbers A and B considered to be coprimes?

2.a) What do you mean by a "Feistel Structure for Block Ciphers"? Explain. (5)

2.b) Divide $23x^2 + 4x + 3$ by $5x + c$. assuming that the polynomials are over the field $\mathbf{Z}_7$. (5)

OR

What are the asymmetries between the modulo n addition and modulo n multiplication over $\mathbf{Z}_n$? (5)

3.a) Describe the "mix columns" transformation that constitutes the third step in each round of AES. (5)

3.b) What is the difference between algorithmically generated random numbers and true random numbers? (5)

4.a) Miller-Rabin algorithm for primality testing is based on a special decomposition of odd numbers. What is that? Explain. (5)

4.b) In RSA algorithm, the necessary condition for the encryption key e is that it be coprime to the totient of the modulus. But, in practice, what is e typically set to and why? (5)

5.a) What is meant by the strong collision resistance property of a hash function? (5)

5.b) How can public-key cryptography be used for document authentication? (5)

OR

What seems so counterintuitive about the counter mode (CTR) for using a block cipher?

6.a) What is the role of the SSL Record Protocol in SSL/TLS? Explain. (5)

OR

How many layers are in the TCP/IP protocol suite for internet communications? Name the layers. Name some of the protocols in each layer.

6.b) What does PGP stand for? What is it used primarily for? And what are the five services provided by the PGP protocol? (5)

Tribhuvan University
Institute of Science and Technology
2069
✡

Bachelor Level/ Third Year/ Fifth Semester/ Science — Full Marks: 60
Computer Science and Information Technology (CSc. 313) — Pass Marks: 24
(Cryptography) — Time: 3 hours.

Candidates are required to give their answer in their own words as for as practicable.
The figures in the margin indicate full marks.

Attempt all the questions.

1. Answer the following questions in short (**any five**): (5 x 2=10)

   a. How monoalphabetic substitution differs from polyalphabetic. Briefly define with suitable example.
   b. What are the components of authentication system? Give an example of authentication system.
   c. What do you mean by avalanche effect?
   d. How chosen plaintext attack differs from chosen ciphertext attack?
   e. What do you mean by multiplicative inverse? Find multiplicative inverse of each nonzero elements in Z_{11}.
   f. Even though we have a strong algorithm like 3-DES, still AES is preferred as a reasonable candidate for long term use. Why?
   g. Give an example for a situation that compromise in confidentiality leads to compromise in integrity.

2.a) Consider a Deffie-Hellman scheme with a common prime p = 11 and a primitive root g = 2.

   i. Show that 2 is a primitive root of 11.
   ii. If user A has public key $Y_a = 9$, what is A's private key X_a?
   iii. If user B has public key $Y_b = 3$, what is shared key K, shared with A. (2 X 3=6)

2.b) Construct a playfair matrix with the key "*KEYWORD*". Using this matrix encrypt the message "*WHY DON'T YOU*". (4)

3.a) How Trojan horse differs from viruses? Discuss about possible types of Trojan horses. (2+3)

3.b) Does Kerberos protocol ensures authentication and confidentiality in secure system? Explain. (5)

4.a) How Hash functions differ from MAC? Given a message m, discuss what arithmetic and logical functions are used by MD4 to produce message digest of 128 bits. (2+4)

4.b) Discuss the five principle services provided by PGP protocol. (4)

5.a) What is the purpose of S-Boxes in DES? Prove that DES satisfies complementation property. (6)

5.b) Given the plaintext "ABRA KA DABRA", compute the ciphertext for (4)

i. The Ceaser cipher with key = 8
ii. The Railfence cipher with rails = 3

6.a) What do you mean by digital signature? How digital signatures can be enforced using encryptions? Illustrate with an example. (1+5)

6.b) Determine whether the integers 105 and 294 are relatively prime. Explain your answer using Euclidean algorithm. (4)

CSc. 313-2070✡

Tribhuvan University
Institute of Science and Technology
2070

✡

Bachelor Level / Third Year /Fifth Semester/Science
Computer Science and Information Technology
(CSc. 313 – Cryptography)

Full Marks: 60
Pass Marks: 24
Time: 3 hours.

Candidates are required to give their answers in their own words as for as practicable.
The figures in the margin indicate full marks.

Attempt all questions.

1. Answer the following questions in short **(any five)**: (5x2=10)

   (a) Difference between monoalphabetic substitution ciphers and polyalphabetic substitution ciphers.

   (b) What are the two building blocks of all classical ciphers?

   (c) DES encryption was broken in 1999. Does that make this an unimportant cipher? Why do you think that happened?

   (d) What does a field have, that an integral domain does not? Why is $\mathbf{Z}_n$ not an integral domain?

   (e) Does a field contain a multiplicative inverse for every element of the field?

   (f) What are the four steps that are executed in a single round of AES processing?

   (g) What is a hash code? Why can a hash function not be used for encryption?

2. (a) What is Euclid's algorithm for finding the GCD of two numbers? Explain. (5)

OR

What is Euler's theorem? What is the totient of a prime number?

   (b) Calculate the result of the following if the polynomials are over GF(2): (5)
   $(x4 + x2 + x + 1) + (x3 + 1)$
   $(x4 + x2 + x + 1) - (x3 + 1)$
   $(x4 + x2 + x + 1) \times (x3 + 1)$
   $(x4 + x2 + x + 1) / (x3 + 1)$

3. (a) Let's go back to the first step of processing in each round of AES. How does one look up the 16x16 S-box table for the byte-by-byte substitution? (5)

   (b) What do you mean by man-in middle attack? Is man-in-middle attack possible in Deffie-Hellman. How? (5)

4. (a) There are two aspects to a secure communication link: authentication and confidentiality. How do you understand these two words? Does the Kerberos protocol give us both? (5)

   (b) Miller-Rabin test says that if a candidate integer n is prime, it must satisfy one of two special conditions. What are those two conditions? (5)

5. (a) How do you create public and private keys in the RSA algorithm fo (5)

OR

What are the notions Public Key Ring and Private Key Ring in PGP?

(b) What is the difference between a connection and a session in SSL/TLS? Can a session include multiple connections? Explain the notions "connection state" and "session state" in SSL/TLS. What security features apply to each? (5)

6. (a) How hash functions differ from MAC? Discuss how data integrity can be achieved from either of them. (5)

(b) What is a certificate and why are certificates needed in public key cryptography? (5)

Tribhuvan University
Institute of Science and Technology
2071

✡

Bachelor Level / Third Year /Fifth Semester/Science
Computer Science and Information Technology (CSc.313)
(Introduction to Cryptography)

Full Marks: 60
Pass Marks: 24
Time: 3 hours

Candidates are required to give their answers in their own words as far as practicable.
The figures in the margin indicate full marks.
Attempt any ten questions.

1. Answer following questions in short (**any five**). [5x2=10]
   a. Suppose a key logger program intercepts user password and is used to modify the user account. Now, justify whether it's a violation of confidentiality, integrity, or availability or some of combination of them.
   b. How zombies differ from logic bombs?
   c. Mention the advantages of using stream ciphers over block ciphers.
   d. What does Euler Totient Theorem states? What is the value of Totient(15)?
   e. Differentiate session keys from interchange keys.
   f. How Message Authentication Codes differ from Hash Functions?
   g. Briefly describe SubBytes and ShiftRows in AES.

2. a. In public key cryptosystem, each of the communicating parties, in general, should know the public keys of each other before attempting security encryptions. How this can be achieved? Write a Public Key Authority Protocol for public-key distribution among any two users. [4]
   b. How Kerberos Version 4 differs from Kerberos Version 5? How once per type of service approach is ensured by Kerberos Protocol. [6]

3. a. Configure a Vignere table for the characters from A-H. Use the table to encrypt the text DAD CAFÉ EACH BABE using the key FADE. [4]
   b. Mention the details of logical operations used in MD4. How the Majority function in Pass 1 of MD4 works? [6]

4. a. Encrypt the message "help" using the Hill cipher with the key $\begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$. Show your calculations and the result. [4]
   b. What do you mean by arbitrated digital signature? How signatures are generated using Digital Signature System? [6]

5. a. In a RSA system, a user Named Alice has chosen the primes 7 and 11 to create a key pair. Compute the public key (e_{Alice}, n) and the private key (d_{Alice}, n). Now encrypt the message = "bye" using the public key of Alice. [6]
   b. How Transport Mode of IPSec Operation differs from the Tunnel mode? [4]

6. a. How subkeys are generated in DES encryption procedure? Write a protocol for decrypting ciphertext using DES. [6]
   b. How Jailing and Backoff can be used to demotivate online dictionary attack in authentication system. [4]

CSc. 313-2072 ✡

Tribhuvan University
Institute of Science and Technology
2072

✡

Bachelor Level / Third Year /Fifth Semester/Science
Computer Science and Information Technology
(CSc. 313 – Cryptography)

Full Marks: 60
Pass Marks: 24
Time: 3 hours.

Candidates are required to give their answers in their own words as for as practicable.
The figures in the margin indicate full marks.

Attempt all questions.

1. Answer the following questions in short **(any five)**: (5x2=10)

   (a) What does Euler Totient function means? What will be the value of PHI(119).

   (b) What properties does a good hash function should have?

   (c) What is the purpose of S-Box in DES?

   (d) Define each of the terms confidentiality, integrity and availability.

   (e) What do you mean by primitive root of a prime number p? Is 3 a primitive root of 7?

   (f) Describe the concept behind public key infrastructure.

   (g) What are the possible phases that a virus can go through, during its life cycle.

2. (a) In a RSA system, a user has chosen the primes 5 and 19 to create a key pair. The public key is {e = 5, n = ?} and the private key is {d = ?, n = ?}. Decide the private key {d, n}. Show encryption and decryption process for the message "TOGA". (6)

   (b) Encrypt the message "MEET ME TONIGHT" using the Hill cipher with the key $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$.
   Show your calculations and the result. (4)

3. (a) Differentiate between SSL Session and SSL Connection. How SSL Record Protocol provides confidentiality and message integrity. (2+3)

   (b) What basic arithmetic and logical functions are used in SHA-1? (5)

4. (a) Briefly describe about MixColumns and AddRoundKey stages in AES. How many bytes in a state are affected by ShiftRows round? (5+1)

   (b) List the participants of Secured Electronic transaction (SET). Discuss the key features of SET. (4)

5. (a) In which situation using Kerberos system seem to be good? Describe what the major components of Kerberos system are. (2+4)

   (b) Given the plaintext "LOST IN PARADISE", compute the ciphertext for
   (i) The Ceaser cipher with key = 5
   (ii) The Railfence cipher with rails = 4 (4)

6. (a) Differentiate between direct digital signature and arbitrated digital signature. How signing and verifying process is done in Digital Signature Standard. (2+4)

   (b) What do you mean by Man-in-Middle attack? Is man in middle attack possible in Diffie-Hellman algorithm for key exchange? How? (4)