Institute of Information Technology (IIT)
Jahangirnagar University
4th Year 2nd Semester B.Sc (Hons.) Final Examination 2021
Course: ICT-4259 (Computer Network Security)

Time: 3 Hours **Full Marks: 60**

Answer any FIVE questions
All parts of a particular question must be answered consecutively

---

1. a) Distinguish between threat and attack. Explain three key concepts of the CIA triad. [4]
   b) List and briefly define categories of security mechanisms. [3]
   c) 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. [5]
      i) A student maintaining a blog to post public information.
      ii) An examination section of a university that is managing sensitive information about exam papers.
      iii) An information system in a pathological laboratory maintaining the patient's data.
      iv) A student information system used for maintaining student data in a university that contains both personal, academic information and routine administrative information (not privacy related). Assess the impact for the two data sets separately and the information system as a whole.
      v) A university library contains a library management system, which controls the distribution of books among the students of various departments. The library management system contains both the student data and the book data. Assess the impact for the two data sets separately and the information system as a whole.

2. a) What is a KDC? How can Alice send a confidential message to Bob using the KDC? [3]
   b) What does 'symmetric-key agreement' mean? Illustrate the processes of creating a symmetric-key between Alice and Bob using Diffie-Hellman Key Agreement protocol. [3]
   c) What is Kerberos and why it is named so? Describe the function of each servers involved in Kerberos protocol. [3]
   d) What are the approaches to distribute a public key? What is a digital certificate and what information it carries? [3]

3. a) What does authentication mean? Briefly describe three types of factors that are used for authentication. [3]
   b) A message can be authenticated either by hash code or MAC code. Give proper illustration for any one of these two methods. [3]
   c) Illustrate the processes of verification by hashing the fixed password approach. [3]
   d) List several attacks while authentication is done by fixed password. What are the benefits of one-time password over fixed password for verification? [3]

4. a) Illustrate the encryption algorithm of DES.
   b) Perform encryption and decryption using the RSA algorithm, for the following:
      i. p = 3; q = 11, e = 7, M =31 [4]
      ii. p = 5; q = 11, e = 3, M =9 [4]
   c) Analyze and explain the various techniques an attacker can use to perform a man-in-the-middle attack on a Wi-Fi network and evaluate the potential impact on resources of the network and its users. [4]

i) What can we say about f(x, y)?
ii) Propose

5. a) Illustrate the general idea behind symmetric-key and asymmetric-key cryptography.
b) What services are provided by cryptography? How does asymmetric-key cryptography prove the authenticity of the message originator? [3]
c) Suppose you are the network administrator of an organization. To provide confidentiality of your organization's data, you have to choose either symmetric-key or asymmetric-key cryptosystem. Which system do you want to choose for the organization and why? [4]
d) Which components a cryptographic process must have? Three Pass Protocol can be used to send sensitive information across an insecure network. Give a postal analogy. [2]

6. a) An encryption key used in a transposition cipher is given as 4 1 5 3 2. Determine the corresponding decryption key and then decrypt the message "**GLHUA ITSRE BTEEH ESDMT NIEIC**" using keyed transposition cipher with the decryption key you determined. [3]
b) What are the three steps in which encryption or decryption is done in columnar transposition cipher? Encrypt the message "**The enemy of my enemy is my friend**" using Columnar transposition cipher with the help of encryption key as 41532. [3]
c) Encrypt the message 'crypto' using **any TWO** of the following substitution ciphers. (Ignore the space between words and use modulo 26). Decrypt the message to get the original plaintext. [3]
(i) Affine cipher with key = (11, 9) [$11^{-1} = 19$]
(ii) Autokey cipher with initial key = 12
(iii) Vigenere cipher with keyword = 'pabna'
(iv) Playfair cipher with the keymatrix you consider
d) List two types of traditional symmetric-key ciphers. Suppose you want to encrypt a message using 33 modulus. What will be the possible key domain if Affine cipher is used? [3]

7. a) What is binary operation? Is not division a binary operation? Express the following set of integers in set notation: [3]
(i) Set of all positive integers
(ii) Set of all non-negative integers
(iii) Set of additive inverse in 10 modulus
(iv) Set of multiplicative inverse in 10 modulus
b) What does Z_{13} and Z^*_{13} mean? Using Euler's Phi-Function, determine the number of elements in- [3]
i) Z^*_{59} ii) Z^*_{64} iii) Z^*_{33} iv) Z^*_1
c) Assume that A and B are two integers in N modulus. Write the appropriate condition such that - [3]
(i) A is the multiplicative inverse of B
(ii) A is the additive inverse of B.
Prove using extended Euclidean algorithm that the multiplicative inverse of **10** does not exist in 26 modulus.
d) When two integers X and Y are called co-prime? Find the result of the following operations: [3]
(i) 0 mod N (ii) -15 mod 8 (iii) 35 mod 29 (iv) N mod N
[Here, N is a positive integer].

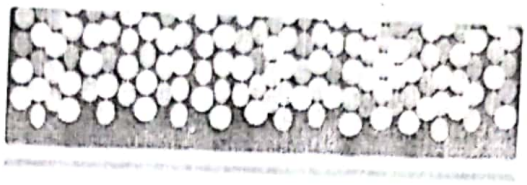
Institute of Information Technology
Jahangirnagar University
4th Year 2nd Semester B.Sc (Hons.) Final Examination, 2021
Subject: Information Technology
IT4201: Human Computer Interaction

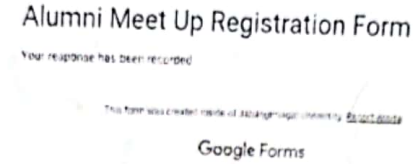
Time: 3 Hours | Full Marks: 60

Answer any **Five (05)** from the following questions. Figures at the right indicate the marks.

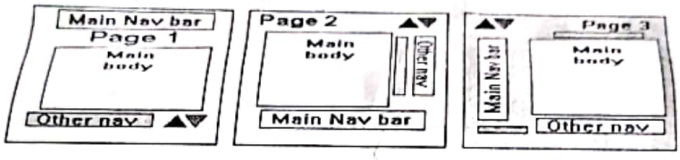
1. **a)** List and explain important human characteristics in designing user interface and explain the response of user for a poor design. 3

b) i) 2+2





ii)



Do the above two figures satisfy the principles of HCI? Justify your answer by relating to two principles of it.

c) Illustrate the memory whose memory access time is about 0.1 second with its different types using examples 5

2. **a)** Suppose, you are thinking about a topic and how to reach a conclusion using your conscience and knowledge. For doing it, which type of thinking will you utilize? Explain that with its classification and examples. 6

b) List and explain the principles of user interfaces design 3

c) How to achieve "user-friendliness" in computer design? Can you suggest 5 such designs? 3

3. **a)** Suppose you want to capture a picture in your cell phone and execute your intention. Explain your interaction with respect to Donald Norman's model. 6

b) Discuss about the four golden rules of design with examples. 6

4. **a)** Suppose you want to develop a web application on getting the live cricket update. From a usability perspective, what things you will consider when working on it. 2

b) Suppose your client wanted to have a prototype of the live cricket update web application. Briefly write down the techniques you will follow in creating the prototype. 4

c) Compare between standards and guidelines with examples. 3+3

5. a) i)

```
repeat
  read-event(task)
  case myevent.type
     type_1:
        do type_1 processing
     type_2:
        do type_2 processing
  ..... ..... ..... ..... ..... .....
     type_n:
        do type_n processing
  end case
end repeat
```

ii)

```
void main(String [] args) {
  Menu menu = new Menu();
  menu.setOption("Save");
  menu.setOption("Quit");
  menu.setAction("Save",mySave)
  menu.setAction("Quit",myQuit)
    ...
}
```

```
int mySave (Event e) {
}
```

```
int myQuit (Event e) {
}
```

Explain the working procedure of the above examples depending on its respective paradigms. 3+3

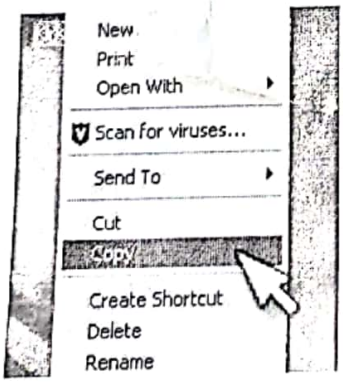
b) Suppose you want to develop a web application on getting the live cricket update. Explain with example how you will divide the file works using MVC and PAC?

6. a) Briefly discuss the universal design principles with examples. 7

b) Discuss about cognitive walkthrough and heuristic evaluation approaches. 5

7. a) "Consider a company that wants to develop a wireless information system to help tourists with personal digital assistants (PDAs) at Cox's Bazar Airport.", develop a conceptual model for this system. Draw it. 3

b) Consider the following figure and explain it according to BNF. 5



c) *Explain Fitt's Law. Suppose 60 and 40 are the constant values of a monitor. 160 be the distance from the starting point to the target and 40 be the width of the target along the axis of motion. Calculate the time to move the cursor using Fitt's Law.* 2+2

INSTITUTE OF INFORMATION TECHNOLOGY
JAHANGIRNAGAR UNIVERSITY
4TH YEAR 2ND SEMESTER FINAL EXAMINATION-2021

COURSE CODE: IT-4203 COURSE TITLE: WIRELESS AND MOBILE COMMUNICATIONS
TOTAL MARKS: 60 TIMES: 3 HOURS

ANSWER ANY FIVE (5) QUESTIONS

1. a) Distinguish between frequency selective and at fading. 2
   b) A telephone operator has found that there is a high blocking probability in a base station. In addition, the coverage area of that BS required to be improved. Please explain with illustration, how can we improve the Coverage and Capacity of the Systems? 4
   c) A total of 24 MHz of bandwidth is allocated to a particular FDD cellular telephone system that uses two 30 kHz simplex channels to provide full duplex voice and control channels. Assume each cell phone user generates 0.1 Erlangs of traffic. Assume Erlang B is used. 6
      i. Find the number of channels in each cell for a four-cell reuse system.
      ii. If each cell is to offer capacity that is 90% of perfect scheduling, find the maximum number of users that can be supported per cell where omnidirectional antennas are used at each base station.
      iii. What is the blocking probability of the system in (ii) when the maximum number of users are available in the user pool?
      iv. If each new cell now uses 120 sectoring instead of omnidirectional for each base station, what is the new total number of users that can be supported per cell for the same blocking probability as in (iii)?
      v. If each cell covers five square kilometers, then how many subscribers could be supported in an urban market that is 50km×50km for the case of omnidirectional base station antennas?
      vi. If each cell covers five square kilometers, then how many subscribers could be supported in an urban market that is 50km×50km for the case of 120 sectored antennas?

2. a) Hand-off Provides continuity of communication across cells. Explain the statement. Why should we provide a higher priority to handoff calls? 3
   b) Explain Spread spectrum multiple access (SSMA). When a user will experience "near-far" problem for SSMA? How can it be mitigated? 3
   c) In the North American Narrowband TDMA cellular system, the one-way bandwidth of the system is 12.5 MHz. The channel spacing is 30 kHz, and there are 395 total voice (data) channels in the system. The frame duration is 40 ms, with 8 time slots per frame. The system has an individual data rate of 16.2 kbps in which the speech w/ error protection has a rate of 13 kbps. Calculate the efficiency of the TDMA system. 3
   d) "Small-scale fading is detrimental in radio communication systems." How? Explain 3

3. a) Calculate Error rate for Quadrature Phase Shift Keying. 3
   b) Explain Friis Free Space Propagation Model. Find the far field distance for an antenna with maximum dimension of 1 m and operating frequency of 900 MHz 3
   c) How OFDM Subcarriers Work? 3
   d) What are main limitations of CSMA? How can you eliminate it? Many of the wireless applications use CSMA/CA protocol for their medium access technique, why? 3

4. a) Calculate the received power at a distance of 3 km from the transmitter if the path – loss exponent γ is 4. Assume the transmitting power of 4 W at 1800 MHz, a shadow effect of 10.5 dB, and the power at reference distance (d_0=100m) of -32 dBm. What is the allowable path loss? 3
   b) Assuming the speed of a vehicle is equal to 60 mph(88ft/sec), carrier frequency, fc=860 MHz, and rms delay spread τ_d 2 μ sec, calculate coherence time and coherence bandwidth. At a coded symbol rate of 19.2 kbps (IS-95) what kind of symbol distortion will be experienced? What type of fading will be experienced by the IS -95 channel? 3

c) "Doppler shift is the random changes in a channel introduced as a result of a mobile user's mobility" Explain the statement. Consider a transmitter which radiates a sinusoidal carrier frequency of 1850 MHz. For a vehicle moving 60 mph, Compute the received carrier frequency if the mobile is moving directly towards the transmitting and moving away from the transmitter. 3

d) Calculate S/I ratio for 3 and 6 sector cases when cluster size is 7 and compare S/I for both cases 3

5. a) Distinguish among various data networks in terms of deployed techniques and features. 4

b) We have seen our data service in the mobile phone always switches from "LTE" to [4] "H+" to "E" and vice versa. This means, we are getting the signals from different data services in the same location. Draw a functional block representation which shows the overlay structures of 2G, Edge, 3G, 4G. 4

c) The near-far problem always exist in the CDMA and it is a challenge for the system designer. What is near-far problem? Does the problem exist in GSM? Explain the WCDMA handover and power control. 4

6. a) In GSM, protection from unauthorized access is achieved through strong authentication procedures that validate the true identity of subscriber before he or she is permitted to receive service. Explain the relevant call flows for the authentication procedures showing the graphical direction. 3

b) Base Station is referred as Node-B and control equipment for Node-B's is called Radio Network Controller (RNC) as if the BSC of GSM. Explain the functions of these equipments. 3

c) Fixed Channel Allocation does not solve "hot spot" problem or localized traffic congestion. How? explain 2

d) We consider a cellular system in which total available voice channels to handle the traffic are 960. The area of each cell is 6 km² and the total coverage area of the system is 2000 km². Calculate (i) the system capacity if the cluster size, N is 12 and (ii) the system capacity if the cluster size is decreased to 7. Does decreasing the reuse factor N increase the system capacity? Explain 4

7. a) Consider a GSM system with a one-way spectrum of 12.5 MHz and channel spacing of 200 kHz. There are 3 control channels per cell and reuse factor is 7. Assuming an Omnidirectional antenna with 6 interferers in the first tier and a slop path loss of 40 dB/decade, calculate the number of calls per hour per cell site with 2% blocking during the system busy hour and an average call holding time is 120 seconds, The GSM uses 8 voice channels per RF channel. 4

b) Discuss two different types of handoff algorithms. Draw the flow chart or steps involved in the handoff process. 3

c) Explain some important features of WiMAX and LTE Network. 3

d) Briefly explain 4 important weakness of 5G Technology 2

Institute of Information Technology
Jahangirnagar University
4th Year 1st Semester B.Sc (Hons.) Final Examination, 2021
Subject: Information Technology
IT4107: Parallel and Distributed System

Time: 3 Hours | Full Marks: 60

Answer any **Five (05)** from the following questions. Figures at the right indicate the marks.

1. a) If you are planning to design a distributed system where the computers will be resided in different geographical locations what consequences you must be considered? 3
   b) How grid system differs from cluster system in distributed environment? Explain. 2
   c) Describe the challenges that any designer who is planning to design a distributed system must consider before start designing the system. 5
   d) How the traditional client-server model can be modified in distributed system? 2

2. a) An experimental file server is up 3/4 of the time and down 1/4 of the time, due to bugs. How many times does this file server have to be replicated to give an availability of at least 99%? 3
   b) i. Describe how connectionless communication between a client and a server proceeds when using sockets. and 3
      ii. Is a server that maintains a TCP/IP connection to a client stateful or state-less?
   c) [illegible] to time synchronize. The link from A to B takes 20ms but these numbers are not known to the computers. They synchronize using *Cristian's algorithm* in one round. Node A's time is 500 and Node B's time is 632. Node A starts the protocol. At the completion of the protocol what time does Node A believe it is? 4
   d) *Briefly describe the roles of middleware in a distributed system?* 2

3. a) i. Dependable systems are often required to provide a high degree of security. Why? 4
      ii. Consider the behavior of two machines in a distributed system. Both have clocks that are supposed to tick 1000 times per millisecond. One of them actually does, but the other ticks only 990 times per millisecond. If UTC updates come in once a minute, what is the maximum clock skew that will occur?
   b) What is called bully algorithm? What are the applications of bully algorithm in distributed system? 2
   c) **Scenario.** The Bully Algorithm solves the leader election problem in a synchronous system with process crashes and recoveries. Suppose the Bully Algorithm is used in an asynchronous system where processes may crash and may recover. Before the algorithm is executed, the system administrator determines the timeouts T and T' based on observed message and processing latencies over a short period of time. The algorithm is configured to use these selected timeouts. 4
      i. Describe an execution of the Bully algorithm (in this asynchronous system model with N > 2) that leads to more than one process declaring itself the leader. (N: nodes)
   d) What is stub? How are stubs generated? 2

4. a) Consider a URL as www.mail.yahoo.com/mail/inbox.html . A name resolver may resolve the name using either iterative or recursive way. Which one is better in your opinion? Justify why. 4
   b) Why global clock cannot be imposed in distributed system? What alternate solution Lamport provided regarding this problem? Explain. 4
   c) Make a brief comparison among mutual exclusion algorithms. 4

5. a) i. What is three-tiered client-server architecture?
ii. Does it make sense to implement persistent asynchronous communication by means of RPCs?

b) In this problem you are to compare reading a file using a single-threaded file server and a multithreaded server. It takes 15 msec to get a request for work, dispatch it, and do the rest of the necessary processing, assuming that the data needed are in a cache in main memory. If a disk operation is needed, as is the case one-third of the time, an additional 75 msec is required, during which time the thread sleeps. How many requests/sec can the server handle?
i. If it is single threaded.
ii. If it is multithreaded.

c) Define heterogeneity and mention the characteristics of heterogeneity? 2

d) Define load balancing in distributed systems? 2

6. a) i. Dependable systems are often required to provide a high degree of security, Why? 3
iii. What is called software agents? Discuss the different types of software agents.

b) Does using time stamping for concurrency control ensure serializability? Explain in your words. 3

c) What is Flynn's Taxonomy? 2

d) Explain Task and Data parallelism using appropriate examples. 4

7. a) Describe the binding agent mechanism for locating a server in case of remote procedure call. 4

b) What are the differences between a local procedure call and a remote procedure call? 2

c) Explain crash failure, Omission failure, and Timing failure with appropriate examples. 3

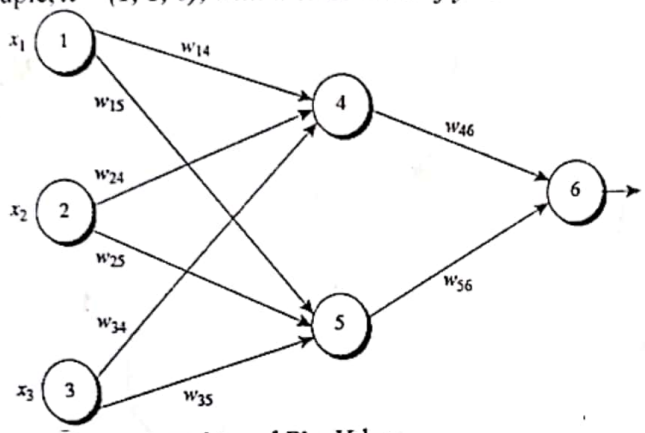
d. Consider a distributed system consisting of four replicated servers. Each of the servers is available at any instant with a probability of 90%. If the system is designed so that the system can be operational if any one of the four servers is operational, what is the overall system availability? What if the system is designed such that all four servers have to be available for the entire system to be available? 3

Institute of Information Technology
Jahangirnagar University
4th Year 1st Semester B.Sc (Hons.) Final Examination, 2021
Subject: Information Technology

Time: 3 Hours | IT4101: Course Title **Artificial Intelligence and Neural network** | Full Marks: 60

Answer any **Five (05)** from the following questions. Figures at the right indicate the marks.
(Sequence must be maintained in answering each of the questions)

1. Figure shows a multilayer Feed-Forward neural network. Let the learning rate be **0.9**. The initial weight and bias values of the network are given in Table, along with the first training tuple, $x = (1, 1, 0)$, *with a class label of* $y=1$. **[4x3=12]**



Initial Input, Weight, and Bias Values

x_1	x_2	x_3	w_{14}	w_{15}	w_{24}	w_{25}	w_{34}	w_{35}	w_{46}	w_{56}	θ_4	θ_5	θ_6
1	1	0	0.2	−0.3	0.4	0.4	−0.5	0.4	−0.3	−0.2	−0.4	0.3	0.2

Find out the following:
(a) Net Input and Output **(b)** Error at Each Node **(c)** Weight and **(d)** Bias Updating

2. a. *Write short notes on cross-validation.* **[2]**

b. *What is Bootstrapping? What is the significance of 0.632 bootstrapping technique and why it is so called?* **[4]**

c. *The data tuples of table are sorted by decreasing probability value, as returned by a classifier. For each tuple, compute the values for the number of true positives (TP), false positives (FP), true negatives (TN), and false negatives (FN). Compute the true positive rate (TPR) and false positive rate (FPR). Plot the ROC curve for the data.* **[6]**

Tuple #	Class	Probability
1	P	0.95
2	N	0.85
3	P	0.78
4	P	0.66
5	N	0.60
6	P	0.55
7	N	0.53
8	N	0.52
9	N	0.51
10	P	0.40

3. a. Define artificial intelligence (AI). Explain all four approaches of AI. **[3]**

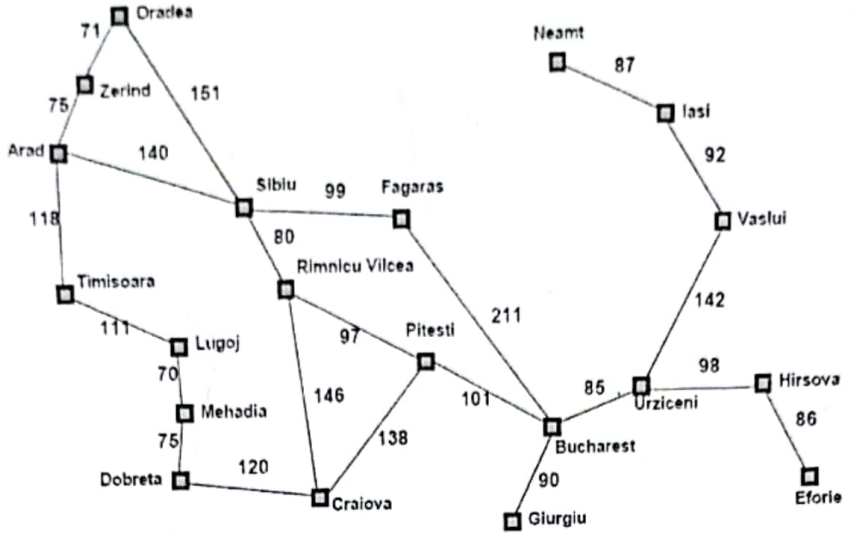
b. What do you mean by supervised and unsupervised learning? Differentiate between them. **[3]**

c. Define the terms: agent, agent function. **[2]**

d. How agents interact with environments through sensors and actuators? Use a vacuum-cleaner world with just two locations to explain those interactions. [4]

4. a. Explain Min-Max algorithm and Alpha –beta pruning. [3x2=6]

b. Use Figure:1 to find the way from 'Zerind' to 'Bucharest' using A* search. Show the stages clearly. [6]



Straight-line dista to Bucharest
Arad 366
Bucharest 0
Craiova 160
Dobreta 242
Eforie 161
Fagaras 178
Giurgiu 77
Hirsova 151
Iasi 226
Lugoj 244
Mehadia 241
Neamt 234
Oradea 380
Pitesti 98
Rimnicu Vilcea 193
Sibiu 253
Timisoara 329
Urziceni 80
Vaslui 199
Zerind 374

Figure 1: Values of h_{SLD} (straight line distances) to Bucharest from other cities.

5. a. How does the KNN algorithm work? How do we choose the factor K? [4]

b. We have a data from the questionnaires survey and objective testing with two attributes (acid durability and strength) to classify whether a special paper tissue is good or not. [8]

Acid Durability (seconds)	Strength (kg/square meter)	Classification
7	7	Bad
7	4	Bad
3	4	Good
1	4	Good

Now the factory produces a new paper tissue that pass laboratory test with Acid durability, 3 and strength, 7. Without another expensive survey, can you guess what the classification of this new tissue is?

6. a. What is meant by problem solving agent? Briefly explain goal formulation and problem formulation. [3]

b. What an agent-design assumes its environment is, if it does not have any idea of it? [1]

c. Give some real-life example of unsupervised machine learning is being used now-a-days. [2]

d. Write short notes on: [3x2=6]

I. 8-queens problem
II. Airline travel problem
III. The 8-puzzle

7. a. What will be the final state of vacuum problem if it is sensor less? Explain with appropriate figure. [4]

b. What are three distinct problem types lead by partial environment information? [2]

c. What is meant by heuristic search strategy? What is the significance of heuristic function? [2]

d. Explain greedy best-first search. What are the properties of greedy best-first search? [4]