Note: 1. Attempt all questions. Each question carries equal marks.

Q1. (a) Describe conventional encryption model. What are the requirements for secure use of conventional encryption?

(b) Explain the following terms:

(i) Confidentiality

(ii) Integrity

(iii) Availability.

OR

(a) What do you understand by stream cipher and block cipher?

(b) Briefly explain cipher block chaining (CBC) and counter (CTR) mode of operation?

Q2. (a) Explain Diffie-Hellman key exchange algorithm.

(b) Perform encryption and decryption using the RSA algorithm for the following-

\[ P=17, q=31, e=7, m=2. \]

OR

(a) What are the principles of the public key cryptosystems?

(b) What is elliptic curve? Explain elliptic curve cryptography with example.

Q3. (a) What is one-way authentication?

(b) Describe certificate-based authentication mechanism?

OR

(a) What do you understand by IP security?

(b) Explain architecture of Secure Socket Layer (SSL)?

Q4. (a) Give brief introduction on software vulnerabilities.

(b) What is phishing attack? Discuss the types of phishing attacks?

OR
(a) Explain various software threats.

(b) Explain various types of virus.

Q5. (a) Explain application level gateways.

(b) What do you understand by web security problem?

OR

(a) Write short note on HTTP.

(b) Write notes on the following:

(i) Cookies

(ii) Firewalls.
IT 801
Model Test Paper - II
INFORMATION SECURITY

Time: 3 Hours                                                                                                         MM: 100

Note: 1. Attempt all questions. Each question carries equal marks.

Q1. (a) With help of a block diagram explain DES encryption algorithms.

(b) What are the block cipher design principles and modes of operation.

OR

(a) Encrypt “meet me” using Hill cipher with key \[
\begin{pmatrix}
9 & 4 \\
5 & 7 
\end{pmatrix}
\]. Also decrypt the same.

(b) Explain public key cryptosystem. Describe Diffie-Hellman key exchange algorithm.

Q2. (a) Write short note on DSA.

(b) For a Diffie-Hellman scheme with a common prime q=11 and a primitive root \(\alpha=2\).

(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 secret key \(K\), shared with A?

OR

(a) What is hash function?

(b) Explain attack on collision resistance.

Q3 (a) Write short note on eavesdropping.

(b) Explain asymmetric based authentication.

OR

(a) What was Kerberos designed for? Explain the architecture of Kerberos.

(b) Write short note on IP security. What are the various application and benefits of IPSec?

Q4. (a) Discuss the types of security threats.

(b) What is the difference between virus and worm? What are typical phases of virus
Q5. (a) What are methods for intrusion detection?
(b) Explain the concept of honey pot.

OR

(a) Discuss the firewall design principles. What are the various types of firewalls?
(b) Write notes on any two of the following:
   (i) Uniform resource locator
   (ii) Packet filters
   (iii) Intruder and its types.
Note: 1. Attempt all questions. Each question carries equal marks.

Q1. a) Describe the taxonomy of neural network architecture.

b) Explain what the use of bias input.

OR

a) What is the significance of Windrow’s learning rule?

b) Differentiate between supervised and unsupervised training with example.

Q2. a) Distinguish between linearly separable and linearly inseparable problem giving two examples of each. Why a single layer of perception can’t be used to solve inseparable problem.

b) Explain why perceptron training algorithm are required?

OR

a) What are the limitations of back propagation algorithm? Define its characteristics and application.

b) What do you understand by multilayer perceptron? Discuss the distinguish characteristics of a multilayer perceptron.

Q3. a) Explain the use of counter propagation network in data compression.

b) Consider a set of vectors

\[
\begin{align*}
[1,1,0,0,0,1,0],[0,0,1,1,1,1,0],[1,0,1,1,1,1,0],[0,0,0,1,1,1,0],[1,1,0,1,1,1,0]
\end{align*}
\]

to be clustered using ART 1 algorithm.

OR

a) Explain ART; mention its working, training, and principle of ART network.

(b) Write a short note on adaptive resonance theory.

Q4. a) Write a short note on neuro genetic hybrid system and applications of FLC systems.
b) Write different properties and operation in fuzzy set.

OR

a) Explain the extension principle in fuzzy set theory.

b) Define membership function & states its importance in fuzzy.

Q5. a) What is travelling sales problem? How does a genetic algorithm solve the TSP.

b) Explain in detail about the various operators involved in Genetic algorithm.

OR

a) Explain the convergence criteria of genetic algorithm.

b) Discuss the genetic algorithm optimization of timetabling problem.
Note: 1. Attempt all questions. Each question carries equal marks.

Q1. a) Given a two input neuron with the following parameters:
   
   bias(b)=2.4, weights(W)=[2,5], and input(p)=[-4,5]^T.

   Calculate the neuron output for the symmetrical hard limit transfer function mentioned below:

   \[ \text{Out} = \begin{cases} -1 & \text{if net} < 0 \\ +1 & \text{if net} \geq 0 \end{cases} \]

   Also find the output for hyperbolic tangent function given as:

   \[ \text{Out} = \frac{e^{\text{net}} - e^{-\text{net}}}{e^{\text{net}} + e^{-\text{net}}} \]

   OR

   i) What is Adaline? Explain algorithm used in Adeline Network.

   ii) Explain Mc-Cullah and Pitt’s model.

Q2. i) Explain the algorithm for ADALINE and MADALINE network.

   ii) Find the weight change expression in error back propagation algorithm for the weight b/w input layer & hidden layer. Assume we are using hyperbolic tangent function as activation function (i.e, \( f(\text{net}) = \tanh(\text{net}) \)).

   OR

   Prove that a multilayer linear fed forward neural network is computationally equivalent to a single layer neural network.

Q3. a) What do you understand by ART? Differentiate between ART and ART1?

   What does <resonance> mean in context of ART network.

   b) Explain the meaning and application of vigilance parameter in ART network.
a) State the training procedure of Kohonen Layer and Gross Berg Layer in counter Propagation network?

b) What is interpolative mode of counter propagation network?

Q4. a) Explain fully rules and reasoning with proper methods.

b) How is a conical rule formed based on

OR

a) Difference between crisp and fuzzy sets.

b) Explain the need of crisp after fuzzy theory

Q5 a) State Charles Darwin’s theory of evolution.

b) Write a short note of genetic algorithm and explain the operation of simple Genetic algorithm.

OR

a) Explain various operators involved in genetic algorithm.

b) Describe the working principle of genetic algorithm.
Note: 1. Attempt all questions. Each question carries equal marks.

Q.1 (a) What do you mean by the term Artificial Intelligence? Explain its Applications?

(b) What do you mean by Production Rules? Explain Production System?

OR

(a) What do you mean by the term Heuristic? Explain Heuristic Search? Explain A* Algorithm?

(b) Solve the given Crypto arithmetic Problem

\[
\begin{align*}
S & \ E & \ N & \ D \\
+ & S & O & R & E \\
\hline
M & O & N & E & Y \\
\end{align*}
\]

Q.2 (a) Explain the term Knowledge? Explain Knowledge Representation?

(b) Explain Theorem Proving Techniques with Examples?

OR

(a) Explain Logic? Explain Propositional Logic and Predicate Logic?

(b) Explain Characteristics of Knowledge Representation Techniques?

Q.3 (a) Explain Probabilistic Reasoning and Baye’s Theorem?

(b) Explain the term Schema? Give Applications of Fuzzy Logic?

OR

(a) Explain Script? What are the Elements used in Reasoning by Scripts?

(b) Explain Semantic Nets and Partitioned Semantic Nets with Examples?

Q.4 (a) Explain the Applications of AI in Game Playing?

(b) Explain Block World Problem in Robotics? Give an Example also?
OR

(a) Explain Natural Language Processing? Explain its Phases?
(b) Explain Syntactic Processing? What is Parsing?

Q.5 (a) Explain Learning and Training?

(b) Explain Neural Networks? Differentiate between AI and Neural Networks?

OR

(a) Explain Common Sense Reasoning? Give an Example?
(b) What is an Expert System? What are the Main Parts of an Expert System?
Note: 1. Attempt all questions. Each question carries equal marks.

Q.1 (a) Explain Types of Production Systems? Explain Control Strategies?
(b) Explain MAN, WOLF, GOAT & CABBAGE Problem with respect to 7
    Problem Characteristics?

   OR

(a) Explain WATER JUG Problem with Rules and State Space Representation?
(b) Explain Depth First Search, Breadth First Search and Best First Search with
    Examples.

Q.2 (a) Explain Clause Form? Write Steps to Convert a Statement into Clause Form?
(b) Explain Deduction and Inferencing?

   OR

(a) Explain Reasoning? Explain Monotonic Reasoning and Non Monotonic
    Reasoning?
(b) Explain Refutation and Backward Chaining with Examples?

Q.3 (a) What are Frames? How Reasoning can be done using Frames?
(b) What is Fuzzy Logic? How is it Different from Traditional Logic?

   OR

(a) What do you mean by Forward Reasoning and Backward Reasoning?
    Explain with Examples?
(b) What is Conceptual Dependency? Explain its Functions?

Q.4 (a) Explain Game Playing Strategies? Explain Minimax Algorithm with
   Example?
(b) Explain the terms Thinking, Planning and Understanding?
(a) Explain Types of Parsing? Explain Top Down Parsing and Bottom Up Parsing with Examples?

(b) Explain the Use of Artificial Intelligence in the Field of Robotics?

Q.5 (a) Explain Supervised Learning and Unsupervised Learning? Differentiate between them?

(b) Explain the Types of Neural Networks? What do you mean by an Activation Function of a Neural Network?

OR

(a) What do you mean by Explanation Based Learning Technique?

(b) Give Names of 3 Expert Systems? Explain any one of them in brief?
Note: 1. Attempt all questions. Each question carries equal marks.

1. (a) Define the term 'Data Mining'. What are differences between data mining strategies and data mining techniques? Explain with examples.

(b) Write differences between the following

(i) Supervised learning and unsupervised learning

(ii) Training data and test data

(iii) Prediction and summarization

(iv) KDD vs DM

OR

(a) What are the limitations of data mining? What kind of answers we can and we cannot expect from a data mining algorithm application?

(b) Write the differences and similarities between the following

(i) Discrimination and prediction

(ii) Characterization and clustering

(iii) DBMS and DM

2. (a) What are the differences between the three main types of data warehouse usage: information processing, analytical processing and data mining? Also discuss OLAP mining (OLAM).

(b) Describe the following terms with examples:

(i) Data cube

(ii) Data warehouse architecture

OR

(a) What are the different ways to classify data?

(b) Explain about the following:
3. (a) Why preprocessing of data is required? What are the various forms of data preprocessing?
(b) Using the information ahead below, draw the following curves

(i) Quantile plot
(ii) q-q plot
(iii) Scatter plot
(iv) Loess curves

<table>
<thead>
<tr>
<th>Unit Price (Rs.)</th>
<th>Items Sold</th>
</tr>
</thead>
<tbody>
<tr>
<td>40</td>
<td>275</td>
</tr>
<tr>
<td>43</td>
<td>400</td>
</tr>
<tr>
<td>47</td>
<td>250</td>
</tr>
<tr>
<td>74</td>
<td>360</td>
</tr>
<tr>
<td>75</td>
<td>520</td>
</tr>
<tr>
<td>78</td>
<td>560</td>
</tr>
<tr>
<td>115</td>
<td>310</td>
</tr>
<tr>
<td>117</td>
<td>280</td>
</tr>
<tr>
<td>120</td>
<td>390</td>
</tr>
</tbody>
</table>

OR

(a) What is data cleaning? Explain basic methods of data cleaning.
(b) Describe various forms of Data Normalization. Also specify their value ranges.

4. (a) What is market basket analysis? Write a priori algorithm. Also demonstrate the working of a priori algorithm.
(b) Describe the principle of pruning in level-wise algorithms. What is its importance?
(a) Describe association rule with item constraint. What is the problem with it? Propose a method for this.

(b) A database has five transactions. Let min. sup = 60% and mm.conf. = 80%

<table>
<thead>
<tr>
<th>Transaction</th>
<th>Items-bought</th>
</tr>
</thead>
<tbody>
<tr>
<td>T100</td>
<td>{M, O, N, K, E, Y}</td>
</tr>
<tr>
<td>T200</td>
<td>{D, O, N, K, E, Y}</td>
</tr>
<tr>
<td>T300</td>
<td>{M, A, K, E}</td>
</tr>
<tr>
<td>T400</td>
<td>{M, U, C, K, Y}</td>
</tr>
<tr>
<td>T500</td>
<td>{C, O, O, K, I, E}</td>
</tr>
</tbody>
</table>

Find all frequent itemsets using apriori

List all of the strong association rules (with support S and confidence C) matching the following meta rule, where X is a variable representing customers and item denotes variables representing items

for all x ∈ transaction, buys (X, item₁) ∧ buys (X, item₂) ∧ buys (X, item₃) [S, C]

5 (a) what are the advantages and disadvantages of NaiveBayes algorithm compared to C4.5 algorithm?

(b) Define the following terms:

(i) K-clusters

(ii) Intra-attribute summary

(iii) Cluster projection

(a) What are the different methods of computing the best split? What is Gini Index? What are entropy gain and gain ratio?
(b) The accompanying data provide information about 12 customers with attributes age and income:

(21, 21) (22, 26) (25, 35) (27, 24) (27, 18) (29, 15)

(32, 27) (35, 24) (37, 56) (37, 29) (38, 56) (40, 23) Assume an Euclidean distance measure and use the K-means clustering algorithm to identify these clusters starting with the three means: (27, 24) (29, 15) (22, 26). Sketch the clustered graph.
Note: 1. Attempt all questions. Each question carries equal marks.

1. (a) What is a Data Warehouse? How is a DW different from a database?
   (b) Discuss the major challenges in DM regarding DM methodology & performance issues.

   OR

   (a) What do you understand by DM? Discuss the role of DM as a step in knowledge discovery process.
   (b) Explain in brief the major components of a typical DM system architecture.

2. (a) Discuss various types of OLAP servers. How are the data actually stored in different server architectures?
   (b) Differentiate between Star & Snowflake schemas with the help of examples.

   OR

   (a) What do you understand by Partial materialization? What the significance of Partial materialization is as compared as compared to the Full materialization of the data cube?

   (b) What are the differences among the three main types of DW usage, information processing, analytical processing & DM?

3. (a) Discuss in brief, why do we pre-process data in DM?
   (b) What do you understand by Concept Hierarchy generation? Discuss it in case of numeric data & categorical data.

   OR
Propose an algorithm in pseudo-code for automatic generation of a Concept Hierarchy for categorical data based on the number of distinct values of attributes the given schema.

(b) Discuss why analytical categorization is needed & how it can be performed?

4. (a) Write the A-priori algorithm for discovering frequent item sets for mining single dimensional Boolean Association Rule & explain it with the help of an example.
   (b) Differentiate between Multi-level & Multi-dimensional Association Rule.

OR

(a) What do you understand by ARM? Discuss partitioning approach for Association mining.
(b) Explain FP growth algorithm for mining Association Rule in large databases.

5. What are the different methods of classification? Explain any two.

OR

(a) What are the different categories of clustering methods?

(b) Differentiate between k-means & k-medoid partitioning methods.