

Hall Ticket Number :									
----------------------	--	--	--	--	--	--	--	--	--

<b>R-20</b>
-------------

**Code: 20A56BT**

III B.Tech. II Semester Supplementary Examinations Nov/Dec 2023

**Cryptography and Network Security**

(Common to CSE and AI&DS)

Max. Marks: 70

Time: 3 Hours

\*\*\*\*\*

- Note: 1. Question Paper consists of two parts (**Part-A** and **Part-B**)  
2. In Part-A, each question carries **Two marks**.  
3. Answer **ALL** the questions in **Part-A** and **Part-B**

**PART-A**

(Compulsory question)

- |   |                 |     |    |
|---|-----------------|-----|----|
| 1. Answer <b>all</b> the following short answer questions | ( 5 X 2 = 10M ) | CO  | BL |
| a) Define Security service.                               |                 | CO1 | L1 |
| b) What is Birthday Attack on Digital Signatures?         |                 | CO2 | L2 |
| c) What are the keys used by PGP?                         |                 | CO3 | L2 |
| d) How is replay attack prevented by IPSec?               |                 | CO4 | L1 |
| e) What is meant by intrusion detection?                  |                 | CO5 | L1 |

**PART-B**

Answer *five* questions by choosing one question from each unit ( 5 x 12 = 60 Marks )

Marks CO BL

**UNIT-I**

- |   |     |     |    |
|---|-----|-----|----|
| 2. Explain about OSI Security architecture model with neat diagram. | 12M | CO1 | L2 |
|---|-----|-----|----|

**OR**

- |  |    |     |    |
|--|----|-----|----|
| 3. a) List and explain the security mechanisms defined by X.800.       | 6M | CO1 | L2 |
| b) Write the categories of attacks. What are the x.800 listed attacks? | 6M | CO1 | L1 |

**UNIT-II**

- |   |    |     |    |
|---|----|-----|----|
| 4. a) Define mono-alphabetic cipher. What is the difference between mono-alphabetic cipher and polyalphabetic cipher?   | 6M | CO2 | L1 |
| b) 'A' and 'B' agreed to use RSA algorithm for the secret communication. 'A' securely choose two primes, p=5 and q=11 and a secret key d=7. Find the corresponding public key. 'B' uses this public key and sends a cipher text 18 to 'A'. Find the plain text. | 6M | CO2 | L2 |

**OR**

5. a) Construct a Playfair matrix with the key largest. Encrypt this message: MEET ME AT THE TOGA PARTY 6M CO2 L2  
 b) Explain the approaches of digital signature standard. 6M CO2 L1

**UNIT-III**

6. a) Explain the authentication procedures defined by X.509 certificate. Illustrate the concept of 'certificate chain' for verification of digital signature on X.509 certificate. 6M CO3 L2  
 b) What are the main features of Kerberos Version 4? 6M CO3 L1

**OR**

7. a) Explain the operational description of PGP. 6M CO3 L2  
 b) Give the summary of cryptographic algorithms used by S/MIME. 6M CO3 L2

**UNIT-IV**

8. a) What is the need for security services at transport layer of Internet Protocol? 6M CO4 L2  
 b) Discuss about the key features of SET. 6M CO4 L1

**OR**

9. a) Illustrate the working of Secure Electronic Transaction (SET) in detail. 6M CO4 L2  
 b) What is the need for encapsulation of security payload? Write and explain different fields of top level format and substructure of ESP packet. 6M CO4 L2

**UNIT-V**

10. a) Write short notes on Signature based IDS. 6M CO5 L1  
 b) List the design goals of firewalls. 6M CO5 L2

**OR**

11. a) Write the characteristics of firewall. 6M CO5 L1  
 b) What is rule based Intrusion Detection? Explain. 6M CO5 L2

\*\*\* End \*\*\*

Hall Ticket Number :									
----------------------	--	--	--	--	--	--	--	--	--

<b>R-20</b>
-------------

**Code: 20A3062T**

III B.Tech. II Semester Supplementary Examinations Nov/Dec 2023

**Machine Learning**  
(Common to CSE & AI&DS)

Max. Marks: 70

Time: 3 Hours

\*\*\*\*\*

- Note: 1. Question Paper consists of two parts (**Part-A** and **Part-B**)  
 2. In Part-A, each question carries **Two marks**.  
 3. Answer **ALL** the questions in **Part-A** and **Part-B**

**PART-A**

(Compulsory question)

1. Answer **all** the following short answer questions ( 5 X 2 = 10M )
- |   |     |    |
|---|-----|----|
|   | CO  | BL |
| a) Define concept learning.   | CO1 | L1 |
| b) Why does entropy is used in decision tree learning?                        | CO2 | L2 |
| c) Is Bayes optimal classifier supervised or unsupervised algorithm? Justify. | CO3 | L2 |
| d) Differentiate the inductive and analytical learning.                       | CO4 | L2 |
| e) What is an agent in reinforcement learning?                                | CO5 | L1 |

**PART-B**

Answer **five** questions by choosing one question from each unit ( 5 x 12 = 60 Marks )

Marks CO BL

<b>UNIT-I</b>
---------------

2. a) Discuss in detail about the components of designing learning system. 6M CO1 L1  
 b) Describe the various issues in machine learning algorithms. 6M CO1 L2

**OR**

3. a) Explain the task, performance, and experience for designing the checkers learning system. 4M CO1 L2  
 b) Apply the Candidate Elimination algorithm to find the general and specific boundary hypothesis for the given dataset.

Sub1	Sub2	Sub3	Sub4	Sub5	CGPA	Rank
Better	Good	Medium	High	High	Excellent	Yes
Better	Good	High	High	High	Excellent	Yes
Normal	Medium	High	High	Medium	Medium	No
Better	Good	High	High	High	Medium	Yes

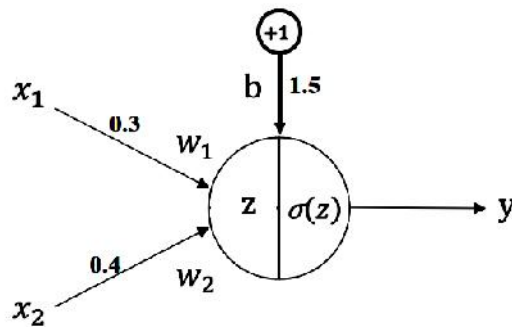
8M CO1 L3

<b>UNIT-II</b>
----------------

4. a) Describe the need of inductive bias in decision tree learning. 4M CO2 L1  
 b) Illustrate the artificial neural network with input layer, hidden layer and output layer for binary class classification. Explain. 8M CO2 L3

**OR**

5. a) Apply Artificial Neural Network with input values  $x_1 = 0.2$ ,  $x_2 = 0.1$  and Desired (Actual) output  $Y = 0.06$ . learning rate  $\alpha = 0.001$ .



- I. Apply the sigmoid function to predict the value.
- II. Apply Mean Squared Error to calculate the loss.

8M CO2 L3

- b) Identify the method to reduce the overfitting in decision tree learning.

4M CO2 L1

### UNIT-III

6. a) Explain minimum description length principle algorithm in detail.  
b) Describe the baldwin effect in model's evolution and learning.

6M CO3 L2

6M CO3 L2

**OR**

7. a) Explain the evolution of population using schema theorem.  
b) Illustrate the various steps in expectation-maximization algorithm and explain.

6M CO3 L2

6M CO3 L3

### UNIT-IV

8. a) Explain the FOIL learning algorithm in detail.  
b) Describe the knowledge level learning in explanation-based learning.

8M CO4 L2

4M CO4 L1

**OR**

9. a) How does PROLOG-EBG discover new features during learning? Explain.  
b) Explain the learn-one-rule algorithm to select an optimal hypothesis in hypothesis space.

4M CO4 L4

8M CO4 L2

### UNIT-V

10. a) Explain the learning task in reinforcement learning with suitable example  
b) Describe the non-deterministic rewards and actions in reinforcement learning.

6M CO5 L2

6M CO5 L2

**OR**

11. a) Explain the Q-learning algorithm to find an optimal policy with all essential steps.  
b) Show the relationship of reinforcement learning to dynamic programming.

8M CO5 L2

4M CO5 L1

\*\*\* End \*\*\*