CBCS SCHEME

USN | | | | | | | | | | |

18SCS31

Third Semester M.Tech. Degree Examination, Dec.2019/Jan.2020
Machine Learning Techniques

Time: 3 hrs. Max. Marks: 100

Note: Answer any FIVE full questions, choosing ONE full question from each module.

Module-1

1 a. What is Machine learning? Mention any three issues in Machine learning. **(04 Marks)**

b. List the different steps to design a learning system. Explain any two in brief. **(06 Marks)**

c. Write the candidate Elimination algorithm. Find specific and generic hypotheses for the concept enjoy sport given below. **(10 Marks)**

Example	Sky	Air Temp	Humidity	Wind	Water	Forecast	Enjoy sport
1	Sunny	Warm	Normal	Strong	Warm	Same	Yes
2	Sunny	Warm	High	Strong	Warm	Same	Yes
3	Rainy	Cold	High	Strong	Warm	Change	No
4	Sunny	Warm	High	Strong	Cool	Change	Yes

OR

2 a. Explain ID3 algorithm for decision tree learning. **(10 Marks)**

b. Consider the following set of training examples:

Instance	Classification	a_1	a_2
1	+	T	T
2	+	T	T
3	-	T	F
4	+	F	F
5	-	F	T
6	-	F	T

i) What is the Entropy of these examples with respect to the target function classification?

ii) What is the information gain of a_2 and a_1?

iii) Which will be selected as the root node a_2 or a_1? **(10 Marks)**

Module-2

3 a. Explain gradient descent algorithm for training a linear unit. Also derive gradient descent rule. **(10 Marks)**

b. Derive Back propagation rule considering output unit weights and hidden unit weights. **(10 Marks)**

OR

4 a. Explain a prototypical Genetic Algorithm. **(10 Marks)**

b. Discuss about common operators for Genetic Algorithm with example. **(10 Marks)**

Module-3

5 a. Explain Naïve Bayes algorithm for learning and classifying text. **(10 Marks)**

b. What is Bayesian Learning? Discuss the features of Bayesian learning method. **(06 Marks)**

c. Determine h_{MAP} from Bayes theorem. **(04 Marks)**

OR

6 a. Explain EM algorithm in detail. **(10 Marks)**

b. Describe Bayesian Belief Networks by taking suitable example. **(10 Marks)**

Module-4

7 a. Explain K-Nearest Neighbor algorithm for approximating a discrete-valued function $f:R^n \rightarrow v$. **(10 Marks)**

b. Explain case based reasoning by taking suitable example. **(10 Marks)**

OR

8 a. Describe basic FOIL algorithm in detail. **(10 Marks)**

b. Write a note on Locally Weighted Linear Regression. **(10 Marks)**

Module-5

9 a. Define Q function. Explain algorithm for Q learning by taking suitable example. **(10 Marks)**

b. What is reinforcement learning? How reinforcement learning problem differs from other function approximation tasks. **(10 Marks)**

OR

10 a. Compare Inductive learning and Analytical learning by giving suitable illustration. **(10 Marks)**

b. Explain the explanation based learning algorithm PROLOG-EBG. **(10 Marks)**

* * * * *

CBCS SCHEME

USN | | | | | | | | | | |

18SCS332

Third Semester M.Tech. Degree Examination, Dec.2019/Jan.2020
Software Project Planning and Management

Time: 3 hrs. Max. Marks: 100

Note: *Answer any FIVE full questions, choosing ONE full question from each module.*

Module-1

1 a. What is SMART criteria? Explain. (10 Marks)
b. List and explain the common pitfalls to watch out for in metrics program. (10 Marks)

OR

2 a. What is configuration management? Explain the steps that constitute software configuration management. (10 Marks)
b. List the functionality provided by most of the SCM tools. Explain repository structure and identification of elements in detail. (10 Marks)

Module-2

3 a. What is risk management? Explain in detail risk management cycle. (10 Marks)
b. What is risk mitigation? Given the common categories of risks, the symptoms to watch out for and the possible mitigation strategies. (10 Marks)

OR

4 a. What is work break down structure? Explain with a figure how is work breakdown structure done. (10 Marks)
b. Explain the issues disused during project closure? (10 Marks)

Module-3

5 a. Explain the dimensions of requirements gathering. (10 Marks)
b. What are the skill sets required during the requirements gathering phase. (10 Marks)

OR

6 a. What are the challenges during the requirements management phase? (10 Marks)
b. What are the 3-phases of estimation? Explain with a neat figure. (10 Marks)

Module-4

7 a. What is testing? List the testing activities. Explain the first two activities of testing in detail. (10 Marks)
b. List the different types of testing done during a product life cycle. Explain White box testing in detail. (10 Marks)

OR

8 a. Why and how is Black box testing done? Explain. (10 Marks)
b. Explain the metrics for the maintenance phase. (10 Marks)

Module-5

9 a. What are the challenges in building global teams? (10 Marks)
b. Explain some effective management techniques for managing global teams. (10 Marks)

OR

10 a. With a figure explain the three deployment model. (10 Marks)
b. Explain the levels of People–Capability Maturity Model(P–CMM) (10 Marks)

* * * * *

CBCS SCHEME

USN | | | | | | | | | | |

18SCS322

Third Semester M.Tech. Degree Examination, Dec.2019/Jan.2020
Information and Network Security

Time: 3 hrs. Max. Marks: 100

Note: ***Answer any FIVE full questions, choosing ONE full question from each module.***

Module-1

1 a. Explain about the types of attacks on encrypted messages. **(05 Marks)**

b. Perform encryption and decryption over the plaintext "PAY" using hill cipher technique with key matrix : $K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$. **(12 Marks)**

c. What are the two problems with the one-time pad? **(03 Marks)**

OR

2 a. Differentiate between stream ciphers and block ciphers. **(04 Marks)**

b. Explain about DES encryption with neat diagram. **(10 Marks)**

c. Discuss about the parameters and design choices that determine the actual algorithm of a Feistel cipher. **(06 Marks)**

Module-2

3 a. Perform encryption and decryption using the RSA algorithm for the given values. P = 11, q = 13, e = 11, M = 17. **(08 Marks)**

b. Why do you need public key cryptosystems? **(06 Marks)**

c. Explain about the counter measures for the timing attack of RSA. **(06 Marks)**

OR

4 a. Consider a Diffie–Hellman key exchange technique with a common prime q = 71 and a primitive root $\alpha = 7$.

i) If user A has private key $X_A = 5$, what is A's public key Y_A?

ii) If user B has private key $X_B = 12$, what is B's public key Y_B?

iii) What is the shared secret key? **(06 Marks)**

b. Consider an Elgamal scheme with a common prime q = 71 and a primitive root $\alpha = 7$

i) If B has public key $Y_B = 3$ and A choose the random integer k = 2, what is the cipher text of M = 30?

ii) If a now chooses a different value of K, so that the encoding of M = 30 is C = (59, C_2), what is the integer C_2? **(08 Marks)**

c. Explain about PRNG based on RSA. **(06 Marks)**

Module-3

5 a. Explain about the public key distribution of secret keys with neat diagram. **(08 Marks)**

b. How is an X-509 certificate revoked? **(04 Marks)**

c. Explain about the public key infrastructure X model with neat diagram. **(08 Marks)**

OR

6 a. Explain about Kerberos version 5. **(08 Marks)**
b. Explain about mutual authentication using asymmetric encryption. **(08 Marks)**
c. Explain about the services provided by a federated identify management. **(04 Marks)**

Module-4

7 a. List out the wireless network security threats. **(06 Marks)**
b. Explain about four way handshake in 1EEE 802.11i. **(08 Marks)**
c. Explain about 1EEE 802MPDU format. **(06 Marks)**

OR

8 a. Explain about web security threats. **(04 Marks)**
b. Explain about SSL protocol stack. **(08 Marks)**
c. Explain about SSH transport layer protocol. **(08 Marks)**

Module-5

9 a. Explain about PGP cryptographic functions. **(09 Marks)**
b. Explain about MIME content types. **(07 Marks)**
c. List out the applications of IPsec. **(04 Marks)**

OR

10 a. Explain about IPsec Architecture. **(06 Marks)**
b. Explain about encapsulating security pay load packet format. **(08 Marks)**
c. Explain about DKIM functional flow. **(06 Marks)**

* * * * *