University of Dhaka
Department of Computer Science and Engineering
4th Year 1st Semester Final Examination, 2020
CSE-4101: Artificial Intelligence (3 Credits)

Total Marks: 60 **Time: 2 Hours**

Answer any 3 (three) of the following questions

---

1 (a) "If we are going to say that a given program thinks like a human, we must have some way of determining how humans think. We need to get inside the actual workings of human minds." – Which methods, according to the cognitive modelling approach, may we use to accomplish this? **[4]**

(b) "An agent's rationality depends on four things: **[10]**

I. agent's prior knowledge about the environment,
II. the actions an agent can perform,
III. agent's percept sequence to date, and
IV. the performance measure that defines the criteria of success."

To what degree do you agree with this statement? Justify your answer with an example agent.

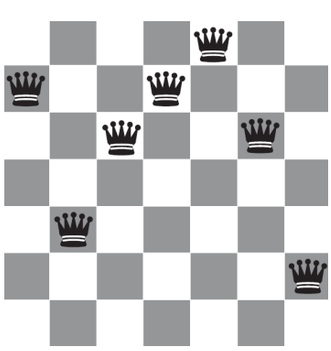
(c) **[6]**

I. The utility function and the performance measure both assess how well an agent is performing. Explain the difference between the two. Explain why problem formulation must follow the goal formation.
II. For each of the following agents, develop a PEAS description of the task environment:
   - Robot Soccer Player
   - Autonomous Mars Rover

2 (a) Consider the problem of placing k knights on an n×n chessboard such that no two knights are attacking each other, where k is given and $k \leq n^2$. **[12]**

I. Choose a CSP formulation. In your formulation, what are the variables?
II. What are the possible values of each variable?
III. What sets of variables are constrained, and how?
IV. Now consider the problem of putting as many knights as possible on the board without any attacks. Explain how to solve this with local search by defining appropriate ACTIONS and RESULT functions and a sensible objective function.

(b) **[8]**



The Min-conflicts algorithm, a local search algorithm, is surprisingly effectives for many Constraint Satisfaction Problems. Amazingly, on the n-queens problem, if you do not count the initial placement of queens, the run time of min-conflicts is roughly independent of problem size. It solves even the million-queens problem in an average of 50 steps (after the initial assignment).

In any case, an initial assignment of a 7-queen problem is illustrated in the above figure.

I. Use the min-conflicts algorithm to solve the problem.

II. As we know that both the backtracking and the local search algorithms have been used to solve CSPs, which one is more applicable to use in an online setting when the problem changes, and why?

III. What is the impact of constraint weighting in solving a CSP?

3 (a) Let's consider the following statements. **[10]**

Everyone who loves all animals is loved by someone.
Anyone who kills an animal is loved by no one.
Jack loves all animals.
Either Jack or Curiosity killed the cat, who is named Tuna.

You must utilize the resolution inference procedure to determine whether or not the following assertion is true:

"Curiosity kill the cat".

We represent the original sentences, some prior knowledge, and the negated goal G in first order predicate logic to make things easy for you.

A. $\forall x \ [\forall y \ \ Animal(y) \Rightarrow Loves(x, y)] \Rightarrow [\exists y \ \ Loves(y, x$

B. $\forall x \ [\exists z \ \ Animal(z) \wedge Kills(x, z)] \Rightarrow [\forall y \ \neg Loves(y, x)]$

C. $\forall x \ \ Animal(x) \Rightarrow Loves(Jack, x)$

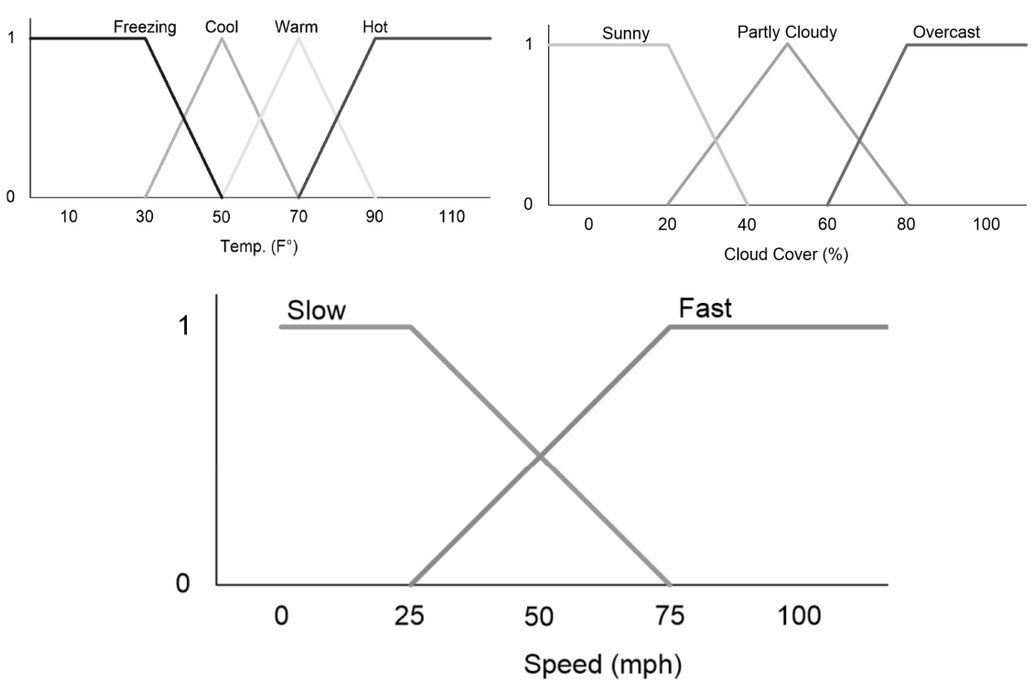
D. $Kills(Jack, Tuna) \vee Kills(Curiosity, Tuna)$

E. $Cat(Tuna)$

F. $\forall x \ \ Cat(x) \Rightarrow Animal(x)$

¬G. $\neg Kills(Curiosity, Tuna)$

(b)



Assume that the driving speed is the combination of output of the following rules: **[10]**

- If it's Sunny and Warm, drive Fast

  Sunny (Cover)^Warm (Temp) ⇒ Fast (Speed)

- If it's Cloudy and Cool, drive Slow

  Cloudy (Cover) ^Cool (Temp) ⇒ Slow (Speed)

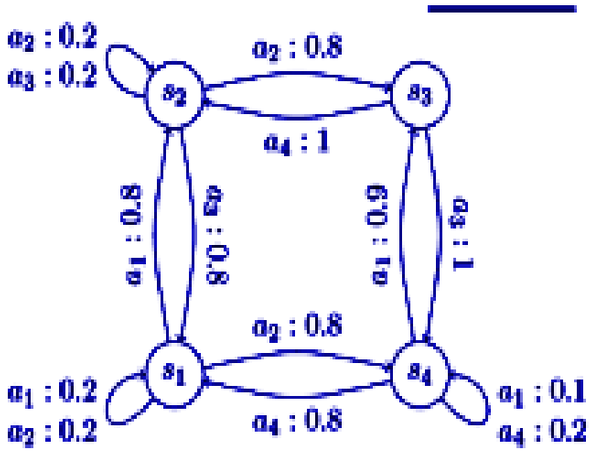
The above three figures can be used to determine the degree of membership for the respective fuzzy sets. Use a fuzzy inference process to determine the precise driving speed if the temperature is **65 F°** and **90%** cloud cover? You must show all the steps in doing so.

[Note that you might need to use "fuzzy AND", which is AB = min (A, B)].

4 (a)

s	$r(s)$
s_1	0
s_2	0
s_3	1
s_4	0

s_i	a	s_j	$T(s_i, a, s_j)$
s_1	a_1	s_1	0.2
s_1	a_1	s_2	0.8
s_1	a_2	s_1	0.2
s_1	a_2	s_4	0.8
s_2	a_2	s_2	0.2
s_2	a_2	s_3	0.8
s_2	a_3	s_2	0.2
s_2	a_3	s_1	0.8
s_3	a_4	s_2	1
s_3	a_3	s_4	1
s_4	a_1	s_4	0.1
s_4	a_1	s_3	0.9
s_4	a_4	s_4	0.2
s_4	a_4	s_1	0.8



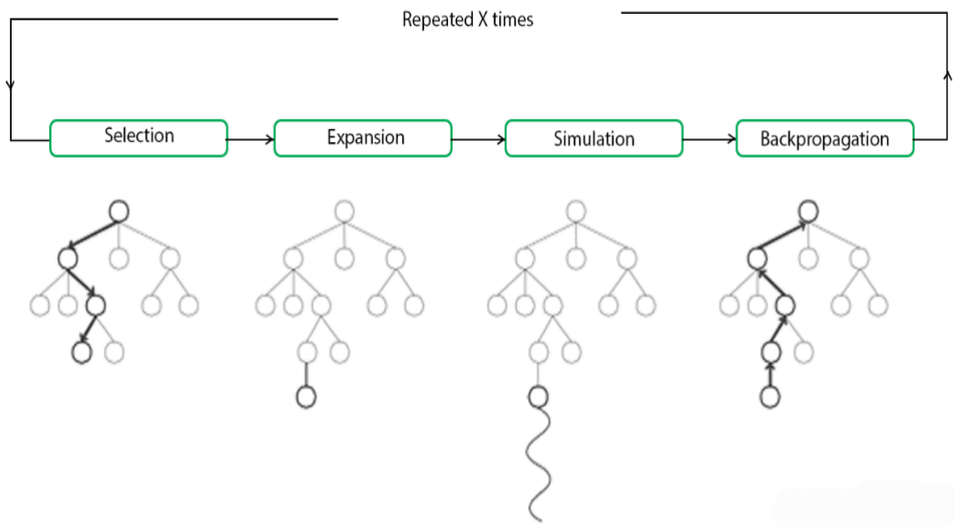
Graphical representation of a sample Markov decision process along with values for the transition and reward functions are given in the above figure. Let the start state be s_1. Use a value iteration algorithm to generate utilities of the states at t = 3 and t = 4, and write them down in the blank cells of the following table. For t = 3, consider $\gamma = 0.5$ and $\varepsilon = 0.1$ and For t = 4, consider $\gamma = 0.85$ and $\varepsilon = 0.3$. Show the optimal policy from the utility values found by the algorithm. **[10]**

In an agent's decision-making process, why do we require "Bellman update equation" instead of "Bellman equation"? The Bellman update equation is provided below for your convenience.

$$u^{t+1}(s) \leftarrow r(s) + \gamma \max_a \sum_{s'} T(s, a, s') u^t(s').$$

	Time (t)				
	0	1	2	3	4
$u(s_1)$	0	0	0	.18	
$u(s_2)$	0	0	.4	.44	
$u(s_3)$	0	1	1		
$u(s_4)$	0	0	.45		

(b)



Monte Carlo Tree Search (MCTS) is a method used to predict the path (moves) that should be taken by the policy to reach the final winning solution. To be precise, it is an algorithm that figures out the best move out of a set of moves by Selecting → Expanding → Simulating → Updating the nodes in tree to find the final solution (see the above figure). This method is repeated until it reaches the solution and learns the policy.

Briefly mention the right intuition for each of the steps. Which steps employ Reinforcement Learning and why? **[5]**

(c) In an Artificial Neural Network, why do we need to use activation function(s)? Why non-linear activation functions are preferred compared to the linear ones. Mention an example setting where linear activation function can be utilized. **[5]**

5 (a) Suppose a Baysian network has the form of a chain: a sequence of Boolean variables X_1 , X_2 , ..., X_n where Parents(X_i) = X_{i-1} for i = 2, …, n. What is the complexity of computing P(X_1| X_n= true) using the enumeration method? And using the variable elimination method? **[7]**

(b) I. Suppose you are building a classifier and you have a learning curve indicating low training error but high error on the cross validation set. Draw the learning curve with the amount of training examples in the x-axis and briefly justify your graph. Explain why this is a problem. **[3]**

II. What should you do now to improve the situation and why? **[3]**

(c) Suppose you want to predict whether or not floods will occur this year in a district of Bangladesh. Also suppose that you have decided to consider only three types of information for this prediction: amount of rainfall, water level of rivers, and age of dams. Draw a neural network architecture for this scenario that has two hidden layers with three units in each. Write down the functions of all the intermediate signals and also the output function using appropriate mathematical notations. **[7]**

University of Dhaka
Department of Computer Science and Engineering
4th Year 1st Semester Final Examination, 2020
CSE-4102: Mathematical and Statistical Analysis for Engineers (3 Credits)
Total Marks: 60 **Time: 2 Hours**
Answer any 3 (three) of the following questions

---

1 (a) Listed below are measured amounts of greenhouse gas emissions from cars in three different categories. The measurements are in tons per year, expressed as CO_2 equivalents. Use a 0.05 significance level to test the claim that the different car categories have the same mean amount of greenhouse gas emissions.

4-cylinder	7.2, 7.9, 6.8, 7.4, 6.5, 6.6, 6.7
6-cylinder	8.7, 7.7, 6.9, 8.7, 8.2, 9.0, 7.1
8-cylinder	7.2, 8.1, 7.0, 6.1, 8.7, 6.2, 7.3

Show **step by step** calculations and find the following:

I. The Null and alternate hypothesis **[1]**
II. Value of test statistic **[3]**
III. P-value **[1]**
IV. Critical Value **[1]**
V. State the test result in non-technical words. **[1]**
VI. Use the Bonferroni test with a 0.05 significance level to identify which means are equal and which are different from the others. **[6]**

(b) A dataset lists the measured CO_2 gas emissions from 32 factories at BEPZA. The sample has a mean of 7.78 tons and a standard deviation of 1.08 tons. Use a 0.05 significance level to test the claim that all factories have a mean CO2 gas emission of 8.00 tons.

Show **step by step** calculations and find the following:

I. State the NULL and alternate hypothesis. **[1]**
II. What is the test statistic and what is its value? **[2]**
III. What is the critical value? **[1.5]**
IV. Write the P-value. **[1.5]**
V. State the test result in non-technical words. **[1]**

2 (a) Explain the basic characteristics of Linear Programming (LP). **[4]**

(b) It costs \$x, \$y and \$z to produce the first, second and each additional block of 25 microchips, respectively. Let h(n) be the cost of production for n blocks of 25 microchips. A single microchip sells for \$p whereas a whole block of 25 microchips sells for \$q. Corona Electronics wants to maximize the profit with an initial investment of \$1M. Find whether the problem can be solved using LP or not. Justify your answer with proper logical explanations. **[6]**

(c) WOB has recently issued \$2M for designing two computer labs (X-Lab and Y-Lab). Each lab has to set up workstations operated through the dedicated servers individually. Different properties of the servers are:

Server	Installation Cost (\$)	Cost per Workstation (\$)	Misc cost per workstation (\$)
A-Server	35000	400	45
B-Server	25000	300	55

Each of the labs are evaluated by some reputation points based on the workstations it uses. Properties of the labs are as follows:

Lab	*maxW*	α_A	α_B
X-Lab	60	5	4
Y-Lab	70	3	5

maxW: Maximum No of Workstations
α_A : Reputation point per workstation operated through A-Server
α_B : Reputation point per workstation operated through B-Server

Formulate a LP to maximize the total reputation points of these two labs. **[10]**

3 (a) The heights are measured for the simple random sample of the Bollywood actresses Priyanka, Deepika, Alia, Kareena, Kangana, Katrina, Anushka, Vidya, and Sonam Kapoor. They have a mean height of 70.0 in. and a standard deviation of 1.5 in. Another dataset lists the heights of 40 Indian women who are not movie actresses, and they have heights with a mean of 63.2 in. and a standard deviation of 2.7 in.

I. Use a 0.01 significance level to test the claim (using P-value method) that the mean height of Bollywood actresses is greater than the mean height of non-actress Indian women. Clearly state the hypothesis, value of test statistic, P-value and state the result in non-technical terms. **[7]**

II. Construct a 90% confidence interval estimate of the difference between the mean height of Bollywood actresses and the mean height of non-actress women of India. **[5]**

Note that for each of the above two questions, just writing the correct result will carry no marks; so show your step by step calculations.

(b) Listed below are the numbers of chirps of a bird in 1 minute and the corresponding temperatures in Fahrenheit. Is there a statistically significant linear correlation between the number of chirps in 1 minute and the temperature? Prove it. Find the confidence interval for the correlation coefficient. **[3+5]**

Chirps in 1 min	882	1188	1104	864	1200	1032	960	900
Temperature (°F)	69.7	93.3	84.3	76.3	88.6	82.6	71.6	79.6

4 (a) Listed below are MPA film ratings for some Hollywood movies from 2001 to 2016 under both the old rating system used by the Motion Picture Association and a new rating system they have introduced in 2021. The new ratings were implemented as the viewers complained that the old ratings were too high.

Old rating	16	18	27	17	33	28	33	18	24	19	18	27	22	18	20	29	19	27	20	21
New rating	15	16	24	15	29	25	29	16	22	17	16	24	20	16	18	26	17	25	18	19

I. Use a 0.01 significance level to test the claim that the old ratings are higher than the new ratings. **[6]**

II. Construct a 95% confidence interval of the mean of the differences between the old ratings and the new ratings. **[4]**

Note that for each of the above two questions, just writing the correct result will carry no marks; so show your step by step calculations.

(b) Using the Simplex method solve the following problem: **[10]**

$$Maximize\ Z = f(x,y) = 3x + 2y$$
$$subject\ to: 2x + y \leq 18$$
$$2x + 3y \leq 42$$
$$3x + y \leq 24$$
$$x \geq 0,\ y \geq 0$$

5 (a) A dataset includes 23 athletes from planet X, and those athletes have height with a mean of 120.8 in and a standard deviation of 22.9 in. That same data set also includes 12 athletes from planet Y, and those athletes have height with a mean of 118.1 in and a standard deviation of 20.8 in.

I. Construct a 95% confidence interval estimate of the standard deviation of the height of all athletes from planet X. **[4]**

II. Construct a 95% confidence interval estimate of the standard deviation of the lengths of all athletes from planet Y. **[4]**

III. Compare the variation of the height of athletes from planet X to the variation of the height of athletes from planet Y. Does there appear to be a difference? **[2]**

Note that, for each of the above three questions, just writing the correct result will carry no marks; so show your step by step calculations.

(b) Consider the function

$$p(x_1, x_2) = 8x_1^2 - 4x_1x_2 + 5x_2^2$$

I. If we write the function in the form $p(\vec{x}) = \vec{x}.A\vec{x}$, then what is the value of A? **[2]**

II. Find the orthogonal eigen basis for and the associated eigenvalues. **[4]**

III. Determine whether $p(0,0)$is the global minimum. **[4]**

University of Dhaka
Department of Computer Science and Engineering
4th Year 1st Semester B. Sc. Final Examination, 2020
CSE-4126: Introduction to Data Science

Total Marks: 60 **Time: 2 Hours**

(Answer any three (3) of the following questions)

1. a) Construct a Bayesian Decision Network (BDN) for making a decision based on the following situation. (*Note: assuming a Bayesian Decision Network is just a directed acyclic graph with a set of nodes and edges will cause a 50% penalty of the total marks allocated in this question.*) 8

Scenario:

On a gloomy winter morning, David wakes up with a strange feeling. He is not sure if he has a flu. Normally, he does not care about flu but when there is high fever, he has to take aspirin. He uses a nice and handy thermometer to measure body temperature. By the way, he does not like taking aspirin for normal flu with low or no fever as he is allergic to aspirin. He actually hates flu as he struggles to decide whether taking aspirin will be beneficial or not. By the way, the benefit of aspirin also depends on the fever condition after taking an aspirin.

Hints: the BDN can have the following nodes:

Chance: Flu, Fever, Temperature, FeverAfterAspirin, Reaction

Decision: Take_Aspirin

Utility: an utility node U

b) Say, X and Y are the two random discrete binary variables. The following tables represent, respectively, the joint probability and conditional probability of X and Y. Calculate the conditional probabilities of Y in terms of X. 6

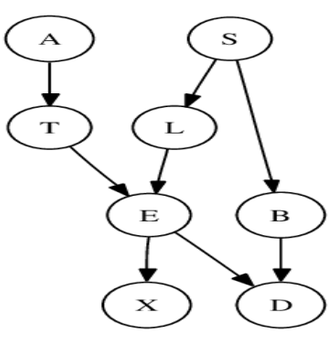
Joint probability		
X	**Y**	**P(X, Y)**
+x	+y	0.2
+x	-y	0.3
-x	+y	0.4
-x	-y	0.1

Conditional probability		
X	**Y**	**P(X|Y)**
+x	+y	0.3
+x	-y	0.75
-x	+y	0.7
-x	-y	0.25

c) Consider the following directed acyclic graph representing the structure of a Bayesian Network. 6

I) Is node D conditionally dependent on Node A?
II) Is D d-separated from X if an evidence on S is given?
III) Are S and T conditionally independent where node B is initialized?

Justify your answers using causal chain, common cause, and common effect. Also show how active triples and inactive triples play role in the above cases.



2. a) What do you mean by classification? Explain with an example. 3

b) Consider the following class-labeled tuples where the playTennis be the class label attribute. Construct a decision tree from the given data. 12

Outlook	Temperature	Humidity	Wind	playTennis
Sunny	Hot	High	Weak	No
Sunny	Hot	High	Strong	No
Overcast	Hot	High	Weak	Yes
Rain	Mild	High	Weak	Yes
Rain	Cool	Normal	Weak	Yes
Rain	Cool	Normal	Strong	No
Overcast	Cool	Normal	Strong	Yes
Sunny	Mild	High	Weak	No
Sunny	Cool	Normal	Weak	Yes
Rain	Mild	Normal	Weak	Yes
Sunny	Mild	Normal	Strong	Yes
Overcast	Mild	High	Strong	Yes
Overcast	Hot	High	Weak	Yes
Rain	Mild	High	Strong	no

c) How can we use tree pruning to improve the performance of a decision tree? 5

3. a) Let's consider a data from the now-defunct Berkeley Restaurant Project, a dialogue system from the last century that answered questions about a database of restaurants in Berkeley, California (Jurafsky et al., 1994). Here is some text normalized sample user queries (a sample of 9332 sentences is on the website): 12

can you tell me about any good cantonese restaurants close by
mid priced thai food is what i'm looking for
tell me about chez panisse

The following table shows the bigram counts from a piece of a bigram grammar from the Berkeley Restaurant Project. Note that the majority of the values are zero. In fact, I have chosen the sample words to cohere with each other; a matrix selected from a random set of seven words would be even more sparse.

	I	**want**	**to**	**eat**	**chinese**	**food**	**as**	**lunch**
I	5	827	0	9	0	0	2	0
want	2	0	608	1	6	5	1	5
to	2	0	4	686	2	0	211	6
eat	0	0	2	0	16	2	0	42
chinese	1	0	0	0	0	82	0	1
Food	15	0	15	0	1	4	0	0
as	1	0	1	0	0	0	0	0
lunch	2	0	0	0	0	1	0	0

The following table shows the frequency of the eight words:

I	**want**	**to**	**eat**	**chinese**	**food**	**as**	**lunch**
2533	927	2417	746	158	1093	278	341

Calculate the probability of the sentence “I want Chinese food” where some other probabilities are as follows:

P(I | <stop>) = 0.25, p(chinese | want) = 0.0011, p(food | chinese) = 0.05 and p(<stop> | food) = 0.68

Hint: You can calculate a bigram probability table from the above two tables.

b) Consider the following corpus: 8

I am Sam
Sam I am
Who is Sam
I do not like Sam

Construct a bag of words from the corpus given above and show the Term frequency (normalized by the frequency of the most frequent word), inverse document frequency and TFIDF for each of the words in the bag.

4. a) Suppose we have a directed graph with n nodes where each node has fewer than some constant $k << n$ incoming or outgoing edges. In the adjacency dictionary representation, which of the following operations are constant time ($O(1) \equiv O(k)$)? 6

1. Checking if there is a link between two nodes A -> B
2. Finding all the outgoing edges of a node A
3. Finding all the incoming edges of a node A
4. Deleting all outgoing and incoming edges of a node A
5. Deleting the link between two nodes A -> B
6. Adding a new node Z to the graph and adding links A ->Z, Z -> B

b) Can we substitute normalization with discretization? If yes, then how? If no, then why not? 5

c) What is the renowned assumption in Naïve Bayes? What role does the assumption play? 5

d) Suppose, we have a dataset for building a machine learning model with *n* rows. If we consider *m%* of the dataset as training data and *(100-m)%* as testing dataset. Are there any maximum and minimum number of rows and range of values of *m* in practice and in theory? If yes, then show the range. If no, then explain why there is not such range? What happens if *m < 100-m* in terms of learning model accuracy or learning process efficiency? 4

5. a) What is the usefulness of unsupervised learning? 3

b) Using k-means algorithm, cluster the following points (with (x, y) representing locations) into three separate clusters. Consider Euclidean distance as the distance function and A_1, B_1 and C_1 as the initial cluster centers. 12
A_1 (2, 10), A_2 (2, 5), A_3 (8, 4), B_1 (5, 8), B_2 (7, 5) B_3 (6, 4), C_1 (1, 2), C_2 (4, 9)

c) With an appropriate example, explain how outliers affect the k-means algorithm. 5

University of Dhaka
Department of Computer Science and Engineering
Fourth Year First Semester 2020 Final examination
CSE 4134: Software Project Management

Duration: 2 Hrs **Full Marks: 60**

Answer any three (3) of the following questions.

1.	**(a)**	State the definition of software project management. Describe the characteristics of a software project.	**6**
	(b)	Is there any difference between software project management and other project management? Justify	**4**
	(c)	Why the management should be *smart*? Explain.	**4**
	(d)	Differentiate between problem decomposition and process decomposition.	**6**
2.	**(a)**	Briefly describe product scope and project scope.	**4**
	(b)	In control scope, we use trend analysis in addition with variance analysis. Is the variance analysis suffice the purpose? Justify your position.	**4**
	(c)	What is affinity diagram? Briefly describe it.	**4**
	(d)	Assume that you are a project manager of an e-commerce site development team. How do you collect requirements?	**8**
3.	**(a)**	Briefly describe fixed price contract and cost-reimbursable contract.	**4**
	(b)	What is critical path? Is the critical path remain critical throughout the project? Define free float, total float, project float and negative float.	**4**
	(c)	An activity in a project network has the following characteristics: Early Start (ES) = 5, Early Finish (EF) = 10, and Late Finish (LF) = 14. What will be the Late Start (LS)?	**4**
	(d)	Assume that you are in charge to arrange an annual picnic of the department. You have to prepare	
		i) Work break down structure	**4**
		ii) Stake holder register	**4**
4.	**(a)**	Compare and contrast conformance and non-conformance cost.	**4**
	(b)	What is audit? Who conduct the audit? Mention the objective of quality audit.	**4**
	(c)	Briefly describe RACI chart with its applications.	**4**
	(d)	Regarding a project, you have the following data. Figures are in million taka. BAC = 200 PV = 100 AC = 120 EV = 80	

Answer the following questions. **4**

i) Assume that all future work will be performed at the budgeted rate, what will be the estimate at completion (EAC) and estimate to completion (ETC). **4**

ii) Assume that what the project has experienced to date can be expected to continue in future, what will be the estimate at completion (EAC) and variance at completion (VAC).

5. (a) Give an example of each of the following types of risk. **4**

i) Internal
ii) External
iii) Technical
iv) Unforeseeable
v) Business risk
vi) Pure insurable risk

(b) Describe different types of strategy for positive risk or opportunity. **4**

(c) Briefly describe "Perform Integrated Change Control" with its key inputs and outputs. **4**

(d) Consider that you are going achieve a vendor certification on "Project Management Professional". To appear for the exam, you have to satisfy the following requirements. **8**

i) At least 3500 hours experience in project work
ii) At least 35 hours preparatory course for this exam

Assume that achieving the vendor certification is a project. Your task is to develop a risk register having following column.

- Name of the risk
- Risk type
- Probability to occurs
- Impact
- Strategy
- Response

You have to identify at least five risk including positive risk and negative risk.

University of Dhaka
Department of Computer Science and Engineering
4th Year 1st Semester B. Sc. Final Examination, 2020
CSE-4137: Cryptography and Security

Total Marks: 60 **Time: 2 Hours**

(Answer any three (3) of the following questions)

1. a) Differentiate between passive and active attacks? Discuss any two active attacks. 1.5+2.5
   b) State the important property of XOR that makes it suitable for an encryption operation. Prove the validity of the property with an example. Prove One Time Pad has perfect secrecy. 3+2
   c) Construct a Playfair matrix with the key **LARGEST**. Now encrypt the following sentence explaining each transformation: 1+4

   JUDI MUST KNOW JOHN

   d) Why GF (2^n) is important? Consider a set of polynomials that belong to the finite field GF (3^2). List all the polynomials and explain the reasons. 3+3

2. a) Explain the notion of semantic security. Discuss why stream ciphers are semantically secure. 3+3
   b) Using the Extended Euclidean algorithm, find the multiplicative inverse of 551 mod 1761. 4
   c) Suppose you perform encryption and decryption using the Feistel structure. What is the relationship between the output of the second encryption round (consisting of RE2 and LE2) and the output of the fourteenth round of decryption (consisting of RD14 and LD14)? Prove that this relationship holds in the Feistel structure. 5
   d) AES decryption is not identical to AES encryption. Explain the changes you need to make to perform the AES encryption and decryption using the same circuit. Draw the AES decryption circuit after you make the necessary changes. 3+2

3. a) Describe Diffie Hellman key exchange protocol and discuss how it can suffer from man in the middle attack? 5+5
   b) Find the out come of Shift Row Transformation step in AES algorithm for the following scenario: 5

87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

   c) How the key expansion algorithm work in case of AES? 5

4. a) Consider an Elgamal public key scheme with a common prime **q** = 71 and a primitive root **α** = 7. 4
      1. If **B** has a public key $\mathbf{Y_B}$ = 3 and **A** chooses the random integer **k** =2, what is the ciphertext of **M** = 30?
      2. 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?
   b) Explain how the Birthday Paradox attack can be performed on the cryptographic hash function and derive the computational complexity of this attack. List some application scenarios that can use the cryptographic hash function. 3+1+2
   c) Discuss the concept of a chain of certificates using an example. 5
   d) Why is the result produced by Bio-metric not always accurate? Discuss in detail the impact of selecting threshold values on bio-metric data. 5

5. a) Consider the following threats and describe how each is handled using SSL: 6

   i. Brute-Force Cryptanalytic Attack: An exhaustive search of the key space for a conventional encryption algorithm.
   ii. Replay Attack: Earlier handshake messages are replayed.
   iii. IP Spoofing: Uses forged IP addresses to fool a host into accepting bogus data.

   b) Explain the Transport mode and Tunnel mode operation of IPSec. Also, discuss the application scenarios where they can be used. 3+3

   c) Compare AES to DES with respect to the following elements of DES. Indicate comparable element in AES or explain why it is not needed in AES. 8

   (i) XOR of subkey material with the input to the f function.
   (ii) XOR of the f function output with the left half of the block.
   (iii) f function.
   (iv) Permutation P.
   (v) Swapping of the halves of the block.

University of Dhaka
Department of Computer Science and Engineering
4th Year 1st Semester Final Examination 2020
CSE–4139: Computer Graphics
Full Marks: 60 **Time: 2:00 Hrs**

Answer any three (3) of the following questions.

1. **(a)** Suppose you have to draw a line from (x_0, y_0) to (x_1, y_1). Derive initial decision variable d_{init} and its essential derivatives ΔN and ΔNW for the line using mid-point line drawing algorithm. **6**

(b) Write an algorithm or a program in C to draw the above line. **6**

(c) Determine the first *8*-pixel coordinates of the above line including the dynamic values of decision variable for each pixel. Assume $|dx/dy| = 0.6$. **8**

2. **(a)** Define homogeneous coordinate system. **4**

(b) Derive |4x4| rotation matrix for a 3D point rotating across Y-axis and the center of rotation is (a, b, c). **8**

(c) The following projection matrix is applied to the 3D vertex (40.0, 30.0, 20.0). To what two-dimensional point is the vertex projected? **8**

$$\begin{Vmatrix} 1.0 & 0.0 & 0.1 & -3.0 \\ 0.0 & 1.0 & 0.0 & 2.0 \\ 0.0 & 0.0 & 1.0 & -4.0 \\ 0.0 & 0.0 & 1.0 & 0.0 \end{Vmatrix}$$

3. **(a)** Explain the terms Ambient, Diffuse and Specular in local light model. **6**

(b) A point light at position p is illuminating a point x on a surface. Explain why the strength of the light is proportional to $1/(p - x)^2$, i.e., one over the squared distance between the light and the point on a surface. Does this rule is analogous with standard light/illumination model? Explain. **6**

(c) Let a line is passing through the points (3.0, 4.5, 7.0) and (5.0, -3.0, 15.0). Does the line intersect a sphere centered at (1.0, 2.5, 40) with a radius 25? If yes then determine the intersection coordinates. **8**

4. **(a)** What is the difference between geometric and parametric continuity in combining curve segments? **4**

(b) Derive the |4x4| basis matrix of Bezier Cubic Curve from its standard equation. **8**

(c) Let P_0 (– 10.0, – 20.0, 0.0), P_1 (5.0, 10.0, 0.0), P_2 (20.0, 15.0, 0.0) and P_3 (30.0, – 10.0, 0.0) are the control points of a Bezier curve. Sketch the evaluation of the curve at (approximately) t = 0.75 using the de Casteljau algorithm. Also determine $P_{(t)}$ at $t = 0.75$. **8**

5. **(a)** Describe different types of color model. **4**

(b) Write an algorithm to convert RGB color values into HSV color values. **8**

(c) Covert the following RGB colors into HSV color values: **8**
i) (1.00, 0.85, 0.50) ii) (0.25, 0.70, 0.80) iii) (0.40, 0.50, 0.30) iv) (0.80, 1.00,0.25)