DEPARTMENT OF COMPUTER SCIENCE AND ENGG.
NATIONAL INSTITUTE OF TECHNOLOGY, TIRUCHIRAPPALLI.
B.Tech END SEMESTER EXAMINATION
CSPC 63 Principles of Cryptography

09/05/22 Time: 2 hours

ANSWER ALL THE QUESTIONS

MAX: 30 Marks

1.(i) Find the multiplicative inverse of 132 in Z_{180} using the extended Euclidean algorithm (3)

(ii) Using Lagrange's theorem, find the orders of all potential subgroups of $< Z_{19}{}^*, x >$ (3)

2.John is reading a mystery book involving cryptography. In one part of the book, the author gives a ciphertext "CIW" and two paragraphs later the author tells the reader that this is s shift cipher and the plaintext is "yes". In the next chapter, the hero found a tablet in a crave with "XVIEWYWI" engraved on it. John immediately found the actual meaning of the ciphertext.

(a) What type of attack did John launch here? (2)

(b) What is the plaintext? (4)

3.With a neat block diagram, explain the general design of AES cipher. (6)

4(i)What is the one way function in RSA? (2)

(ii) Assume that Alice and Bob's ElGamal public key(e1 =2 and e2 = 8) to send two messages P =17 and P' = 37 using same random integer r = 9. Eve intercepts the ciphertext and somehow she finds the value of P = 17. Show how eve can use a known plain text attack to find the value of P'. (4)

5.(i) What are Cryptographic hash functions? What are the properties to be satisfied by these functions? Explain. (3)

106119100:

National Institute of Technology, Tiruchirapppalli - 15
Department of Computer Science and Engineering
End Semester Examination
CSPC62 – Compiler Design

Course/Department : B.Tech./CSE
Semester/Section : VI B
Date and Time : 05-05-2022 & 10.00 AM - 12.00 PM

Batch : 2019-2023
Session : Jan/2022
Marks : 30

Answer ALL Questions with proper steps and justification.
Draw diagrams wherever necessary.

1. a) Discuss on the need of input buffering in Lexical analysis. Give an example.

   b) With the help of a diagram, explain buffer pairs and sentinels. (2)

   c) Identify the lexemes in the following C code and categorize it to appropriate tokens. (3)
   printf("Error at line no %d position %d", l_no, p_no); (1)

2. a) Compute FIRST and FOLLOW for the grammar given below.

   $S \rightarrow ACB|CbB|Ba$ (2)
   $A \rightarrow da|B$
   $B \rightarrow g$
   $C \rightarrow h|\varepsilon$

   b) Construct LALR parsing table for the following grammar.

   $S \rightarrow CB|BC$ (4)
   $C \rightarrow Cad|d$
   $B \rightarrow BaC|a$

3. a) Write the three-address code for the following pseudocode. Identify the basic blocks in the resultant three-address code and draw the control flow graph. (4)

```
void selectionSort(int arr[], int n) {
   int i, j, min_idx, temp;
   for (i = 0; i < n-1; i++) {
      min_idx = i;
      for (j = i+1; j < n; j++)
         if (arr[j] < arr[min_idx])
            min_idx = j;
      temp = arr[min_idx];
      arr[min_idx] = arr[i];
      arr[i] = temp;
   }
}
```
(2)

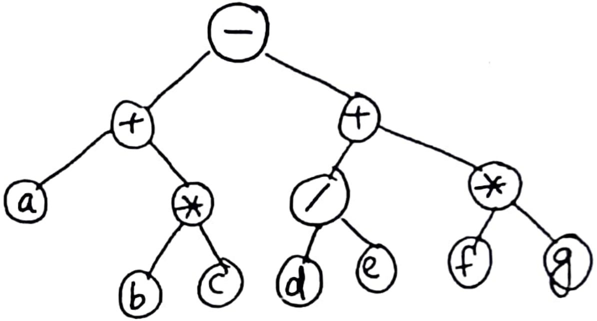
   b) With the help of a suitable example discuss on Backpatching. (2)

4. a) Construct DAG for the expression a + a * (b - c) + (b - c) ^ d. (2)

   b) With the help of suitable examples explain Loop optimization techniques. (2)

   c) Write data flow equations for statement of the form, S → if Expression then S1 else S2.

5. a) Label the following DAG and perform code generation using the labelled DAG. Assume two registers (R0 and R1) can be used for computation. (4)



b) Explain the issues in the design of Code generator. (2)

NATIONAL INSTITUTE OF TECHNOLOGY, TIRUCHIRAPPALLI-15
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
B.Tech. DEGREE, VI SEMESTER EXAM, MAY -2022

CSPE64-Data Analytics

DATE: 11-05-2022 **TIME: 10:00 a.m. -12:00 Noon** **MAX.MARKS:50 Marks**

Answer all Questions **10 X 5=50 Marks**

1. Briefly describe the following advanced database systems and applications: spatial databases, text databases, multimedia databases, stream data, the World Wide Web.

2. The table below shows the demand for a particular brand of printer in a shop for each of the last nine months.

Month	1	2	3	4	5	6	7	8	9
Demand	10	12	13	17	15	19	20	21	20

Calculate a three month moving average for months three to nine. What would be your forecast for the demand in month ten?

Apply exponential smoothing with a smoothing constant of 0.3 to derive a forecast for the demand in month ten.

Which of the two forecasts for month ten do you prefer and why?

3. Explain the Bloom filter technique with an example to check the availability of user name in a Web service so that only valid users that belong to a particular set are allowed through the system.

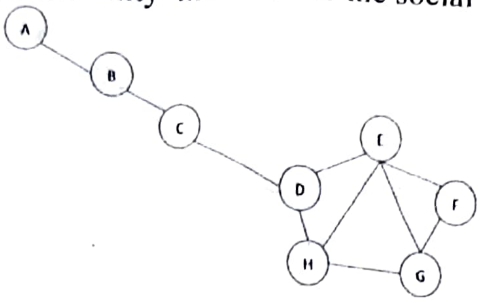
4. Explain the rules for forming buckets in Datar-Gionis-Indyk-Motwani (DGIM) Algorithm

5. Use DBSCAN algorithm to cluster the following set of data: P1(0, 2), P2(5, 0), P3(7,3), P4(0, 5), P5(3, 1), P6(5, 2), P7(1, 7), P8(6, 6). Assume the value of radius is 4 and minpts is 3.

6. A database has ten transactions. Let the minimum support = 30%. Find the frequent item sets using Apriori algorithm

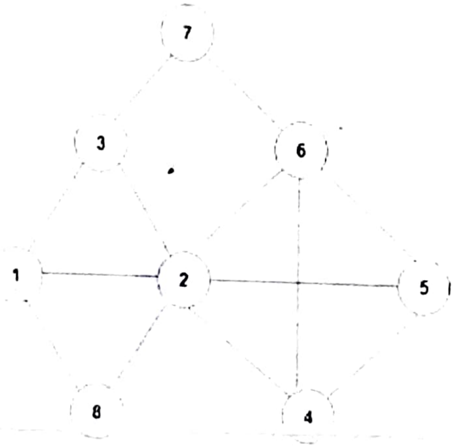
TID	**List of Items**
T1	pen, pencil
T2	pencil, book, eraser
T3	pen, book, eraser, chalk
T4	pen, eraser, chalk
T5	pen, pencil, book
T6	pen, pencil, book, eraser
T7	pen, Ink
T8	pen, pencil, book
T9	pen, pencil, eraser
T10	pencil, book, chalk

7. Compute the Eigen vector centrality measure for the social network graph given below



8. Perform community detection for the following graph using clique percolation technique

K=3 or 4.



9. Create a Student's collections in MongoDB and perform inserting, updating and querying of student details in a document database.

10. Write a R program for creating visualization of models for data using bar chart and pie chart.

--Best Wishes--

NATIONAL INSTITUTE OF TECHNOLOGY, TIRUCHIRAPPALLI
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Final Assessment : CSPC61 - Embedded Systems Architectures

Semester: VI Section: A & B	Maximum Marks: 30 Duration: 2 Hours	Date : 06.05.2022 Time: 10.00 am to 12.00 am

ANSWER ALL THE QUESTIONS

Instruction: Some questions require explanation for your answer. If such questions are attempted without explanation, it won't be considered for evaluation.

1.a.	What development models is Embedded Systems Design and Development Lifecycle Model based upon? Give a brief definition about it.	(1M)
1.b.	Give a neat sketch of Embedded Systems Design and Development Lifecycle Model.	(2M)
1.c.	Find an odd one out and write the reason for your answer. i. OpenCable Application Platform ii. Digital Video Broadcasting iii. Digital Imaging and Communications in Medicine iv. Bluetooth	(1M)
1.d.	State the purpose of garbage collection algorithms. And name and describe non-blocking types of garbage collection algorithms.	(2M)
2.a.	Flash memory is divided into blocks called _____ and Accessing Flash for writing or erasing is a more ______ process.	(1M)
2.b.	Match the Following 1. System buses - A) I/O communication port 2. Backplane buses - B) plugged into the board on-the-fly 3. I/O buses -C) shorter, higher speed, custom buses 4. Expandable buses -D) interconnect memory, the master processor	(2M)
2.c.	Write at least one example for the following schemes : 1) Simplex 2) Half-duplex 3) Full duplex	(1.5M)
2.d.	The PCI bus is made up of ____ lines carrying multiplexed data and _____ address pins as well as other control signals implemented via the remaining _____ pins	(1.5M)
3.a.	Finish the sentence: The software's implicit perception of hardware is that it exists in one of ___ states at any given time. And name those states and write a brief definition about it.	(2M)
3.b.	Does Priority based interrupt handling schemes create impact on Interrupt latency of lower priority interrupt? Justify your answer with explanation.	(1M)
3.c.	Draw a task state diagram in process management.	(2M)
3.d.	During process creation using EXEC/FORK system call, What is the correct sequence of execution? a) Parent task creates the child task using FORK system call b) Child task program got loaded into the memory	(1M)

c) Child task is the copy of the parent task is created and reside in the memory

d) Parent tasks calls EXEC system call to load the child task program

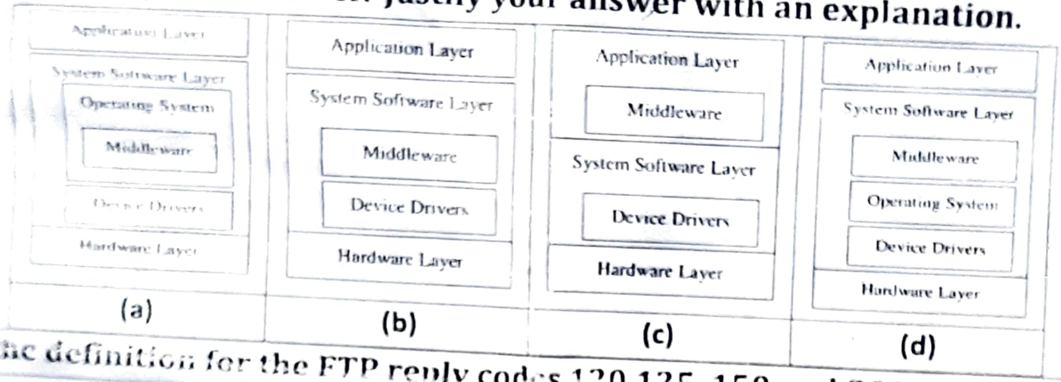
i) a-c-d-b

ii) a-b-d-c

iii) a-d-b-c

iv) a-b-c-d

4.a. Which figure(s) is/are incorrect in terms of mapping middleware software into the Embedded Systems Model? Justify your answer with an explanation. (2M)



(a) (b) (c) (d)

4.b. Write the definition for the FTP reply codes 120,125, 150 and 200.

4.c. In Embedded C, the Unsigned int is a _____ bit data type and takes a value in the range of _____ (1M) (1M)

4.d. Write the syntax for Linux POSIX thread.

5.a. What is a cross compiler? And state the need of a cross compiler in an embedded system development. (2M) (2M)

5.b. Point out the uniqueness of Brook programming language over C programming language in Embedded GPU Design. (1M)

5.c. In case of embedded security _____ can be used by both remote endpoint devices (clients) and servers (1M)

5.d. According to 4+1 architecture, Match the following: (2M)

1. logical structure	A) processor throughput
2. process structure	B) hardware and software mapping
3. development structure	C) system integrity
4. physical structure	D) Functional elements

****

National Institute of Technology

Tiruchirappalli, Tamil Nadu – 620 015

Machine Learning Techniques and Practices – FA **Date: 12.05.2022**

Time: 10:00 – 12:00 AM

Duration: 2 Hr

Total Marks: 30

Note: *MCQ may have multiple answers. In such case, you have to write all the correct choices. Otherwise, mark will not be awarded for that question.*

1. (a) What is the purpose of info() and describe() methods?

(b)Assume that your dataset comprises of 50 features. How many number of principal component axises are possible? Suppose if you want to do dimensionality reduction using the identified axises, then how many number of features you can drop at max *[**Hint:** Do not worry about the exact amount of information that is being carried out by each axis].*

(c) Hierarchical clustering tries to ____________

(i) Put the data into the number of clusters you tell it to

(ii) Tell you what two things are pair-wise similar

(iii) Both (i) and (ii)

(iv) None of the above

(2 M + 2 M + 1 M)

2. (a) Consider the following dataset where Y is the actual value and Y' is the predicted value for the feature X. Find the value of R^2.

X	Y	Y'
1	11	11
2	4	3.8
3	6	5.6
4	9	9.4
5	2	2.5

(b) State whether the model developed in 2(a) is good or not with reason. ***(6 M + 2 M)***

3. *(a) Write the various formulae that can be used to calculate the spearman correlation coefficient and explain the terminologies in short. [**Hint:** Write all the formula and sub formula as well]*

(b) State the conditions under which one should not use the distance based formula to calculate the spearman correlation coefficient.

(4 M + 3 M)

(2 M)

4. Match the following:

(i) Feature Scaling	(1) Represent the dataset in a lesser dimensional space
(ii) Feature Selection	(2) Bring the value of a feature between a certain range
(iii) PCA	(3) Handle class imbalance problem
(iv) SMOTE	(4) Reduce the number of features

5. Consider the following dataset.

Name	Weight *(in kg)*	Height *(in cm)*	Grade	Target Class
Bala	80	180	S	0
Krishnan	70	160	S	0
Karthik	80	120	B	1
Sai	75	200	A	1
Krishna	60	100	A	1

(a) Perform the following encodings for the feature "Grade": Binary Encoding; Label Encoding; and Ordinal Encoding.

(b) What is the major difference between the Label and Ordinal Encodings?

(c) Perform MinMax scaling for the feature "Height *(in cm)*". *[**Hint:** Write the formula and then solve]*

(4 M + 2 M + 2 M)

Question Paper Code: HSIR 14

End Semester Examination 2022

Subject: Professional Ethics

Total Marks-30

Time: 2 Hours

1. Answer all the five questions (5×1=5)

a. Give one example of gender-based discrimination.

b. What do you mean by intellectual property right?

c. What is meant by proprietary information?

d. Stealing from lab/ Falsification/ Fabrication/ Plagiarism- which one doesn't fall under research misconduct (Identify the correct option).

e. Define ethical pluralism. Idea of many theories incompatible with your thoughts

2. Answer all the five questions (5×2=10)

a. What is FMEA? Failure. mode and effect analysi

b. What do you mean by conscientious moral commitment? sensitive to moral val.,
[illegible] [illegible], of situation
best output work

c. Write down two conditions of a valid consent.

d. List two reasons for the risk-benefit analysis.

e. Write down two ethical responsibilities of consulting engineers.

3. Write a brief report on **any two** of the following accidents: **(2×3=6)**

a. Three-Mile Island US Mar 1979 PORV open, after 13m zinc, [illegible]

b. Chernobyl Accidents. April 1986., Russia, RBMK graphite, [illegible]

c. Bhopal Gas Accident 2;-3 dec. 1984. Union Carbide pest-plant [illegible] [illegible]

d. Challenger Case Study

4. Discuss the pros and cons of multinational companies from the point of view of ethics **(1×4=4)**

Or

What do you mean by occupational crimes? Discuss with three examples.

5. Does globalization solve the global issues? Why or why not? **(1×5=5).**

Or

Discuss the role of professional societies in an engineer's life.

****The End****