मोतीलाल नेहरू राष्ट्रीय प्रौद्योगिकी संस्थान इलाहाबाद
प्रयागराज (इलाहाबाद)–211004 (भारत)

Motilal Nehru National Institute of Technology Allahabad
Prayagraj-211004 [India]

Mid Semester (Even) Examination 2019-20

Programme Name: MCA | Semester: IV[TH]

Course Code: CS34310 | Course Name: Cryptography & Network Security

Year: 2nd | Student Reg. No.: 2018CA660

Duration: 90 Mins | Max. Marks: 20 | 04/03/2020 10:30-12:00PM

Instructions: (Related to Questions)

- All questions are compulsory.
- Answers should be justified and to the point.
- Paper contains 2 pages.

			Marks
Q 1		Show that **Fermat theorem** is a special case of Euler Theorem. Evaluate 3^{201} mod 11 using Fermat theorem.	[2Marks]
Q 2	a	List and briefly define types of **cryptanalytic attacks** based on what is known to the attacker.	
	b	Generate a **pseudo code** for reverse cipher and rail fence cipher with same example. And compare them on basis of security.	[3Marks]
Q 3		Evaluate encryption and decryption using **RSA algorithm** for the following. p=17, q=7; e=5; n= 119; Message=6. Explain how to use **Extended Euclid's algorithm** to find the private key and generalize whether strong primes are necessary in RSA. Explain **five** possible approaches to attack RSA algorithm.	[4Marks]
Q 4		For each of the following elements of DES, indicate the comparable element in AES or explain why it is not needed in AES. (XOR of sub-key material with the input to the f function, XOR of the f function output with the left half of the block, Permutation P, Swapping of halves of the block)	[2Marks]

Q 5 Using the **Play fair matrix,** make a reasonable assumption about how to treat redundant letters in the key. [2Marks]

Encrypt this message:

a) Enemy Attacks Tonight and **key** is Battlefield.

b) Generalize your conclusion with rules of the technique.

Q 6 Encrypt the message "Secure Message" using the **Hill cipher** with the key "Ciphering". Show your calculations and the result. Show the calculations for the corresponding decryption of the cipher text to recover the original plaintext. [3Marks]

Q 7 Using **Chinese Remainder Theorem**, find the smallest multiple of 10 which has remainder 2 when divided by 3, and remainder 3 when divided by 7. [1Marks]

Q 8 Give the explanation of each: [3Marks]

a) The difference between diffusion and confusion?

b) The difference between stream cipher and block cipher?

c) The difference between symmetric encryption and asymmetric encryption?

मोतीलालनेहरू राष्ट्रीय प्रौद्योगिकी संस्थान इलाहाबाद
प्रयागराज-२११००४ भारत
Motilal Nehru National Institute of Technology Allahabad
Prayagraj-211004 [India]

Mid Semester Examination Even Semester 2019-20

Programme Name: MCA
Course Code: CS34104
Branch: ------
Duration: 90 Mins

Semester: IV
Course Name: Data Mining
Student Reg. No.: 2 0 1 8 C A 6 0
Max. Marks: 20

03-02-2020
10:30 – 12:00 PM

Instructions:
1. All Questions are compulsory.
2. Write to the point. Make & State necessary assumptions.

Q 1 Consider the training examples as shown in Table below for a binary classification problem which includes 9 instances having 3 attributes (a1, a2, a3) & specify 2 classes (positive & negative class). **(2+2+2)**

Instance	1	2	3	4	5	6	7	8	9
a_1	T	T	T	F	F	F	F	T	F
a_2	T	T	F	F	T	T	F	F	T
a_3	1.0	6.0	5.0	4.0	7.0	3.0	8.0	7.0	5.0
Target Class	+	+	-	+	-	-	-	+	-

On the basis of this training data, answer the following questions:

a) What is the entropy of this collection of training examples with respect to the positive class?

b) Compute the information gains of a_1, a_2 and a_3 relative to these training examples? What is the best split (among a_1, a_2 and a_3) according to the information gain?

c) For a3, which is a continuous attribute, compute the information gain for every possible split.

Q 2 **a)** What is OLAP? Draw a diagram illustrating the role of OLAP tools in Business Intelligence and explain. **(2+2+2)**

b) List OLAP operations in Multidimensional Data model and explain with an example.

c) Describe briefly discretization and concept hierarchy generation for numerical data?

Q 3 **a)** Consider the following data (in increasing order) for the attribute age: **(2+2+2+2)**

13, 15, 16, 16, 19, 20, 20, 21, 22, 22, 25, 25, 25, 25, 30, 33, 33, 35,35, 35, 35, 36, 40, 45, 46, 52, 70.

Use smoothing by bin means to smooth the above data, using a bin depth of 3. Illustrate your steps. Comment on the effect of this technique for the given data.

b) Suppose the fraction of undergraduate students who smoke is 15% and the fraction of graduate students who smoke is 23%. If one-fifth of the college students are graduate students and the rest are undergraduates, what is the probability that a student who smokes is a graduate student?

c) Given the information in part (b), is a randomly chosen college student more likely to be a graduate or undergraduate student?

d) What is the significance of 'K' in KNN algorithm? How do we decide the value of 'K' in KNN algorithm?

**********End **********

Motilal Nehru National Institute of Technology Allahabad, Prayagraj-211004 [India]
Name of the Department: CSED, Mid Semester (Even) Examination 2019-20

Programme Name: MCA **Semester: IV**

Course Code: CS34103 **Course Name: Computer Network**
Branch: NIL

2	0	1	8	C	A	6	0

Student Reg. No.:

Duration: 90 Minutes **Max. Marks: 20** 02-03-2020

Instructions:(Related to Questions) *Figures to the right indicate the full marks. Attempt all questions.*

Q 1	Differentiate between OSI and TCP/IP models. What do you understand by transmission speed how it is different from propagation speed.	3
Q 2	Wired LAN uses CSMA/CD but wireless prefers CSMA/CA, why? MNNIT is using tree topology where computer center layer 3 core switch is connected to SAC layer 3 distribution switch which in turn connected to layer 2 access switch at care taker room of hostel. Point out switchs and wires using CSMA/CD in the topology.	3
Q3	Draw flow chart for DCF clearly explaining exponential back off within the flow chart. When more than one station are waiting to get medium free, why each stating selects a random waiting time, why not the station starts transmitting immediately when medium becomes free, in this situation.	3
Q4	MNNIT has network adress 210.212.50.0/24 and wants to form subnet for 5 departments. If hosts requirement is as follows: CSED-90, ECED-40, EED-25, CED-13, MED—4. Give a possible sub-netting scheme with net id and broadcast address.	2
Q 5	Draw flow chart for longest prefix match forwarding algorithm at IP layer.	3
Q6	If a router is using same outgoing line for 4 addresses, should the administrator of the router need to aggregate those addresses. In which condition addresses can be aggregated and in which condition addresses can not be aggregated. Is it possible to aggregate: 110.50.96.0/21, 110.50.104.0/21, 110.50.112.0/21, 110.50.120.0/21 If yes, to what and also give routing table before and after aggregation. If not, why?	3
Q7	Trace movement of a packet P from node PC1(IP address 202.141.64.6/22 of MNNIT network to the BSNL(ISP) router R1 (IP address 210.212.50.2/30). BSNL router R1 is connected directly to MNNIT gateway router R2. MNNIT network has no sub-netting. PC1----------R2----------R1-------rest of Internet.	3

मोतीलाल नेहरू राष्ट्रीय प्रौद्योगिकी संस्थान इलाहाबाद
प्रयागराज–211004 भारत

Motilal Nehru National Institute of TechnologyAllahabad
Prayagraj-211004 [India]

Computer Science & Engineering Department

Mid Semester (Even) Examination 2019-20

Programme Name: MCA **Semester: IV**

Course Code: CS 34102 **Course Name:** Software Engineering

Branch:..... **Student Reg. No.:** 2 0 1 8 C A 6 0

Duration: 90 Minutes **Max. Marks: 20**

29-02-2020
leap year
BHUVAN BIRTHDAY

Instructions: (Related to Questions)

1. *Figures to the right indicate the full marks.*
2. *Attempt all questions*
3. *Answers should be VERY BRIEF & PRECISE*

			Marks	Mapped to CO number

Q 1	a	Draw the CFG for the following code snippet:
		IF credit rating > = 4
		
		THEN
		approve
		ELSE
		IF(income>100,000) AND
		(number of children < 3)
		THEN
		approve
		ELSE
		disapprove
		Compute number of Independent Paths in the CFG?
			03	CO3

	b	What is Rapid Throwaway Prototyping? When Should it be used?	1 + 1	CO1
Q 2		To develop a simple standalone application for customer records in python, compute the development time and average staff size for this application. This application will be used to store the personal information of the customer attributes namely customer name, company, contact no, address and credit limit into database. Application will generate credit limit report and personal information report for the customers. Assume all the complexity factors and weighting factors are average and LOC for python is 1200/FP.	05	CO4

Project	a_i	b_i	c_i	d_i
Organic	3.2	1.05	2.5	0.38
Semidetached	3.0	1.12	2.5	0.35
Embedded	2.8	1.20	2.5	0.32

Functional Units	Complexity factors		
	Low	Avg.	High
External Inputs (EIs)	3	4	6
External Outputs (Eos)	4	5	7
External inquiries (EQs)	3	4	6
External Logical files (ILF)	7	10	15
External Interface files (ELF)	5	7	10

Q 3	a	Enumerate major Requirement Engineering Process activities.	2	CO2
	b	A project schedule has the following characteristics as shown in Table below:	2+2+2	CO4

Activity	Name	T_O	T_M	T_P
1-2	A	2	3	10
1-3	B	1	1	1
2-4	C	1	1	1
3-4	D	1	1	1
3-5	E	4	6	8
4-9	F	3	5	7
5-6	G	2	4	6
5-7	H	2	9	10
6-8	I	1	1	1
7-8	J	1	2	3
8-10	K	3	5	7
9-10	L	6	7	8

a) Construct PERT network.
b) Compute Latest Time and Earlier Time?
c) Find the critical path and activities?

Q4.		How do you obtain Instability from Martin's coupling metric?	2	CO3

मोतीलाल नेहरू राष्ट्रीय प्रौद्योगिकी संस्थान इलाहाबाद
प्रयागराज–211004 भारत

Motilal Nehru National Institute of Technology, Allahabad
Prayagraj-211004 [India]

संगणक विज्ञान एवं अभियांत्रिकी विभाग

Mid Semester (Even Semester) Examination 2019-20

Programme Name: MCA / M. Sc. **Semester:**.....IV.....

Course Code: CS34101 **Course Name:** Computer Graphics

Branch:....NA..... **Student Reg. No:** | 2 | 0 | 18 | C | A | 6 | 0 | |

Duration: 90 Minutes **Max. Marks:** 20 28-02-2020

Friday 10:30-12 PM

Instructions: (Related to Questions)

1. Figures to the right indicate the full marks.
2. **Attempt ALL questions . Also Write to the point, exactly what is asked.**
3. **All parts of a question should be answered in one attempt serially NOT here & there.**

			Marks	Mapped to CO number **(Optional)**
Q 1		Explain in brief **construction & working** of the LC Monitors. Why the Plasma Panel displays are NOT used in Laptop **now days**?	03	
Q 2	a	How much Memory is needed for the Frame Buffer to store a 640X400 display with 16 grey levels?	01	
	b	How much time is spent scanning across each row of pixels during screen refreshing a Raster System with a Resolution of 640 X 480 and refresh raster of 60 frames per second?	02	
Q 3	a	**Compare**: **DDA Vs Brasenham** Line Tracing Algorithm.	01	
	b	**Compute & Tabulate points** to be illuminated for tracing a Circle with Radius **r =10** in the circle Octant in the first Quadrant from **x=0** to **x=y** using **Mid Point Circle** Tracing Algorithm.	03	
Q4	a	Show how reflection in line $y = -x$ can be performed by a scaling operation followed by a Rotation.	02	
	b	Show how **shear transformation** may be expressed in terms of **Rotation** & **Scaling**.	02	

Q5		Write down POINT WISE the Cohen – Sutherland Subdivision LINE Clipping Algorithm.	03	
Q6		How the **Laser Printer** prints the best Quality of output? **Write its steps**. How the **3-D Printers** differs with the **2-D** Printers?	02	
Q7		Write any 02 uses of CISCO:SPARK Board (a Smart Board).	01	