NARSIMHA REDDY ENGINEERING COLLEGE
UGC AUTONOMOUS INSTITUTION
Maisammaguda (V), Kompally - 500100, Secunderabad, Telangana state, India
Accredited by NBA & NAAC with 'A' Grade
Approved by AICTE
Permanently affiliated to JNTUH

COURSE FILE

Program Name	: CSE
Name of the Course	: INFORMATION SECURITY
Course Code	: CS4101PC
Semester and Year	: IV-I
Faculty Name	: ANUSHA K , G UDAY KUMAR

S.No	Contents	Included
1	Vision, Mission, COs, POs,PSOs,PEOs	
2	Academic calendar	
3	Syllabus	
4	CO/PO mapping	
5	Nominal Rolls of the Students	
6	Timetable	
7	Lesson Plan	
8	Unit wise Question Bank	
9	Old Question Papers	
10	Question Papers (CIA&SEE)	
11	Tutorial sheets	
12	Learning Methodologies: Experiential learning (Industrial visits, Internships, Mini Projects, Academic Projects, Guest Lectures, Student Workshops etc.,),Problem Solving methodologies(assignments ,qui z, case study etc.) **Note:1. At least TWO learning Methodologies to be included in your course** **2. The above methodologies for illustration ,you may add more**	
13	Subject notes/PPTs/self study material	
14	Feedback on Curriculum Design and development	
15	CO/PO attainment, analysis and Action taken report	

Signature of the Faculty Signature of the Head Signature of the Principal

1. Institute Vision & Mission

Vision of the Institute

To produce competent professionals who can contribute to the industry, research and societal benefits with environment consciousness and ethical Values.

Mission of the Institute

M1: Adapt continuous improvements in innovative teaching-learning practices and state-of-the- art infrastructure to transform students as competent professionals and entrepreneurs in multi-disciplinary fields.

M2: Develop an innovative ecosystem with strong involvement and participation of students and faculty members.

M3: Impart National development spirit among the students to utilize their knowledge and skills for societal benefits with ethical values.

Vision of the Department:

To produce technically competent professionals with quality education in cutting edge technologies with professional ethics.

Mission of the Department:

M1: To impart quality technical education in design and implementation of IT applications through innovative teaching - learning practices

M2: To inculcate Professional behavior, with strong ethical values, and research capabilities.

M3: To educate students to be effective problem solvers with social sensitivity for the betterment of the society and humanity as a whole.

Programme Educational Objectives (PEOs):

PEO-I: Demonstrate proficiency in fundamental concepts and advanced technologies of computer science to succeed in their careers and/or obtain a higher degree.

PEO-II: Analyze complex computing problems in multidisciplinary area and creatively solve them.

PEO-III: Recognize ethical dilemmas in work environment and apply professional code of ethics.

PROGRAM OUTCOMES (POs):

1	**PO1. Engineering knowledge:** Apply the knowledge of basic sciences and fundamental engineering concepts in solving engineering problems.
2	**PO2. Problem analysis:** Identify and define engineering problems, conduct experiments and investigate to analyze and interpret data to arrive at substantial conclusions.
3	**PO3. Design/development of solutions:** Propose an appropriate solution for engineering problems complying with functional constraints such as economic, environmental, societal, ethical, safety and sustainability.
4	**PO4. Conduct investigations of complex problems**: Perform investigations, design and conduct experiments, analyze and interpret the results to providevalid conclusions.
5	**PO5. Modern tool usage**: Select or create and apply appropriate techniques and IT tools for the design & analysis of the systems.
6	**PO6. The engineer and society:** Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.
7	**PO7. Environment and sustainability**: Demonstrate professional skills and contextual reasoning to assess environmental or societal issues for sustainable development.
8	**PO8. Ethics**: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
9	**PO9. Individual and team work**: Function effectively as an individual, and as a member or leader in diverse teams, and in multi-disciplinary situations.
10	**PO10. Communication**: Communicate effectively among engineering community, being able to comprehend and write effectively reports, presentation and give / receive clears instructions.
11	**PO11. Project management and finance**: Demonstrate and apply engineering& management principles in their own / team projects in multidisciplinary environment.
12	**PO12. Life-long learning**: Recognize the need for, and have the ability to engage in independent and lifelong learning.

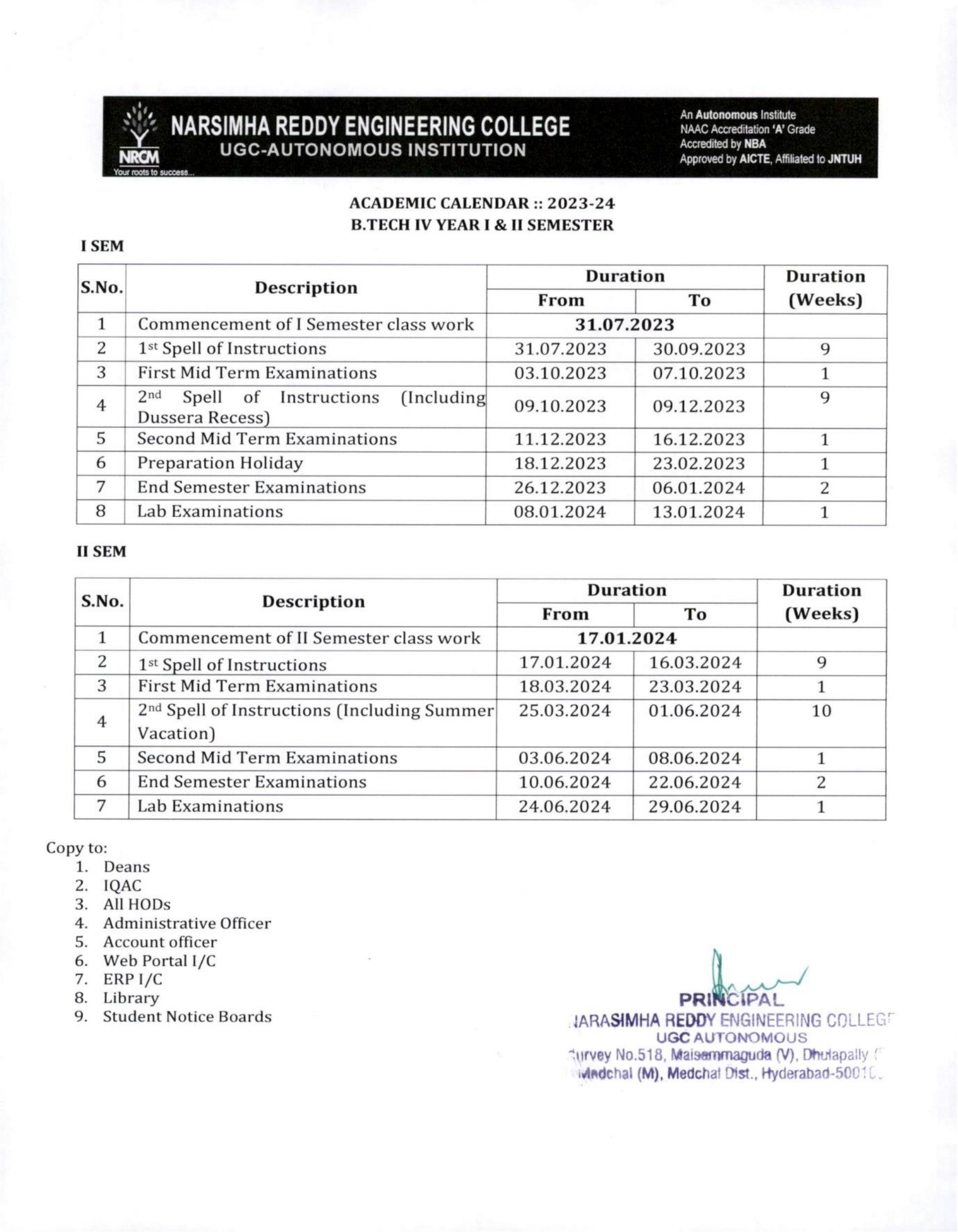
PROGRAM SPECIFIC OUTCOMES (PSOs):

PSO1: Apply acquired knowledge of programming languages, data structures, algorithms and standard software engineering principles to devise effective solutions for intricate computational issues.

PSO2: Design and develop efficient web and mobile based applications under realistic constraints.

PSO3: Apply core and advanced concepts of database management systems,data mining and machine learning to devise engineer solutions for practical problems.

2.ACADEMIC CALENDAR



NARSIMHA REDDY ENGINEERING COLLEGE
UGC-AUTONOMOUS INSTITUTION
NRCM
Your roots to success...

An Autonomous Institute
NAAC Accreditation 'A' Grade
Accredited by NBA
Approved by AICTE, Affiliated to JNTUH

ACADEMIC CALENDAR :: 2023-24
B.TECH IV YEAR I & II SEMESTER

I SEM

S.No.	Description	Duration		Duration (Weeks)
		From	To	
1	Commencement of I Semester class work	**31.07.2023**		
2	1st Spell of Instructions	31.07.2023	30.09.2023	9
3	First Mid Term Examinations	03.10.2023	07.10.2023	1
4	2nd Spell of Instructions (Including Dussera Recess)	09.10.2023	09.12.2023	9
5	Second Mid Term Examinations	11.12.2023	16.12.2023	1
6	Preparation Holiday	18.12.2023	23.02.2023	1
7	End Semester Examinations	26.12.2023	06.01.2024	2
8	Lab Examinations	08.01.2024	13.01.2024	1

II SEM

S.No.	Description	Duration		Duration (Weeks)
		From	To	
1	Commencement of II Semester class work	**17.01.2024**		
2	1st Spell of Instructions	17.01.2024	16.03.2024	9
3	First Mid Term Examinations	18.03.2024	23.03.2024	1
4	2nd Spell of Instructions (Including Summer Vacation)	25.03.2024	01.06.2024	10
5	Second Mid Term Examinations	03.06.2024	08.06.2024	1
6	End Semester Examinations	10.06.2024	22.06.2024	2
7	Lab Examinations	24.06.2024	29.06.2024	1

Copy to:

1. Deans
2. IQAC
3. All HODs
4. Administrative Officer
5. Account officer
6. Web Portal I/C
7. ERP I/C
8. Library
9. Student Notice Boards

PRINCIPAL
NARASIMHA REDDY ENGINEERING COLLEGE
UGC AUTONOMOUS
Survey No.518, Maisammaguda (V), Dhulapally (
Medchal (M), Medchal Dist., Hyderabad-50010

3.SYLLABUS:

CS4101PC: INFORMATION SECURITY

IV-I:CSE								
Course Code	**Category**	**Hours/Week**			**Credits**	**Max Marks**		
CS4101PC	**Core**	**L**	**T**	**P**	**C**	**CIE**	**SEE**	**Total**
		3	**0**	**0**	**3**	**25**	**75**	**100**
Contact Classes:45	**Tutorial classes:15**	**Practical classes: Nill**				**Total Classes:60**		
Prerequisites								

Course Objectives:

- Explain the objectives of information security
- Explain the importance and application of each of confidentiality, integrity, authentication and availability
- Understand various cryptographic algorithms.
- Understand the basic categories of threats to computers and networks
- Describe public-key cryptosystem.
- Describe the enhancements made to IPv4 by IPSec
- Understand Intrusions and intrusion detection
- Discuss the fundamental ideas of public-key cryptography.
- Generate and distribute a PGP key pair and use the PGP package to send an encrypted e-mail message.
- Discuss Web security and Firewalls

Course Outcomes:

- Student will be able to understand basic cryptographic algorithms, message and web authentication and security issues.
- Ability to identify information system requirements for both of them such as client and server.
- Ability to understand the current legal issues towards information security.

MODULE- I

Security Concepts : Introduction, The need for security, Security approaches, Principles of security, Types of Security attacks,

Security services, Security Mechanisms, A model for Network Security

Cryptography Concepts and Techniques: Introduction, plain text and cipher text, substitution techniques, transposition techniques, encryption and decryption, symmetric and asymmetric key cryptography, steganography, key range and key size, possible types of attacks.

MODULE- II

Symmetric key Ciphers: Block Cipher principles, DES, AES, Blowfish, RC5, IDEA, Block cipher operation, Stream ciphers, RC4.
Asymmetric key Ciphers: Principles of public key cryptosystems, RSA algorithm, Elgamal Cryptography, Diffie- Hellman Key Exchange, Knapsack Algorithm.

MODULE- III

Cryptographic Hash Functions: Message Authentication, Secure Hash Algorithm (SHA-512), **Message authentication codes:** Authentication requirements, HMAC, CMAC, Digital signatures, Elgamal Digital Signature Scheme.

Key Management and Distribution: Symmetric Key Distribution Using Symmetric & Asymmetric Encryption, Distribution of Public Keys, Kerberos, X.509 Authentication Service, Public–Key Infrastructure

MODULE- IV

Transport-level Security: Web security considerations, Secure Socket Layer and Transport LayerSecurity, HTTPS, Secure Shell (SSH)
Wireless Network Security: Wireless Security, Mobile Device Security, IEEE802.11 Wireless LAN, IEEE802.11i Wireless LANSecurity

MODULE- V

E-Mail Security: Pretty Good Privacy, S/MIME **IPSecurity:** IP Security overview, IP Security architecture, Authentication Header, Encapsulating security payload, Combining security associations, Internet Key Exchange

Case Studies on Cryptography and security: Secure Multiparty Calculation, Virtual Elections, Single sign On, Secure Inter-branch Payment Transactions, Cross site Scripting Vulnerability.

TEXTBOOKS:

1. Cryptography and Network Security- Principles and Practice: William Stallings, Pearson Education ,6th Edition
2. Cryptography and Network Security: Atul Kahate, McGrawHill,3rd Edition

REFERENCEBOOKS:

1. Cryptography and Network Security: CKShyamala, N Harini, Dr TR Padmanabhan, Wiley India,1st Edition.
2. Cryptography andNetwork Security: Forouzan Mukhopadhyay ,McGrawHill, 3rd Edition
3. Information Security, Principles and Practice: Mark Stamp,Wiley India.
4. Principles of Computer Security:WM.Arthur Conklin, Greg White ,TMH
5. Introduction to Network Security: Neal Krawetz, CENGAGE Learning
6. Network Security and Cryptography : Bernard Menezes, CENGAGE Learning

4.CO/PO Mapping

List of course outcomes:

CO#	After completion of course, students should able to
CO1	Enumerate the fundamental principles that underlie network security.
CO2	Apply asymmetric encryption methods like RSA for secure key exchange.
CO3	Analyze the role of cryptographic hash functions in ensuring message integrity.
CO4	Evaluate the effectiveness of Secure Socket Layer (SSL) and Transport Layer Security (TLS) in web security.
CO5	Design a comprehensive email security solution using Pretty Good Privacy (PGP) or S/MIME.

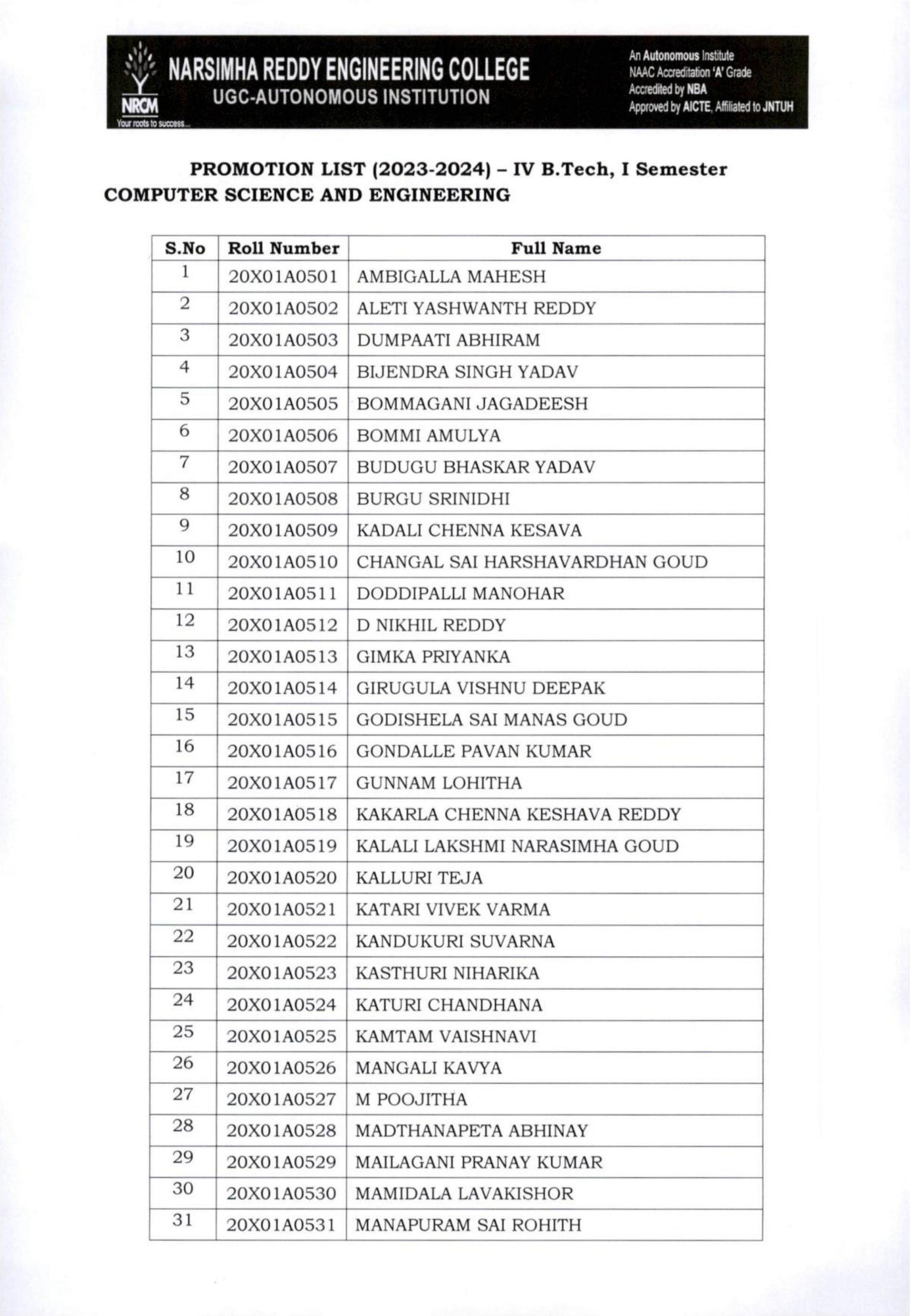
Course Outcome (CO)-Program Outcome (PO) Matrix

Attributes	Knowledge	Analysis	Design	Develop	Modern Tools	Society	Environment	Ethics	Team Work	Communication	Project Management Finance	Life long Learning
Course Outcome	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	-	-	-	-	-	-	-	-	-	-	-
CO2	3	-	-	-	-	-	-	-	-	-	-	-
CO3	2	3	-	-	-	-	-	-	-	-	-	-
CO4	3	-	2	2	-	-	-	-	-	-	-	-
CO5	3	-	2	2	-	-	-	-	-	-	-	-
Avg												

MAPPING OF COURSE OUTCOMES WITH PSO's:

Attributes	Engineering Knowledge and Analysis	System Design	Application of the knowledge on society/environment
COs	**PSO1**	**PSO2**	**PSO3**
CO1	-	-	3
CO2	-	-	3
CO3	-	-	3
CO4	-	-	3
CO5	-	-	3
Avg			

5.Nominal Rolls:



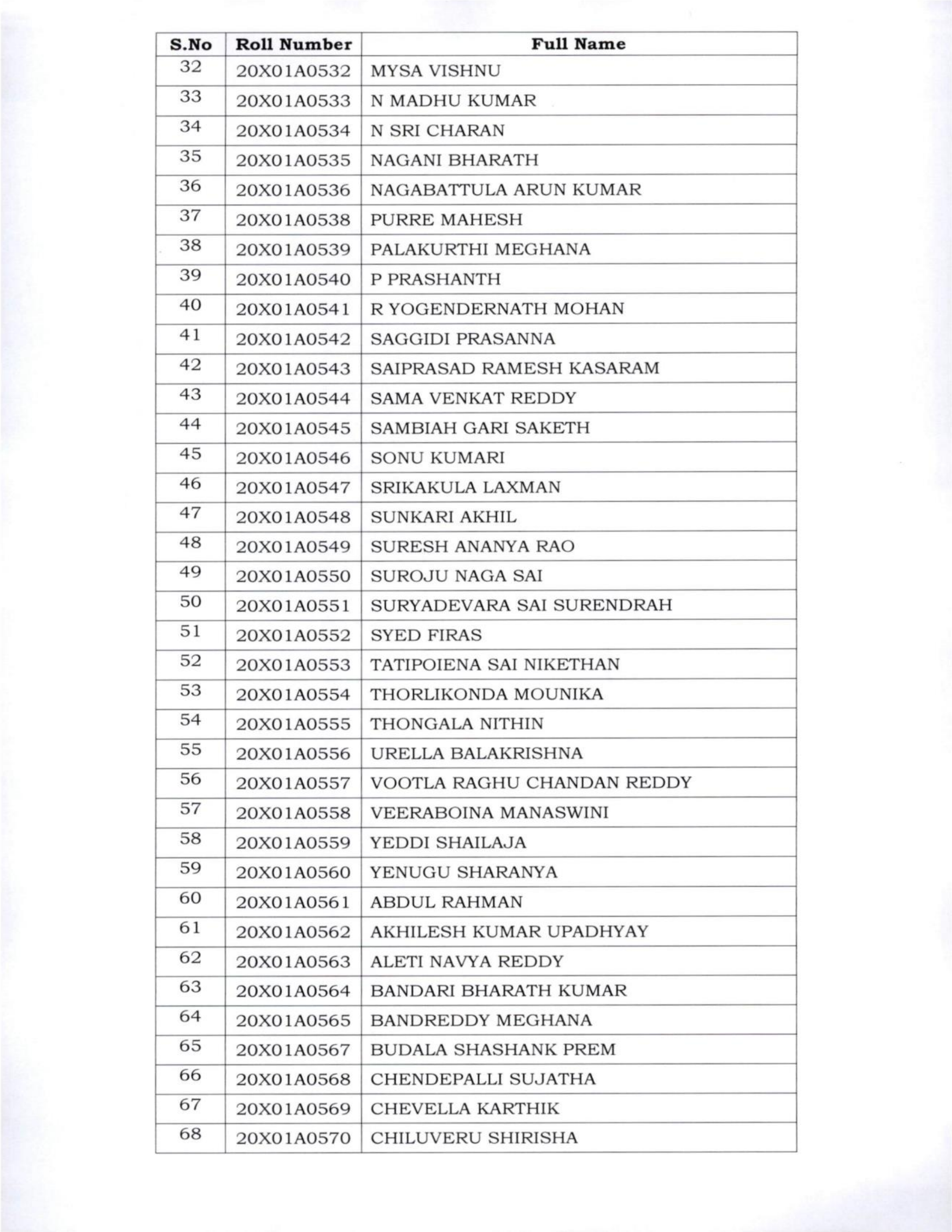
NRCM
Your roots to success...

NARSIMHA REDDY ENGINEERING COLLEGE
UGC-AUTONOMOUS INSTITUTION

An **Autonomous** Institute
NAAC Accreditation **'A'** Grade
Accredited by **NBA**
Approved by **AICTE**, Affiliated to **JNTUH**

PROMOTION LIST (2023-2024) – IV B.Tech, I Semester
COMPUTER SCIENCE AND ENGINEERING

S.No	Roll Number	Full Name
1	20X01A0501	AMBIGALLA MAHESH
2	20X01A0502	ALETI YASHWANTH REDDY
3	20X01A0503	DUMPAATI ABHIRAM
4	20X01A0504	BIJENDRA SINGH YADAV
5	20X01A0505	BOMMAGANI JAGADEESH
6	20X01A0506	BOMMI AMULYA
7	20X01A0507	BUDUGU BHASKAR YADAV
8	20X01A0508	BURGU SRINIDHI
9	20X01A0509	KADALI CHENNA KESAVA
10	20X01A0510	CHANGAL SAI HARSHAVARDHAN GOUD
11	20X01A0511	DODDIPALLI MANOHAR
12	20X01A0512	D NIKHIL REDDY
13	20X01A0513	GIMKA PRIYANKA
14	20X01A0514	GIRUGULA VISHNU DEEPAK
15	20X01A0515	GODISHELA SAI MANAS GOUD
16	20X01A0516	GONDALLE PAVAN KUMAR
17	20X01A0517	GUNNAM LOHITHA
18	20X01A0518	KAKARLA CHENNA KESHAVA REDDY
19	20X01A0519	KALALI LAKSHMI NARASIMHA GOUD
20	20X01A0520	KALLURI TEJA
21	20X01A0521	KATARI VIVEK VARMA
22	20X01A0522	KANDUKURI SUVARNA
23	20X01A0523	KASTHURI NIHARIKA
24	20X01A0524	KATURI CHANDHANA
25	20X01A0525	KAMTAM VAISHNAVI
26	20X01A0526	MANGALI KAVYA
27	20X01A0527	M POOJITHA
28	20X01A0528	MADTHANAPETA ABHINAY
29	20X01A0529	MAILAGANI PRANAY KUMAR
30	20X01A0530	MAMIDALA LAVAKISHOR
31	20X01A0531	MANAPURAM SAI ROHITH



S.No	Roll Number	Full Name
32	20X01A0532	MYSA VISHNU
33	20X01A0533	N MADHU KUMAR
34	20X01A0534	N SRI CHARAN
35	20X01A0535	NAGANI BHARATH
36	20X01A0536	NAGABATTULA ARUN KUMAR
37	20X01A0538	PURRE MAHESH
38	20X01A0539	PALAKURTHI MEGHANA
39	20X01A0540	P PRASHANTH
40	20X01A0541	R YOGENDERNATH MOHAN
41	20X01A0542	SAGGIDI PRASANNA
42	20X01A0543	SAIPRASAD RAMESH KASARAM
43	20X01A0544	SAMA VENKAT REDDY
44	20X01A0545	SAMBIAH GARI SAKETH
45	20X01A0546	SONU KUMARI
46	20X01A0547	SRIKAKULA LAXMAN
47	20X01A0548	SUNKARI AKHIL
48	20X01A0549	SURESH ANANYA RAO
49	20X01A0550	SUROJU NAGA SAI
50	20X01A0551	SURYADEVARA SAI SURENDRAH
51	20X01A0552	SYED FIRAS
52	20X01A0553	TATIPOIENA SAI NIKETHAN
53	20X01A0554	THORLIKONDA MOUNIKA
54	20X01A0555	THONGALA NITHIN
55	20X01A0556	URELLA BALAKRISHNA
56	20X01A0557	VOOTLA RAGHU CHANDAN REDDY
57	20X01A0558	VEERABOINA MANASWINI
58	20X01A0559	YEDDI SHAILAJA
59	20X01A0560	YENUGU SHARANYA
60	20X01A0561	ABDUL RAHMAN
61	20X01A0562	AKHILESH KUMAR UPADHYAY
62	20X01A0563	ALETI NAVYA REDDY
63	20X01A0564	BANDARI BHARATH KUMAR
64	20X01A0565	BANDREDDY MEGHANA
65	20X01A0567	BUDALA SHASHANK PREM
66	20X01A0568	CHENDEPALLI SUJATHA
67	20X01A0569	CHEVELLA KARTHIK
68	20X01A0570	CHILUVERU SHIRISHA

S.No	Roll Number	Full Name
106	20X01A05B0	NAVYA SRI REPAKA
107	20X01A05B1	REGURI MANIVAS
108	20X01A05B2	SATTI RAMPRASAD REDDY
109	20X01A05B3	SANDILKUMAR JAYA SURYA
110	20X01A05B4	SAMMIDI SAI PRAPOORNA
111	20X01A05B5	SANGAM PRAVALIKA
112	20X01A05B6	SARA RAHUL
113	20X01A05B7	THATIPAMULA VISHNUVARDHAN GOUD
114	20X01A05B8	TELIKAPALLI JAYA KRISHNA
115	20X01A05B9	VADDALA VAISHNAVI
116	20X01A05C0	VANAM ADARSH REDDY
117	20X01A05C1	AMARAGONDA ARUN KUMAR
118	20X01A05C2	AMUGOTHU THIRUPATHI
119	20X01A05C4	BALIJA VAMSHI KRISHNA
120	20X01A05C5	BANOTH PAVAN
121	20X01A05C6	BALLA AKASH
122	20X01A05C7	BANALA ARJUN REDDY
123	20X01A05C8	CHINTHALA ARTHI
124	20X01A05C9	CHITYALA UDAY
125	20X01A05D0	DOSAVADA SAI KIRAN
126	20X01A05D1	DYAVARASHETTY MADHURI
127	20X01A05D2	GANGAM CHARANYA REDDY
128	20X01A05D3	GADDAM AMULYA REDDY
129	20X01A05D4	GOTTIMUKKULA SHRAVAN KUMAR
130	20X01A05D5	GUNDAVARAPU UDAYA SAI SREE
131	20X01A05D6	G A SRI DIKSHA
132	20X01A05D7	JAYAM GOUTHAM MUNINDRA
133	20X01A05D8	JEEDI NARESH GOUD
134	20X01A05D9	KONINTI SHRUTHI
135	20X01A05E0	KOTHALU BHARGAVI
136	20X01A05E1	KOTHAPALLY HARIN
137	20X01A05E2	KUMMITHI LOKESH KUMAR REDDY
138	20X01A05E3	KUNCHALA SAI ROHITH
139	20X01A05E4	KUROJU LUCKY
140	20X01A05E5	KURRA AMULYA
141	20X01A05E6	MAMIDI RAJITHA
142	20X01A05E7	METTU KEERTHANA REDDY

S.No	Roll Number	Full Name
143	20X01A05E8	MIRZA SHOEBULLAH BAIG
144	20X01A05F0	VANKADOTH POOJITHA
145	20X01A05F1	GEDDADA VENKAT
146	20X01A05F2	M SATHISH
147	20X01A05F3	SOURAB KUMAR
148	20X01A05F4	DEVIREDDY KETHAN REDDY
149	20X01A05F5	RAZEEQ MOHD
150	20X01A05F6	SINGA RAHUL
151	20X01A05F7	A MAHESH
152	20X01A05F8	KAMBOJA GOUTHAM
153	20X01A05F9	ADEPU SANJAY
154	20X01A05G0	RAYASAM MOHANA KRISHNA
155	20X01A05G1	AKULA AKHIL
156	20X01A05G2	J BHARATH
157	20X01A05G3	INDURTHI NARAYANA REDDY
158	20X01A05G6	ALE SAI DEEPAK
159	20X01A05G7	PEDDYREDDY PAVAN REDDY
160	20X01A05G8	ANNAM ADHARSH
161	21X05A0501	ABBAGOUNI NITHIN GOUD
162	21X05A0502	ASANTI SUMANTH
163	21X05A0503	BANOTH DINESH NAIK
164	21X05A0504	BARENKALA GURU CHARAN
165	21X05A0505	BASA VAMSHI
166	21X05A0506	CHUKKA KARTHIK
167	21X05A0507	DASARI NAGA RAJU
168	21X05A0508	DONTHRABOINA SHIREESHA
169	21X05A0509	GAJJALA VENKAT NARASIMHA REDDY
170	21X05A0510	GUJJARI ANUSHA
171	21X05A0511	JAIN ROHAN
172	21X05A0512	KAMMARI PRAVEEN
173	21X05A0513	KARRA JEEVAN
174	21X05A0514	KASHI RIMPU
175	21X05A0515	KISHTAMGARU NITHIN
176	21X05A0516	KOTAKADI CHANDRA SHEKAR
177	21X05A0517	KOVVURI AJAY
178	21X05A0518	MADDELA KIRAN VISHWANATH
179	21X05A0519	MADUGULA SAI TEJA

S.No	Roll Number	Full Name
180	21X05A0520	MARABOINA SANDEEP
181	21X05A0521	MD ALTHAF
182	21X05A0522	MEDIGE SIDHU
183	21X05A0523	MEKALA JATHIN KUMAR YADAV
184	21X05A0524	NAMPELLI RANJITH
185	21X05A0525	NITTA ARAVIND
186	21X05A0526	PADYALA RAGHU RAM
187	21X05A0527	PANTHULU LUCKY RAJ
188	21X05A0528	PITTALA MANI KEERTHANA
189	21X05A0529	R PAVAN REDDY
190	21X05A0530	THUKKOJI MANASA

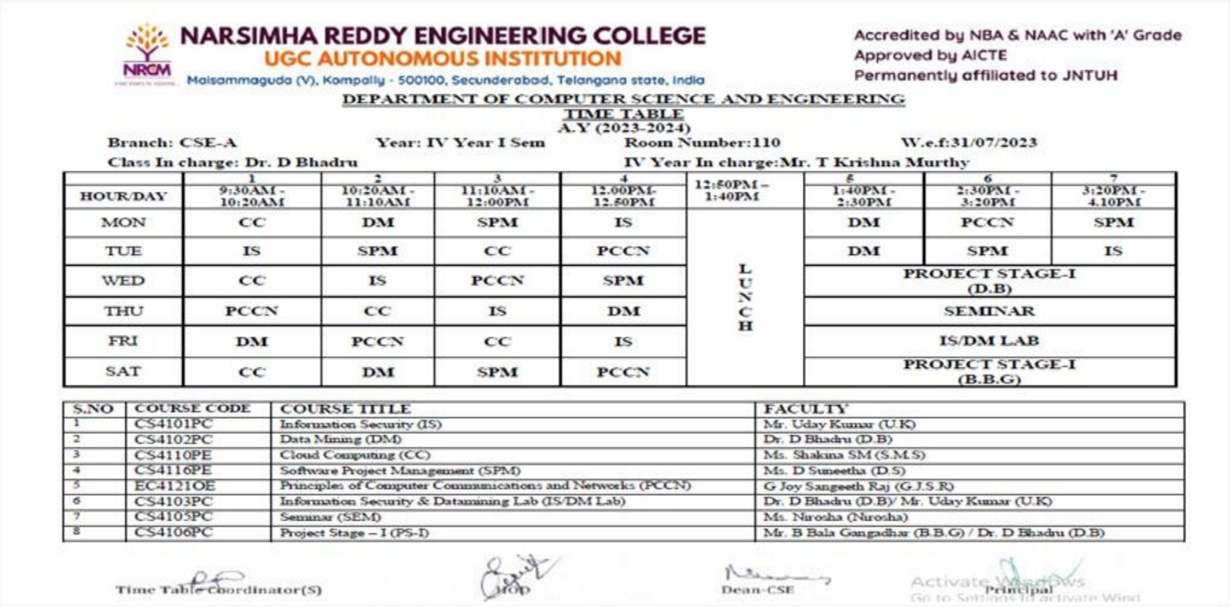
Note: As per the Academic Regulation of NR20 the students who got less credits than the stipulated credits for the promotion from III B.Tech to IV B.Tech will be detained after announcement of Regular & Supplementary Results. Hence, all the Head's and students please make a note of it. **Detained list due to shortage of credit and revised Nominal Rolls will be circulated immediately after declaration of results.**

PRINCIPAL

PRINCIPAL
ARASIMHA REDDY ENGINEERING COLLEGE
UGC AUTONOMOUS
Survey No.518, Maisammaguda (V), Dhulapally (P),
Medchal (M), Medchal Dist., Hyderabad-500100

6.CLASS TIME TABLE

IV CSE A:



NARSIMHA REDDY ENGINEERING COLLEGE
UGC AUTONOMOUS INSTITUTION
Maisammaguda (V), Kompally - 500100, Secunderabad, Telangana state, India

Accredited by NBA & NAAC with 'A' Grade
Approved by AICTE
Permanently affiliated to JNTUH

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
TIME TABLE
A.Y (2023-2024)

Branch: CSE-A Year: IV Year I Sem Room Number:110 W.e.f:31/07/2023

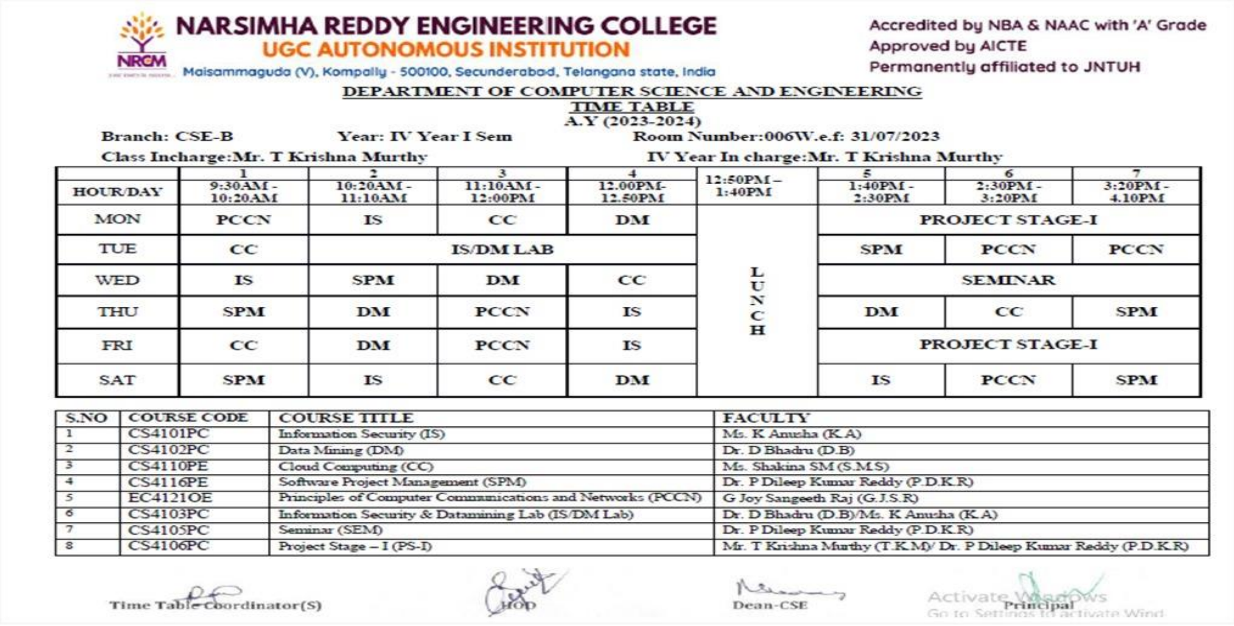
Class In charge: Dr. D Bhadru IV Year In charge:Mr. T Krishna Murthy

	1	2	3	4	12:50PM – 1:40PM	5	6	7
HOUR/DAY	9:30AM - 10:20AM	10:20AM - 11:10AM	11:10AM - 12:00PM	12.00PM- 12.50PM		1:40PM - 2:30PM	2:30PM - 3:20PM	3:20PM - 4.10PM
MON	CC	DM	SPM	IS	LUNCH	DM	PCCN	SPM
TUE	IS	SPM	CC	PCCN		DM	SPM	IS
WED	CC	IS	PCCN	SPM		PROJECT STAGE-I (D.B)		
THU	PCCN	CC	IS	DM		SEMINAR		
FRI	DM	PCCN	CC	IS		IS/DM LAB		
SAT	CC	DM	SPM	PCCN		PROJECT STAGE-I (B.B.G)		

S.NO	COURSE CODE	COURSE TITLE	FACULTY
1	CS4101PC	Information Security (IS)	Mr. Uday Kumar (U.K)
2	CS4102PC	Data Mining (DM)	Dr. D Bhadru (D.B)
3	CS4110PE	Cloud Computing (CC)	Ms. Shakina SM (S.M.S)
4	CS4116PE	Software Project Management (SPM)	Ms. D Suneetha (D.S)
5	EC4121OE	Principles of Computer Communications and Networks (PCCN)	G Joy Sangeeth Raj (G.J.S.R)
6	CS4103PC	Information Security & Datamining Lab (IS/DM Lab)	Dr. D Bhadru (D.B)/ Mr. Uday Kumar (U.K)
7	CS4105PC	Seminar (SEM)	Ms. Nirosha (Nirosha)
8	CS4106PC	Project Stage – I (PS-I)	Mr. B Bala Gangadhar (B.B.G) / Dr. D Bhadru (D.B)

Time Table Coordinator(S) HOD Dean-CSE Principal

IV CSE B



NARSIMHA REDDY ENGINEERING COLLEGE
UGC AUTONOMOUS INSTITUTION
Maisammaguda (V), Kompally - 500100, Secunderabad, Telangana state, India

Accredited by NBA & NAAC with 'A' Grade
Approved by AICTE
Permanently affiliated to JNTUH

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
TIME TABLE
A.Y (2023-2024)

Branch: CSE-B Year: IV Year I Sem Room Number:006W.e.f: 31/07/2023

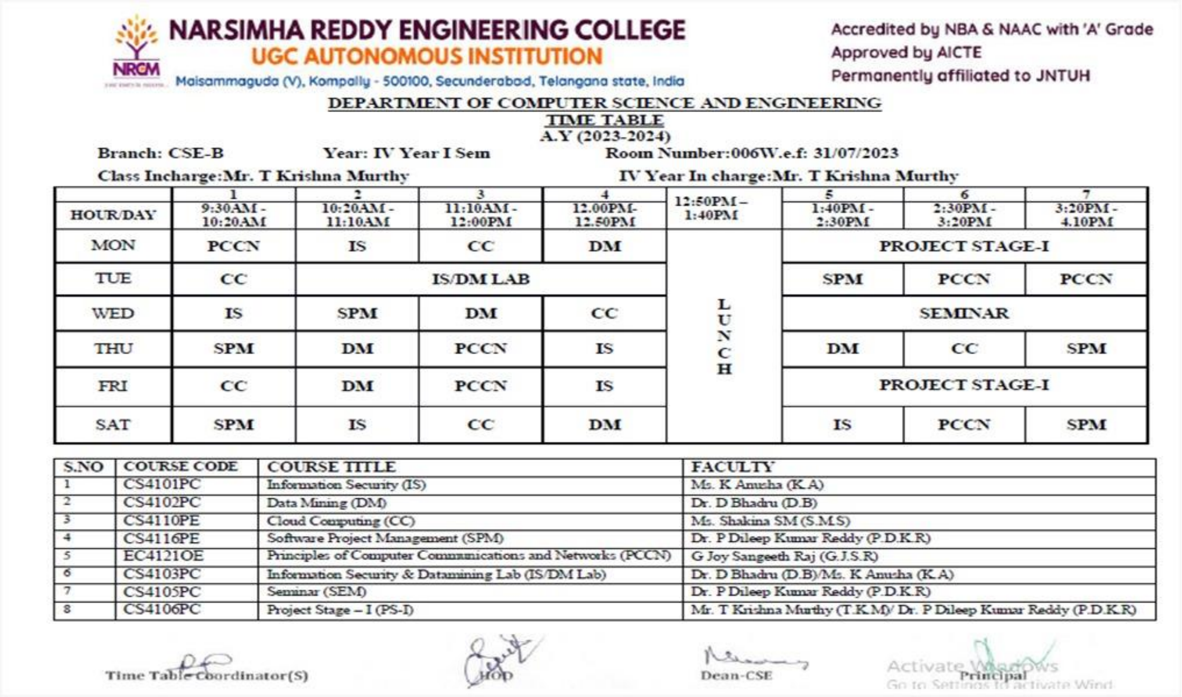
Class Incharge:Mr. T Krishna Murthy IV Year In charge:Mr. T Krishna Murthy

	1	2	3	4	12:50PM – 1:40PM	5	6	7
HOUR/DAY	9:30AM - 10:20AM	10:20AM - 11:10AM	11:10AM - 12:00PM	12.00PM- 12.50PM		1:40PM - 2:30PM	2:30PM - 3:20PM	3:20PM - 4.10PM
MON	PCCN	IS	CC	DM	LUNCH	PROJECT STAGE-I		
TUE	CC	IS/DM LAB				SPM	PCCN	PCCN
WED	IS	SPM	DM	CC		SEMINAR		
THU	SPM	DM	PCCN	IS		DM	CC	SPM
FRI	CC	DM	PCCN	IS		PROJECT STAGE-I		
SAT	SPM	IS	CC	DM		IS	PCCN	SPM

S.NO	COURSE CODE	COURSE TITLE	FACULTY
1	CS4101PC	Information Security (IS)	Ms. K Anusha (K.A)
2	CS4102PC	Data Mining (DM)	Dr. D Bhadru (D.B)
3	CS4110PE	Cloud Computing (CC)	Ms. Shakina SM (S.M.S)
4	CS4116PE	Software Project Management (SPM)	Dr. P Dileep Kumar Reddy (P.D.K.R)
5	EC4121OE	Principles of Computer Communications and Networks (PCCN)	G Joy Sangeeth Raj (G.J.S.R)
6	CS4103PC	Information Security & Datamining Lab (IS/DM Lab)	Dr. D Bhadru (D.B)/Ms. K Anusha (K.A)
7	CS4105PC	Seminar (SEM)	Dr. P Dileep Kumar Reddy (P.D.K.R)
8	CS4106PC	Project Stage – I (PS-I)	Mr. T Krishna Murthy (T.K.M)/ Dr. P Dileep Kumar Reddy (P.D.K.R)

Time Table Coordinator(S) HOD Dean-CSE Principal

IV CSE C:



NARSIMHA REDDY ENGINEERING COLLEGE
UGC AUTONOMOUS INSTITUTION
Maisammaguda (V), Kompally - 500100, Secunderabad, Telangana state, India

Accredited by NBA & NAAC with 'A' Grade
Approved by AICTE
Permanently affiliated to JNTUH

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
TIME TABLE
A.Y (2023-2024)

Branch: CSE-B Year: IV Year I Sem Room Number:006W.e.f: 31/07/2023

Class Incharge:Mr. T Krishna Murthy IV Year In charge:Mr. T Krishna Murthy

	1	2	3	4	12:50PM – 1:40PM	5	6	7
HOUR/DAY	9:30AM - 10:20AM	10:20AM - 11:10AM	11:10AM - 12:00PM	12.00PM- 12.50PM		1:40PM - 2:30PM	2:30PM - 3:20PM	3:20PM - 4.10PM
MON	PCCN	IS	CC	DM	LUNCH	PROJECT STAGE-I		
TUE	CC	IS/DM LAB				SPM	PCCN	PCCN
WED	IS	SPM	DM	CC		SEMINAR		
THU	SPM	DM	PCCN	IS		DM	CC	SPM
FRI	CC	DM	PCCN	IS		PROJECT STAGE-I		
SAT	SPM	IS	CC	DM		IS	PCCN	SPM

S.NO	COURSE CODE	COURSE TITLE	FACULTY
1	CS4101PC	Information Security (IS)	Ms. K Anusha (K.A)
2	CS4102PC	Data Mining (DM)	Dr. D Bhadru (D.B)
3	CS4110PE	Cloud Computing (CC)	Ms. Shakina SM (S.M.S)
4	CS4116PE	Software Project Management (SPM)	Dr. P Dileep Kumar Reddy (P.D.K.R)
5	EC4121OE	Principles of Computer Communications and Networks (PCCN)	G Joy Sangeeth Raj (G.J.S.R)
6	CS4103PC	Information Security & Datamining Lab (IS/DM Lab)	Dr. D Bhadru (D.B)/Ms. K Anusha (K.A)
7	CS4105PC	Seminar (SEM)	Dr. P Dileep Kumar Reddy (P.D.K.R)
8	CS4106PC	Project Stage – I (PS-I)	Mr. T Krishna Murthy (T.K.M)/ Dr. P Dileep Kumar Reddy (P.D.K.R)

Time Table Coordinator(S) HOD Dean-CSE Principal

7. DETAILED LECTURE PLAN (2023-24)

IV CSE B

S.No	UNIT NO	PROPOSED DATE	TOPICS TO BE COVERED	NO OF CLASSES REQUIRED	REFERENCE	DELIVERY METHOD	ACTUAL DAT	REMRKS
	Module-1 **Security Concepts**							
1	I	31-07-2023	Introduction	1	T1,R1	C&T		
2	I	02-08-2023	The need for security Security approaches Principles of security	1	T1,R1	PPT		
3	I	04-08-2023	Types of Security attacks : Pasive attacks Active attacks	1	T1,R1	C&T		
					T1,R1	C&T		
4	I	07-08-2023	Security services	1	T1,R1	PPT		
5	I	09-08-2023	Security Mechanisms	1	T1,R1	C&T		
6	I	10-08-2023	A model for NetworkSecurity	1	T1,R1	PPT		
7	I	12-08-2023	Cryptography Conceptsand Techniques: Introduction	1	T1,R1	C&T		
8	I	14-08-2023	substitution techniques	2	T1,R1	C&T		
9	I	16-08-2023			T1,R1	C&T		
10	I	17-08-2023	transposition techniques	2	T1,R1	C&T		
11	I	18-08-2023			T1,R1	C&T		
12	I	19-08-2023	encryption anddecryption	1	T1,R1	C&T		
13	I	21-8-2023	symmetric and asymmetric key cryptography	1	T1,R1	C&T		
14	I	23-8-2023	steganography	1	T1,R1	C&T		
Module-II Symmetric cryptography								

15	II	24-9-2023	Block Cipher principles	1	T1,R1	C&T			
16	II	25-9-2023	DES	1	T1,R1	C&T			
17	II	26-8-2023	AES	1	T1,R1	C&T			
18	II	28-8-2023	Blowfish	.1	T1,R1	C&T			
19	II	30-8-2023	RC5	1	T1,R1	C&T			
20	II	31-8-2023	IDEA	1	T1,R1	C&T			
21	II	2-9-2023	Block cipher operation	1	T1,R1	C&T			
22	II	4-9-2023	Stream ciphers	1	T1,R1	C&T			
23	II	6-9-2023	RC4	1	T1,R1	C&T			
24	II	9-9-2023	Principles of public key cryptosystems	1	T1,R1	C&T			
25	II	11-9-2023	RSA algorithm	1	T1,R1	C&T			
26	II	13-9-2023	Elgamal Cryptography	1	T1,R1	PPT			
27	II	14-9-2023	Diffie- Hellman KeyExchange, Algorithm	1	T1,R1	C&T			
28	II	15-9-2023	Knapsack algorithm	1	T1,R1	C&T			
Module-III Cryptographic Hash function									
29	III	16-9-2023	Message Authentication	2	T1,R1	C&T			
30	III	20-9-2023	Message Authentication		T1,R1	PPT			
31	III	22-9-2023	Secure Hash Algorithm(SHA-512)	2	T1,R1	C&T			
32	III	25-9-2023	Secure Hash Algorithm(SHA-512)		T1,R1	C&T			
33	III	30-9-2023	Message authentication codes:	2	T1,R1	C&T			
34	III	4-10-2023	Message authentication codes:		T1,R1	PPT			
35	III	9-10-2023	Authentication requirements	1	T1,R1	C&T			
36	III	11-10-2023	HMAC	1	T1,R1	C&T			

37	III	13-10-2023	CMAC	1	T1,R1	C&T		
38	III	16-10-2023	Digital signatures	2	T1,R1	C&T		
39	III	16-10-2023	Digital signatures		T1,R1	C&T		
40	III	19-10-2023	Elgamal Digital SignatureScheme		T1,R1	C&T		
41	III	21-10-2023	**Key Management and Distribution:**	1	T1,R1	C&T		
42	III	30-10-2023	Symmetric Key Distribution Using Symmetric Encryption	1	T1,R1	C&T		
43	III	1-11-2023	Symmetric Key Distribution using Asymmetric Encryption	1	T1,R1	C&T		
44	III	2-11-2023	Distribution of Public Keys	1	T1,R1	C&T		
45	III	3-11-2023	Kerberos	1	T1,R1	C&T		
46	III	4-11-2023	X.509 AuthenticationService,	1	T1,R1	C&T		
47	III	6-11-2023	Public–Key Infrastructure	1	T1,R1	C&T		
Module –IV Transport layer security								
48	IV	8-11-2023	Web security considerations	1	T1,R1	C&T		
49	IV	10-11-2023	Secure Socket Layer	2	T1,R1	C&T		
50	IV	11-11-23	Security Transport		T1,R1	C&T		
51	IV	13-11-23	HTTP	1	T1,R1	C&T		
52	IV	15-11-23	Secure Shell (SSH)	1	T1,R1	C&T		
53	IV	16-11-23	**Wireless NetworkSecurity:** Wireless Security,	1	T1,R1	C&T		
54	IV	17-11-23	Mobile Device Security	1	T1,R1	C&T		
55	IV	18-11-23	IEEE802.11 Wireless LAN	1	T1,R1	C&T		

56	IV	20-11-23	IEEE802.11i Wireless LAN Security	1	T1,R1	C&T		
Module-V **E-mail Security**								
57	V	25-11-23	Pretty Good Privacy	1	T1,R1	C&T		
58	V	27-11-23	S/MIME	1	T1,R1	C&T		
59	V	29-11-23	IPSecurity: IP Security overview,	1	T1,R1	C&T		
60	V	1-12-23	Authentication Header	1	T1,R1	C&T		
61	V	2-12-23	Encapsulating security Payload, Combining security associations	1	T1,R1	C&T		
62	V	4-12-23	Internet Key Exchange, Secure Multiparty Calculation	1	T1,R1	C&T		
63	V	6-12-23	, Virtual Elections	1	T1,R1	C&T		
64	V	7-12-23	Single sign On	1	T1,R1	C&T		
65	V	8-12-23	Secure Inter-branch Payment Transactions, Cross site Vulnerability	1	T1,R1	C&T		
Total Hours				**65**				

LESSON PLAN: IV CSE C

S.No	UNIT NO	PROPOSED DATE	TOPICS TO BE COVERED	NO OF CLASSES REQUIRED	REFERENCE	DELIVERY METHOD	ACTUAL DAT	REMRKS
	Module-1 **Security Concepts**							
1	I	31-07-2023	Introduction	1	T1,R1	C&T		
2	I	3-8-2023	The need for security Security approaches Principles of security	1	T1,R1	PPT		
3	I	4-8-2023	Types of Security attacks : Pasive attacks Active attacks	1	T1,R1 T1,R1	C&T C&T		
4	I	4-8-2023	Security services	1	T1,R1	PPT		
5	I	5-08-2023	Security Mechanisms	1	T1,R1	C&T		
6	I	7-08-2023	A model for NetworkSecurity	1	T1,R1	PPT		
7	I	7-08-2023	Cryptography Conceptsand Techniques: Introduction	1	T1,R1	C&T		
8	I	10-08-2023	substitution techniques	2	T1,R1	C&T		
9	I	11-08-2023			T1,R1	C&T		
10	I	12-08-2023	transposition techniques	2	T1,R1	C&T		
11	I	14-08-2023			T1,R1	C&T		
12	I	14-08-2023	encryption anddecryption	1	T1,R1	C&T		
13	I	17-08-2023	symmetric and asymmetric key cryptography	1	T1,R1	C&T		
14	I	18-08-2023	steganography	1	T1,R1	C&T		
Module-II Symmetric cryptography								
15	II	21-08-2023	Block Cipher principles	1	T1,R1	C&T		
16	II	24-08-2023	DES	1	T1,R1	C&T		
17	II	25-08-2023	AES	1	T1,R1	C&T		

18	II	26-08-2023	Blowfish	.1	T1,R1	C&T		
19	II	28-08-2023	RC5	1	T1,R1	C&T		
20	II	01-09-2023	IDEA	1	T1,R1	C&T		
21	II	01-09-2023	Block cipher operation	1	T1,R1	C&T		
22	II	02-09-2023	Stream ciphers	1	T1,R1	C&T		
23	II	04-09-2023	RC4	1	T1,R1	C&T		
24	II	07-09-2023	Principles of public key cryptosystems	1	T1,R1	C&T		
25	II	08-09-2023	RSA algorithm	1	T1,R1	C&T		
26	II	09-09-2023	Elgamal Cryptography	1	T1,R1	PPT		
27	II	11-09-2023	Diffie- Hellman Key Exchange, Algorithm	1	T1,R1	C&T		
28	II	15-09-2023	Knapsack algorithm	1	T1,R1	C&T		
Module-III Cryptographic Hash function								
29	III	16-09-2023	Message Authentication	2	T1,R1	C&T		
30	III	18-09-2023	Message Authentication		T1,R1	PPT		
31	III	21-09-2023	Secure Hash Algorithm(SHA-512)	2	T1,R1	C&T		
32	III	22-09-2023	Secure Hash Algorithm(SHA-512)		T1,R1	C&T		
33	III	23-09-2023	Message authentication codes:	2	T1,R1	C&T		
34	III	25-09-2023	Message authentication codes:		T1,R1	PPT		
35	III	25-09-2023	Authentication requirements	1	T1,R1	C&T		
36	III	28-09-2023	HMAC	1	T1,R1	C&T		
37	III	30-09-2023	CMAC	1	T1,R1	C&T		
38	III	09-10-2023	Digital signatures	2	T1,R1	C&T		

39	III	12-10-2023	Digital signatures		T1,R1	C&T		
40	III	13-10-2023	Elgamal Digital Signature Scheme		T1,R1	C&T		
41	III	13-10-2023	**Key Management and Distribution:**	1	T1,R1	C&T		
42	III	14-10-2023	Symmetric Key Distribution Using Symmetric Encryption	1	T1,R1	C&T		
43	III	16-10-2023	Symmetric Key Distribution using Asymmetric Encryption	1	T1,R1	C&T		
44	III	19-10-2023	Distribution of Public Keys	1	T1,R1	C&T		
45	III	20-10-2023	Kerberos	1	T1,R1	C&T		
46	III	20-10-2023	X.509 Authentication Service,	1	T1,R1	C&T		
47	III	30-10-2023	Public–Key Infrastructure	1	T1,R1	C&T		
Module –IV Transport layer security								
48	IV	03-11-2023	Web security considerations	1	T1,R1	C&T		
49	IV	03-11-2023	Secure Socket Layer	2	T1,R1	C&T		
50	IV	04-11-2023	Security Transport		T1,R1	C&T		
51	IV	06-11-2023	HTTP	1	T1,R1	C&T		
52	IV	10-11-2023	Secure Shell (SSH)	1	T1,R1	C&T		
53	IV	11-11-2023	**Wireless Network Security:** Wireless Security,	1	T1,R1	C&T		
54	IV	13-11-2023	Mobile Device Security	1	T1,R1	C&T		
55	IV	16-11-2023	IEEE802.11 Wireless LAN	1	T1,R1	C&T		
56	IV	17-11-2023	IEEE802.11i Wireless LAN Security	1	T1,R1	C&T		
Module-V **E-mail Security**								
57	V	18-11-2023	Pretty Good Privacy	1	T1,R1	C&T		

58	V	20-11-2023	S/MIME	1	T1,R1	C&T		
59	V	20-11-2023	IPSecurity: IP Security overview,	1	T1,R1	C&T		
60	V	23-11-2023	Authentication Header	1	T1,R1	C&T		
61	V	24-11-2023	Encapsulating security Payload, Combining security associations	1	T1,R1	C&T		
62	V	27-11-2023	Internet Key Exchange, Secure Multiparty Calculation	1	T1,R1	C&T		
63	V	30-11-2023	, Virtual Elections	1	T1,R1	C&T		
64	V	01-12-2023	Single sign On	1	T1,R1	C&T		
65	V	01-12-2023	Secure Inter-branch Payment Transactions, Cross site Vulnerability	1	T1,R1	C&T		
			Total Hours	**65**				

8.Unit wise Question Bank

UNIT-I

S.No		Questions	BT	CO	PO
Part –A(Short Answer Questions)					
1		Define cryptanalysis and cryptology.	L1	CO1	PO1,PO6
2		What is masquerade?	L1	CO1	PO1,PO6
3		Define passive attack and active attack.	L1	CO1	PO1,PO6
4		Define Denial of service.	L1	CO1	PO1,PO6
5		What is steganography? Mention few techniques in it.	L1	CO1	PO1,PO6
6		Mention few mono-alphabetic and poly-alphabetic ciphers.	L1	CO1	PO1,PO6
7		Define Threat and attack. List out what are the attacks that canbe performed in network.	L1	CO1	PO1,PO6
8		Convert the Given Text “CRYPTOGRAPHY” into cipher text using Rail fence Technique.	L3	CO1	PO1,PO6
9		Define security attack, security mechanism and security services.	L1	CO1	PO1,PO6
10		Define the two basic building blocks of encryption techniques	L1	CO1	PO1,PO6
Part– B(Long Answer Questions)					
11	a)	Explain in detail about OSI security architecture.	L2	CO1	PO1,PO6
	b)	Explain classical encryption techniques (Steps involved in each encryption technique like Caesar cipher, playfair cipher, hill cipher, vigenere cipher, one time pad cipher, rail fence, etc)	L2	CO1	PO1,PO6
12	a)	Explain about steganography, transposition cipher.	L2	CO1	PO1,PO6
	b)	Write short notes on security mechanisms	L6	CO1	PO1,PO6
13	a)	Explain about substitution ciphers in detail with an example.	L2	CO1	PO1,PO6
	b)	What are the goals of security? Explain in detail about security Services?	L1	CO1	PO1,PO6
14	a)	what is meant by security attack? Explain various types of security attacks.	L1	CO1	PO1,PO6
	b)	Draw a matrix that shows the relationship between security mechanisms and attacks.	L2	CO1	PO1,PO6
15	a)	Explain various transposition ciphers with an example	L2	CO1	PO1,PO6
	b)	Explain any three substitution ciphers with an example.	L2	CO1	PO1,PO6
16	a)	Define Cryptography.What is the need of CIA Triad.	L1	CO1	PO1,PO6
	b)	What are the different levels of losses that occur without CIA Triad.	L1	CO1	PO1,PO6

UNIT– II

Symmetric key cipher, Assymmetric cipher

UNIT_II

S.No		Questions	BT	CO	PO
Part –A(Short Answer Questions)					
1		Define symmetric key cryptography and public key cryptography.	L1	CO2	PO3
2		Define Euler’s totient function (used in RSA algorithm).	L1	CO2	PO3
3		Why do we need Diffie Hellman algorithm?	L2	CO2	PO3
4		Mention the various types of cryptanalytic attack.	L1	CO2	PO3
5		What are the operations used in AES?	L1	CO2	PO3
6		What are the various approaches to attacks the RSA algorithm?	L1	CO2	PO3
7		How to find primitive root with an example.	L3	CO2	PO3
8		What primitive operations are used in RC4	L1	CO2	PO3
9		Compare stream cipher with block cipher with example	L3	CO2	PO3
10		Define Euler’s theorem and its application.	L1	CO2	PO3
Part– B(Long Answer Questions)					
11	a)	Discuss various steps of IDEA algorithm.	L3	CO2	PO3
	b)	Explain Diffie-Hellman key exchange algorithm in detail.	L2	CO2	PO3
12	a)	Explain the steps involved in knapsack algorithm with an example.	L2	CO2	PO3
	b)	Explain in detail about the steps involved in DES.	L2	CO2	PO3
13	a)	Explain Elgamal algorithm in detail.	L2	CO2	PO3
	b)	Discuss different block cipher modes of operation	L3	CO2	PO3
14	a)	Explain in detail about the steps involved in Blowfish.	L2	CO2	PO3
	b)	AES consists of four functions in three layers. Which of the functions are primarily for confusion and which are primarily for diffusion? Which of the layers are for confusion and which are for diffusion? Justify your answers.	L3	CO2	PO3
15	a)	Explain the steps involved in RC4.	L2	CO2	PO3
	b)	Explain RSA algorithm. And perform Encryption and Decryption using RSA p=3 q=11 e=7 M=5	L2	CO2	PO3
16	a)	Explain RC5 algorithm	L2	CO2	PO3
	b)	Differentiate Block cipher and Stream Cipher	L4	CO2	PO3

UNIT-III

Cryptographic hash functions

UNIT-III

S.No	Questions	BT	CO	PO
Part –A(Short Answer Questions)				
1	What is meant by Message Authentication?	L1	CO3	PO2,PO3
2	List out the attack on MAC	L1	CO3	PO2,PO3
3	Define Digital signature	L1	CO3	PO2,PO3
4	What you meant by MAC	L1	CO3	PO2,PO3
5	Differentiate Message Authentication Code and Hash function.	L4	CO3	PO2,PO3
6	What are the two approaches of Digital Signature?	L1	CO3	PO2,PO3
7	Define Hash function .	L1	CO3	PO2,PO3
8	List out the different techniques of distributing the public key	L1	CO3	PO2,PO3

9		Define one way property, weak collision resistance and strong collision resistance of hash function.	L1	CO3	PO2,PO3
10		Define the classes of message authentication function.	L1	CO3	PO2,PO3
Part– B(Long Answer Questions)					
11	a)	With the example, explain in detail about Secure Hash Algorithm	L2	CO3	PO2,PO3
	b)	Explain in detail about HMAC and Digital Signature Standard	L2	CO3	PO2,PO3
12	a)	Give a brief note on basic uses of message authentication code.	L3	CO3	PO2,PO3
	b)	Explain the process involved in message digest generation and processing of single block in SHA512.	L2	CO3	PO2,PO3
13	a)	What is the purpose of digital signature? Explain its properties and requirements.	L1	CO3	PO2,PO3
	b)	Explain the requirements of digital signatures and also discuss how problems related to digital signature are taken care by an arbiter?	L2	CO3	PO2,PO3
14	a)	State and explain the different approaches to message authentication	L3	CO3	PO2,PO3
	b)	Explain the format of X.509v3 certificate and certificate revocation list. Explain each in detail.	L2	CO3	PO2,PO3
15	a)	Explain about characteristics of hash functions	L2	CO3	PO2,PO3
	b)	Explain briefly about Kerberos and give its requirements.	L2	CO3	PO2,PO3
16	a)	Explain in detail about Elgamal Digital signature scheme.	L2	L2	PO2,PO3
	b)	Verify the signature with the Elgamal Digital signature of values q=19,α=10,XA=16,m=14,k=5.	L3	L5	PO2,PO3

UNIT-IV

S.No		Questions	BT	CO	PO
Part –A(Short Answer Questions)					
1		Define transport and tunnel mode.	L1	CO4	PO1,PO3
2		What are the benefits of mobile device security.	L1	CO4	PO1,PO3
3		Mention the phases of the Handshake protocol.	L1	CO4	PO1,PO3
4		Why do we need an anti replay service?	L2	CO4	PO1,PO3
5		What is the use of the change cipher spec protocol?	L1	CO4	PO1,PO3
6		What are the two characteristic of wired LAN that are not inherent in wireless	L1	CO4	PO1,PO3
7		What is the need pf padding in Encapsulating Security Payload (ESP)?	L1	CO4	PO1,PO3
8		What is security association?	L1	CO4	PO1,PO3
9		Define the terms: connection and session.	L1	CO4	PO1,PO3
10		How the security associations be combined?	L3	CO4	PO1,PO3
Part– B(Long Answer Questions)					
11	a)	Briefly explain about transport layer security and Padding.	L2	CO4	PO1,PO3
	b)	With a neat diagram, explain the operation of SSL and SSH Record Protocol.	L2	CO4	PO1,PO3
12	a)	Differentiate SSL & TLS	L4	CO4	PO1,PO3
	b)	Write a short notes on IEEE 802.11 i services.	L6	CO4	PO1,PO3
13	a)	Write a short notes on IEEE 802.11 i Phases of operation.	L6	CO4	PO1,PO3
	b)	Explain in detail, the Handshake protocol in secure socket layer	L2	CO4	PO1,PO3

14	a)	Write a short note on Wireless LAN Security.	L6	CO4	PO1,PO3
	b)	Write a short note on HTTPS.	L6	CO4	PO1,PO3
15	a)	What are the different types of mobile device security. Explain each.	L1	CO4	PO1,PO3
	b)	How does mobile device security work?	L3	CO4	PO1,PO3
16	a)	Explain in detail about SSL	L2	CO4	PO1,PO3
	b)	What is the importance of providing Security for wireless LAN	L1	CO4	PO1,PO3

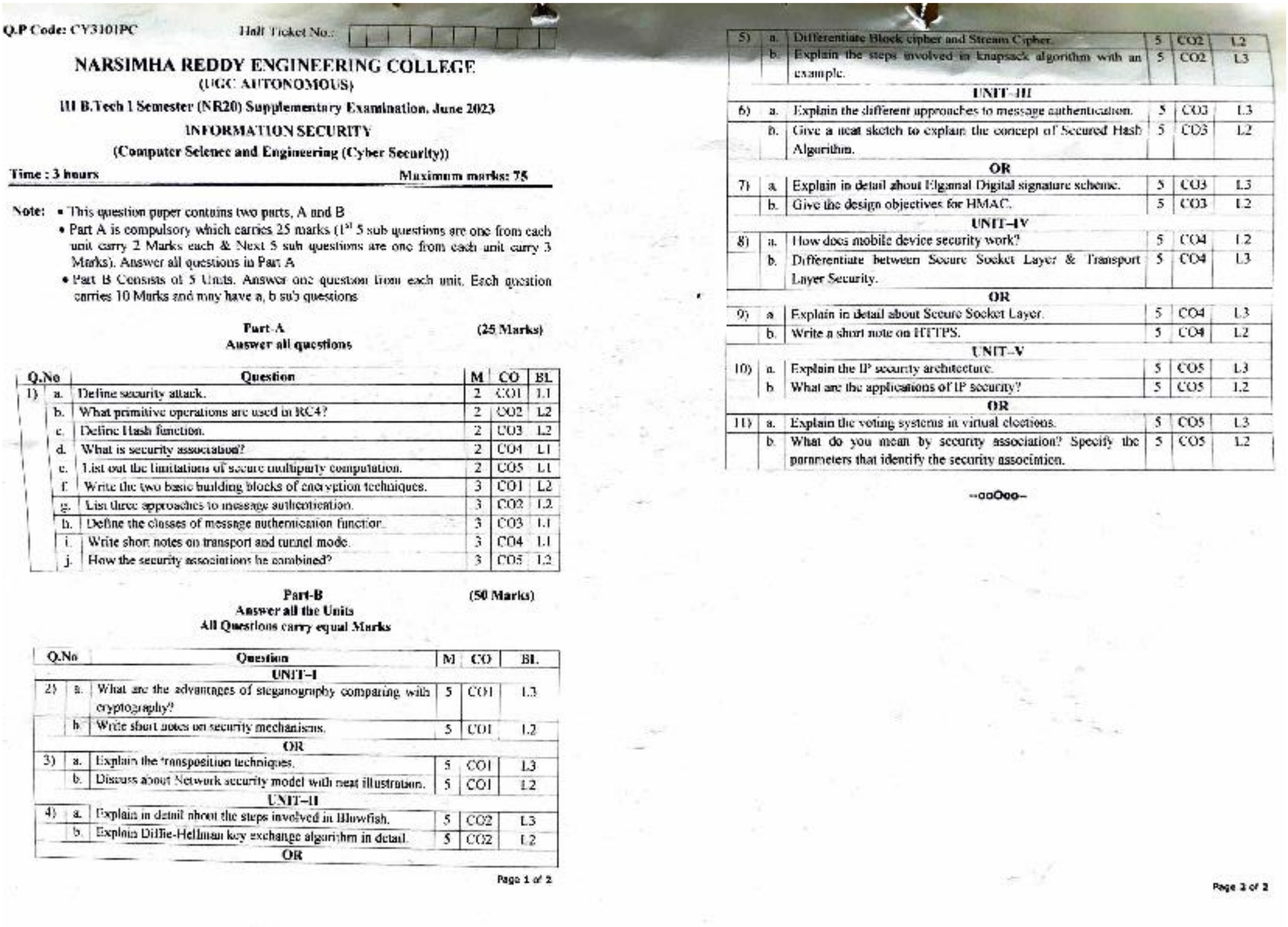
UNIT-
V

Email security

S.No		Questions	BT	CO	PO
Part –A(Short Answer Questions)					
		Mention the services provided by the Pretty Good Privacy (PGP).	L1	CO5	PO5,PO6 ,PO7
2		What are the notations of PGP?	L1	CO5	PO5,PO6 ,PO7
3		What do you mean by IKE.	L1	CO5	PO5,PO6 ,PO7
4		Classify the intruders.	L3	CO5	PO5,PO6 ,PO7
5		How E-mail compatibility is performed?	L3	CO5	PO5,PO6 ,PO7
6		How the password files be protected?	L3	CO5	PO5,PO6 ,PO7
7		List out the limitations of secure multiparty computation.	L1	CO5	PO5,PO6 ,PO7
8		Mention the benefits of IPSec.	L1	CO5	PO5,PO6 ,PO7
9		Define cross site scripting vulnerability.	L1	CO5	PO5,PO6 ,PO7
10		Define different types of voting systems in virtual elections.	L1	CO5	PO5,PO6 ,PO7
Part– B(Long Answer Questions)					
11	a)	Name the protocols that provide security in IPSec.	L2	CO5	PO5,PO6 ,PO7
	b)	Write short notes on PGP.	L6	CO5	PO5,PO6 ,PO7
12	a)	Explain in detail about IP Security Policy	L2	CO5	PO5,PO6 ,PO7
	b)	Explain how S/MIME differs form MIME	L2	CO5	PO5,PO6 ,PO7
13	a)	What are the design goals for a firewall? Also mention its Limitations	L1	CO5	PO5,PO6 ,PO7
	b)	List the five important features of IKE key determination algorithm	L1	CO5	PO5,PO6 ,PO7
14	a)	Write a short note on cross site scripting vulnerability.	L6	CO5	PO5,PO6 ,PO7

	b)	Explain secure inter branch payment transactions.	L2	CO5	PO5,PO6,PO7
15	a)	Explain the secure multiparty calculation..	L2	CO5	PO5,PO6,PO7
	b)	Write a short note on Single sign on.	L6	CO5	PO5,PO6,PO7
16	a)	What are the features of IKE Key algorithm.	L1	CO5	PO5,PO6,PO7
	b)	Explain the voting systems in virtual elections.	L2	CO5	PO5,PO6,PO7

9. PREVIOUS END EXAM QUESTION PAPERS



Q.P Code: CY3101PC Hall Ticket No.: □□□□□□□□□□

NARSIMHA REDDY ENGINEERING COLLEGE

(UGC AUTONOMOUS)

III B.Tech I Semester (NR20) Supplementary Examination, June 2023

INFORMATION SECURITY

(Computer Science and Engineering (Cyber Security))

Time : 3 hours **Maximum marks: 75**

Note:
- This question paper contains two parts, A and B
- Part A is compulsory which carries 25 marks (1st 5 sub questions are one from each unit carry 2 Marks each & Next 5 sub questions are one from each unit carry 3 Marks). Answer all questions in Part A
- Part B Consists of 5 Units. Answer one question from each unit. Each question carries 10 Marks and may have a, b sub questions

Part-A **(25 Marks)**

Answer all questions

Q.No		Question	M	CO	BL
1)	a.	Define security attack.	2	CO1	L1
	b.	What primitive operations are used in RC4?	2	CO2	L2
	c.	Define Hash function.	2	CO3	L2
	d.	What is security association?	2	CO4	L1
	e.	List out the limitations of secure multiparty computation.	2	CO5	L1
	f.	Write the two basic building blocks of encryption techniques.	3	CO1	L2
	g.	List three approaches to message authentication.	3	CO2	L2
	h.	Define the classes of message authentication function.	3	CO3	L1
	i.	Write short notes on transport and tunnel mode.	3	CO4	L1
	j.	How the security associations be combined?	3	CO5	L2

Part-B **(50 Marks)**

Answer all the Units

All Questions carry equal Marks

Q.No		Question	M	CO	BL
		UNIT–I			
2)	a.	What are the advantages of steganography comparing with cryptography?	5	CO1	L3
	b.	Write short notes on security mechanisms.	5	CO1	L2
		OR			
3)	a.	Explain the transposition techniques.	5	CO1	L3
	b.	Discuss about Network security model with neat illustration.	5	CO1	L2
		UNIT–II			
4)	a.	Explain in detail about the steps involved in Blowfish.	5	CO2	L3
	b.	Explain Diffie-Hellman key exchange algorithm in detail.	5	CO2	L2
		OR			
5)	a.	Differentiate Block cipher and Stream Cipher.	5	CO2	L2
	b.	Explain the steps involved in knapsack algorithm with an example.	5	CO2	L3
		UNIT–III			
6)	a.	Explain the different approaches to message authentication.	5	CO3	L3
	b.	Give a neat sketch to explain the concept of Secured Hash Algorithm.	5	CO3	L2
		OR			
7)	a.	Explain in detail about Elgamal Digital signature scheme.	5	CO3	L3
	b.	Give the design objectives for HMAC.	5	CO3	L2
		UNIT–IV			
8)	a.	How does mobile device security work?	5	CO4	L2
	b.	Differentiate between Secure Socket Layer & Transport Layer Security.	5	CO4	L3
		OR			
9)	a.	Explain in detail about Secure Socket Layer.	5	CO4	L3
	b.	Write a short note on HTTPS.	5	CO4	L2
		UNIT–V			
10)	a.	Explain the IP security architecture.	5	CO5	L3
	b.	What are the applications of IP security?	5	CO5	L2
		OR			
11)	a.	Explain the voting systems in virtual elections.	5	CO5	L3
	b.	What do you mean by security association? Specify the parameters that identify the security association.	5	CO5	L2

--ooOoo--

Page 1 of 2

Page 2 of 2

---ooOoo—

10.ASSIGNMENTS

ASSIGNMENT :1

1	a)	Explain in detail about OSI security architecture.
	b)	Explain classical encryption techniques (Steps involved in each encryption technique like Caesar cipher, playfair cipher, hill cipher, vigenere cipher, one time pad cipher, rail fence, etc)
2	a)	Discuss various steps of IDEA algorithm.
	b)	Explain Diffie-Hellman key exchange algorithm in detail.
3	a)	With the example, explain in detail about Secure Hash Algorithm

ASSIGNMENT :2

1	a)	Explain in detail about HMAC and Digital Signature Standard
2	a)	Briefly explain about transport layer security and Padding.
	b)	With a neat diagram, explain the operation of SSL and SSH Record Protocol.
3	a)	Name the protocols that provide security in IPSec.
	b)	Write short notes on PGP.