COURSE FILE

ON

NETWORK SECURITY AND CRYPTOGRAPHY

Course Code –EC723PE

IV B.Tech I-SEMESTER

A.Y.: 2022-2023

Prepared by

Dr. T. Ramakrishna

Associate Professor

Head of the Department
Electronics and Communication Engg. Dept
SRI INDU INSTITUTE OF ENGG & TECH
Sheriguda(V), Ibrahimpatnam(M), R.R.Dist-501 510

PRINCIPAL
Sri Indu Institute of Engineering & Tech.
Sheriguda(Vill), Ibrahimpatnam
R.R. Dist. Telangana-501 510.

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

Academic Year	2022-2023
Course Title	Network Security and Cryptography
Course Code	EC723PE
Programme	B.Tech
Year & Semester	IV year I-semester
Branch & Section	ECE-C
Regulation	R18
Course Faculty	Dr.T.Ramakrishna,Associate Professor

Index of Course File

S. No.	Name of the content
1	Institute vision and mission
2	Department vision and mission
3	Program Educational Objectives/ Program Specific Outcomes
4	Program Outcomes
5	Course Syllabus with Structure
6	Course Outcomes (CO)
7	Mapping CO with PO/PSO and Justification
8	Academic Calendar
9	Time table - highlighting your course periods including tutorial
10	Lesson plan with number of hours/periods, TA/TM, Text/Reference book
11	Web references
12	Lecture notes
13	List of Power point presentations
14	University Question papers
15	Internal Question papers, Key with CO and BT
16	Assignment Question papers mapped with CO and BT
17	Tutorial topics
18	Result Analysis to identify weak and advanced learners - 3 times in a semester
19	Result Analysis at the end of the course
20	Remedial class for weak students - schedule and evidences
21	CO, PO/PSO attainment sheets
22	Attendance register
23	Course file (Digital form)

INSTITUTE VISION AND MISSION

Vision:

To become a premier institute of academic excellence by providing the world class education that transforms individuals into high intellectuals, by evolving them as empathetic and responsible citizens through continuous improvement.

Mission:

IM1: To offer outcome-based education and enhancement of technical and practical skills.

IM2: To Continuous assess of teaching-learning process through institute-industry collaboration.

IM3: To be a centre of excellence for innovative and emerging fields in technology development with state-of-art facilities to faculty and students' fraternity.

IM4: To Create an enterprising environment to ensure culture, ethics and social responsibilityamong the stakeholders.

Head of the Department
Electronics and Communication Engg. Dept
SRI INDU INSTITUTE OF ENGG & TECH
Sheriguda(V), Ibrahimpatnam(M), R.R.Dist-501 510

PRINCIPAL
Sri Indu Institute of Engineering & Tech.
Sheriguda(Vill), Ibrahimpatnam
R.R. Dist. Telangana-501 510.

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

DEPARTMENT VISION AND MISSION

Vision:

To become a recognized center in the field of Electronics and Communication Engineering by producing creative engineers with social responsibility and address ever-changing global challenges.

Mission:

DM1: To facilitate an academic environment that enables student's centric learning.

DM2: To provide state-of-the-art hardware and software technologies to meet industry requirements.

DM3: To continuously update the Academic and Research infrastructure.

DM4: To Conduct Technical Development Programs for overall professional caliber of Stake Holders.

Head of the Department
Electronics and Communication Engg. Dept
SRI INDU INSTITUTE OF ENGG & TECH
Sheriguda(V), Ibrahimpatnam(M), R.R.Dist-501 510

PRINCIPAL
Sri Indu Institute of Engineering & Tech.
Sheriguda(Vill), Ibrahimpatnam
R.R. Dist. Telangana-501 510.

PROGRAM EDUCATIONAL OBJECTIVES

Program Educational objectives are to Promote:

PEO1: Graduates with a strong foundation in Electronics and Communication Engineering, Science and Technology to become successful in the chosen professional career.

PEO2: Graduates with ability to execute innovative ideas for Research and Development with continuous learning.

PEO3: Graduates inculcated with industry based soft-skills to enable employability.

PEO4: Graduates demonstrate with ability to work in interdisciplinary teams and ethical professional behavior.

PROGRAM SPECIFIC OUTCOMES

PSO 1: Design Skills: Design, analysis and development a economical system in the area of Embedded system & VLSI design.

PSO 2: Software Usage: Ability to investigate and solve the engineering problems using MATLAB, Keil and Xilinx.

Head of the Department
Electronics and Communication Engg. Dept
SRI INDU INSTITUTE OF ENGG & TECH
Sheriguda(V), Ibrahimpatnam(M), R.R.Dist-501 510

PRINCIPAL
Sri Indu Institute of Engineering & Tech.
Sheriguda(Vill), Ibrahimpatnam
R.R. Dist. Telangana-501 510.

PROGRAM OUTCOMES

1. **ENGINEERING KNOWLEDGE**: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
2. **PROBLEM ANALYSIS**: Identify, formulate, research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
3. **DESIGN/DEVELOPMENT OF SOLUTIONS**: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.
4. **CONDUCT INVESTIGATIONS OF COMPLEX PROBLEMS**: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.
5. **MODERN TOOL USAGE**: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modelling to complex engineering activities with an understanding of the limitations.
6. **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. **ENVIRONMENT AND SUSTAINABILITY**: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.
8. **ETHICS**: Apply ethical principles and commit to professional ethics and responsibilities and normsof the engineering practice.
9. **INDIVIDUAL AND TEAM WORK**: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
10. **COMMUNICATION**: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, give and receive clear instructions.
11. **PROJECT MANAGEMENT AND FINANCE**: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leaderin a team, to manage projects and in multidisciplinary environments.
12. **LIFE-LONG LEARNING**: Recognize the need for, and have the preparation and ability to engagein independent and life-long learning in the broadest context of technological change.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
B.Tech. in ELECTRONICS AND COMMUNICATION ENGINEERING
IV YEAR COURSE STRUCTURE AND SYLLABUS (R18)

Applicable From 2018-19 Admitted Batch

IV YEAR I SEMESTER

S. No.	Course Code	Course Title	L	T	P	Credits
1	EC701PC	Microwave and Optical Communications	3	0	0	3
2		Professional Elective-III	3	0	0	3
3	EC723PE	Professional Elective-IV(Network Security and Cryptography)	3	0	0	3
4		Open Elective-I	3	0	0	3
5	SM702MS	Professional Practice, Law& Ethics	2	0	0	2
6	EC703PC	Microwave and Optical Communications Lab	0	0	2	1
7	EC704PC	Industrial Oriented Mini Project/Summer Internship	0	0	0	2*
8	EC705PC	Seminar	0	0	2	1
9	EC706PC	Project Stage -I	0	0	6	3
		Total Credits	**14**	**0**	**10**	**21**

IV YEAR II SEMESTER

S. No.	**Course Code**	**Course Title**	**L**	**T**	**P**	**Credits**
1		Professional Elective-V	3	0	0	3
2		Professional Elective-VI	3	0	0	3
3		Open Elective-III	3	0	0	3
4	EC801PC	Project Stage -II	0	0	14	7
		Total Credits	**9**	**0**	**14**	**16**

***MC - Environmental Science – Should be Registered by Lateral Entry Students Only.**

Note: Industrial Oriented Mini Project/ Summer Internship is to be carried out during the summer vacation between 6th and 7th semesters. Students should submit report of Industrial Oriented Mini Project/ Summer Internship for evaluation.

Professional Elective – V

EC811PE	Satellite Communications
EC812PE	Radar Systems
EC813PE	Wireless Sensor Networks

Professional Elective – VI

EC821PE	System On Chip Architecture
EC822PE	Test and Testability
EC823PE	Low Power VLSI Design

COs and Mapping with PO/PSO

Course: NETWORK SECURITY AND CRYPTOGRAPHY (C413) Class: IV ECE-C

Course Outcomes

After completing this course, the student will be able to:

C413.1: Understand various attacks on the network and understanding the need for security [Analysis]

C413.2: Apply various classical encryption techniques on messages and analyze various security services and mechanisms. [Analysis, Evaluation]

C413.3: Compare and contrast symmetric and asymmetric Key Cryptography systems. [Analysis, Evaluation]

C413.4: Describe the cryptographic hash functions, message authentication codes and various key management and distribution techniques. [Analysis]

C413.5: Explain different protocols like SSL, PLS, HTTPS, SSH and various wireless network standards.[Analysis]

C413.6: Analyze how PGP and S/MIME is used to protect messages transmitted through E-mail and explains IPSEC. [Analysis, Evaluation]

<u>Mapping of course outcomes with program outcomes:</u>

High -3 Medium -2 Low-1

Course outcomes	PO 1	PO 2	PO 3	PO 4	PO 5	PO6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2
C413.1	2	3	3	-	-	-	-	-	-	-	-	-	-	-
C413.2	-	-	-	-	-	-	-	-	-	-	-	3	2	-
C413.3	3	2	2	-	-	-	-	-	-	-	2	-	-	-
C413.4	3	2	3	-	-	-	-	-	-	-	-	2	1	-
C413.5	3	-	3	-	2	-	-	-	-	-	2	-	-	-
C413.6	2	-	2	2	2	-	-	-	-	2	-	-	-	1
AVG	**2.6**	**2.3**	**2.6**	**2.0**	**2.0**	**-**	**-**	**-**	**-**	**2**	**2**	**2.5**	**1.5**	**1**

Course: NETWORK SECURITY AND CRYPTOGRAPHY (C413) Class: IV ECE-C

PO1.ENGINEERING KNOWLEDGE: Apply the knowledge of mathematics, science,engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.

PO2.PROBLEM ANALYSIS: Identify, formulate, research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

PO3.DESIGN/DEVELOPMENT OF SOLUTIONS: Design solutions for complex engineering problems and design system components or processes that meet t h e specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

PO4.CONDUCT INVESTIGATIONS OF COMPLEX PROBLEMS: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

PO5.MODERN TOOL USAGE: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.

PO10.COMMUNICATION: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, give and receive clear instructions.

PO11.PROJECT MANAGEMENT AND FINANCE: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

PO12.LIFE-LONG LEARNING: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

CO-PO mapping Justification

C413.1: Understand various attacks on the network and understanding the need for security [Analysis]

	Justification
PO1	Understanding various attacks on the network is essential to apply the knowledge of mathematics, science, and engineering fundamentals in solving complex engineering problems. In the realm of cyber security, a solid grasp of network attacks provides the foundation for developing robust and effective security solutions.
PO2	Understanding various attacks on the network is crucial because it helps engineers identify potential security threats and vulnerabilities in a system. Once they comprehend these network attacks, they can then formulate, research, and analyze complex engineering problems related to cyber security.
PO3	Understanding various attacks on the network is a critical foundation for designing effective solutions for complex engineering problems. By comprehending the nature of network attacks, engineers can develop robust and resilient systems that address security concerns and meet specified needs.

C413.2: Apply various classical encryption techniques on messages and analyze various security services and mechanisms.

	Justification
PO12	By mastering encryption techniques, individuals contribute to the overall security competency of the team, enabling effective collaboration in diverse settings as outlined in po9. The ability to apply encryption is not only a technical skill but also a collaborative and leadership skill that enhances the effectiveness of individuals in teams and multidisciplinary environments.
PSO1	Classical encryption techniques, such as symmetric and asymmetric cryptography, can be employed to safeguard data in embedded systems and VLSI circuits. PSO1, which focuses on the design and development of economical systems in these domains, can benefit from a comprehensive understanding of encryption to enhance data protection and confidentiality features.

C413.3: Compare and contrast symmetric and asymmetric Key Cryptography systems.

	Justification
PO1	Comparing and contrasting symmetric and asymmetric Key Cryptography systems directly aligns with applying the knowledge of mathematics, science, engineering fundamentals, and engineering specialization to the solution of complex engineering problems. It involves understanding the principles, strengths, and weaknesses of both symmetric and asymmetric key cryptography systems.
PO2	Comparing and contrasting symmetric and asymmetric key cryptography systems is directly linked to the ability to identify, formulate, research literature, and analyze complex engineering problems, reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
PO3	The justification lies in the fact that when engineers compare and contrast cryptographic systems, they are better equipped to design solutions that address not only the technical aspects of security but also consider broader factors. By understanding the nuances of symmetric and asymmetric key cryptography, engineers can design system components that

	meet specified needs while taking into account public health and safety, as well as cultural, societal, and environmental considerations.
PO11	Symmetric key cryptography uses a single key for both encryption and decryption. It's efficient but requires secure key distribution. On the other hand, asymmetric key cryptography uses a pair of public and private keys, providing a more secure solution for key exchange but at the cost of computational complexity.

C413.4: Describe the cryptographic hash functions, message authentication codes and various key management and distribution techniques.

	Justification
PO1	Cryptographic hash functions are algorithms that take input data and produce a fixed-size string of characters, which is typically a hash or digest. These functions are crucial for data integrity and digital signatures. By applying the knowledge of mathematics, you can understand the principles behind these functions, ensuring the reliability and security of data.
PO2	To describe cryptographic hash functions, engineers need to delve into the mathematical principles that underlie these algorithms. This involves understanding how the algorithms operate and their applications in information security. This process aligns with this where engineers use first principles of mathematics and engineering sciences to understand and describe complex problems.
PO3	Designing solutions for key management requires a holistic approach. Engineers must consider public health and safety implications, ensuring that secure key distribution methods are in place to prevent unauthorized access that could compromise sensitive information. Environmental considerations may also come into play when designing systems that optimize resource usage in key management processes.
PO12	Recognizing the need for ongoing learning, engineers describing cryptographic hash functions should not only understand the current algorithms but also be prepared to adapt to new advancements and potential vulnerabilities. The ability to engage in independent and lifelong learning ensures that engineers stay updated on emerging hash functions and best practices in the ever-evolving field of cryptography.
PSO1	Describing cryptographic hash functions, message authentication codes, and various key management and distribution techniques is highly relevant to the design, analysis, and development of an economical system in the area of Embedded System & VLSI design.

C413.5: Explain different protocols like SSL, PLS, HTTPS, SSH and various wireless network standards.

	Justification
PO1	Understanding SSL/TLS involves applying mathematical and cryptographic principles. Engineers need to comprehend the algorithms, key exchange mechanisms, and cryptographic protocols underpinning SSL/TLS. This application of mathematical and engineering fundamentals aligns with, where engineers leverage their foundational knowledge to solve complex engineering problems, in this case, ensuring secure communication.
PO3	Identifying and formulating the problem involves recognizing the need for secure communication and understanding the vulnerabilities in traditional protocols. Researching literature on SSL/TLS involves delving into cryptographic principles and analyzing the engineering challenges involved in implementing secure communication. Engineers reach substantiated conclusions by applying first principles of mathematics and engineering sciences to address the complexities of secure data transmission.

PO5	Creating secure communication channels for remote access requires selecting and applying appropriate encryption and authentication techniques, which aligns with creating and applying appropriate techniques in Engineers use modern engineering and IT tools for the implementation of SSH, considering potential security vulnerabilities and modeling to

	understand the limitations of the chosen techniques
PO11	As engineers explain different protocols and wireless network standards by demonstrating knowledge and understanding of engineering principles and applying management principles in the deployment and optimization of secure communication protocols and wireless network standards. This alignment emphasizes the integration of technical expertise and management acumen in engineering projects and multidisciplinary environments.

C413.6: Design state model of a system and determine the transfer function for Linear Time Variant Systems. [Synthesis]

	Justification
PO1	Applying the knowledge of mathematics and science is crucial to understanding the cryptographic algorithms and protocols used in PGP and S/MIME. Engineers need to grasp the mathematical principles behind public-key cryptography, digital signatures, and encryption algorithms to effectively implement and analyze the security mechanisms in these email encryption protocols.
PO3	Designing solutions for email security involves recognizing the complexities of secure communication. Engineers need to consider the specified needs, including the requirements for confidentiality and integrity in email transmission. Additionally, the design process should consider public health and safety by safeguarding sensitive information exchanged via email.
PO4	Analyzing how PGP (Pretty Good Privacy) and S/MIME (Secure/Multipurpose Internet Mail Extensions) are used to protect messages transmitted through email, as well as explaining IPSEC (Internet Protocol Security), involves using research-based knowledge and research methods to provide valid conclusions, aligning with PO4.
PO5	Creating, selecting, and applying appropriate techniques involve choosing the right cryptographic methods for ensuring confidentiality and integrity in email transmission. Engineers apply modern engineering and IT tools to implement and analyze the security mechanisms in PGP and S/MIME.
PO10	Communicating effectively on the complex engineering activities involved in implementing PGP and S/MIME is crucial. Engineers need to comprehend and articulate the intricacies of these cryptographic protocols. Writing effective reports and design documentation is essential for conveying the details of the implementation, potential vulnerabilities, and the overall effectiveness of PGP and S/MIME.
PSO2	By delving into the mechanisms of PGP and S/MIME, engineers gain insights into the cryptographic foundations that are essential for secure communication. This knowledge is highly applicable when investigating and solving engineering problems using tools like MATLAB, Keil, and Xilinx.

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

ACADEMIC CALENDAR 2022-23

B. Tech./B. Pharm. IV YEAR I & II SEMESTERS

I SEM

S. No	Description	Duration	
		From	To
1	Commencement of I Semester classwork	**29.08.2022**	
2	1st Spell of Instructions (including Dussehra Recess)	29.08.2022	31.10.2022 (9 Weeks)
3	Dussehra Recess	03.10.2022	08.10.2022 (1 Week)
4	First Mid Term Examinations	01.11.2022	07.11.2022 (1 Week)
5	Submission of First Mid Term Exam Marks to the University on or before	12.11.2022	
6	2nd Spell of Instructions	09.11.2022	03.01.2023 (8 Weeks)
7	Second Mid Term Examinations	04.01.2023	10.01.2023 (1 Week)
8	Preparation Holidays and Practical Examinations	11.01.2023	19.01.2023 (1 Week)
9	Submission of Second Mid Term Exam Marks to the University on or before	17.01.2023	
10	End Semester Examinations	*20.01.2023*	02.02.2023(2 Weeks)

Note: No. of Working/instructional days: 94

II SEM

S. No	Description	Duration	
		From	To
1	Commencement of II Semester classwork	**03.02.2023**	
2	1st Spell of Instructions	03.02.2023	31.03.2023 (8 Weeks)
3	First Mid Term Examinations	01.04.2023	08.04.2023 (1 Week)
4	Submission of First Mid Term Exam Marks to the University on or before	15.04.2023	
5	2nd Spell of Instructions	10.04.2023	17.06.2023 (10 Weeks)
6	**Summer Vacation**	15.05.2023	27.05.2023 (2 Weeks)
7	Second Mid Term Examinations	19.06.2023	24.06.2023 (1 Week)
8	Preparation Holidays and Practical Examinations	26.06.2023	01.07.2023 (1 Week)
9	Submission of Second Mid Term Exam Marks to the University on or before	01.07.2023	
10	End Semester Examinations	03.07.2023	15.07.2023 (2 Weeks)

Note: No. of Working/ instructional days: 91

9/22

REGISTRAR

SRI INDU INSTITUTE OF ENGINEERING AND TECHNOLOGY

Accredited by NAAC with A+ Grade, Recognized under 2(f) of UGC Act 1956
(Approvedby AICTE, New Delhi and Affiliated to JNTUH, Hyderabad)
Khalsa Ibrahimpatnam, Sheriguda (V), Ibrahimpatnam (M), Ranga Reddy Dist.,
Telangana – 501 510Website: https://siiet.ac.in/

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

Class Timetable

CLASS: IV-B.Tech ECE-C | A.Y:2022-23 | SEMESTER: I | LH: B-202

TIME/ DAY	I 9:40-10:30	II 10:30 -11:20	III 11:20-12:10	IV 12:10-1:00	1:00-1:30	V 1:30-2:20	VI 2:20-3:10	VII 3:10-4:00
MON	DIP	NS&C	MW&OC	JAVA		PPL&E	PPL&E	JAVA
TUE	MW&OC	LIB	NS&C	DIP		INT	CO-CU/DAA	
WED	NS&C	MW&OC	DIP	COUN	LUNCH	JAVA	MW&OC LAB / SEMINAR	
THU	PPL&E	PROJECT STAGE-I				DIP	MW&OC	SPORTS
FRI	JAVA	PROJECT STAGE-I				DIP	NS&C	PPL&E
SAT	NS&C	IOMP				MW&OC	SEMINAR / MW&OC LAB	

*(T) – Tutorial Concern Faculty

Course Code	Course Name	Name of the Faculty	Course Code	Course Name	Name of the Faculty
EC701PC	MW&OC-Microwave and Optical Communications	S.Naresh	EC703PC	MW&OC LAB-Microwave and Optical Communications Lab	Dr.S.Anjaneyulu /S.Naresh
EC713PE	DIP-Digital Image Processing(Prof.Elec.–III)	Dr.S.Anjaneyulu	EC704PC	IOMP-Industry Oriented Mini Project	A.Apsara/G.Anitha/P.Meena
			EC705PC	Seminar	Dr.T.Ramakrishna/G.Swathi/G.Anusha
			EC706PC	Project Stage-I	K.Srikanth/B.Ashwini/T.Divya
EC723PE	NS&C-Network Security and Cryptography (PE – IV)	Dr.T.Ramakrishna	LIB	Library	K.Rajender/D.Aruna Kumari
			SPORTS	Sports	Y.Rajani
CS703OE	JAVA- Java Programming (Open Elective – II)	Ch.Prabhakar	COUN	Counseling	A.Vaani/Dr.S.Anjaneyulu/K.Bhaskar Reddy
			INT	Internet	A.Vaani/P.Krishna Rao
SM702MS	PPL&E- Professional Practice, Law & Ethics	K.Balakrishna	CO-CU/ DAA	Co-Curricular/Department Association Activities	Y.Raju/P.Krishna Rao

Class Incharge | Head of the Department | PRINCIPAL

Sri Indu Institute of Engineering & Tech
Sheriguda (V), Ibrahimpatnam

LESSON PLAN

Programme:B.Tech	Academic Year: 2022-2023
Year: IV	Semester: I
Course Title: Network Security and Cryptography	Course Code: EC723PE
Name of Faculty:Dr.T.Ramakrishna	Number of lectures per week:5

UNIT - I:

Security Services, Mechanisms and Attacks, A Model for Internetwork security, Classical Techniques: Conventional Encryption model, Steganography,Classical Encryption Techniques. Modern Techniques: Simplified DES, Block Cipher Principles, Data Encryption standard, Strength of DES, Block Cipher Design Principles.

No. of Sessions Planned	Topics	Reference	Teaching Method/ Aids
2	Review of fundamentals of networks and security	T1,R1	BB
1	Mechanisms and Attacks	T1,R2	BB
2	A Model for Internetwork security	T1	BB
2	Classical Techniques: Conventional Encryption model	T1	BB
1	Steganography	T1	BB
2	Classical Encryption Techniques	T1	BB
1	Introduction to modern techniques, simplified DES	T1,W1	BB
1	Block Cipher Principles	T1	BB
2	Data Encryption Standard	T1	BB
1	Strength of DES	T1,R1	BB
1	Block Cipher Design Principles	T1,R2	BB

Gap beyond syllabus(if any):
Gap within the syllabus(if any)
Course Outcome 1: Student have understood the fundamentals of networks and security,the various encryption techniques,steganography etc.

*Session Duration: 50minutes
*Total Number of Hours/Unit:16

Course Title: Network Security and Cryptography	Course Code: EC723PE

UNIT-II:
Encryption: Triple DES, International Data Encryption algorithm, Blowfish, RC5, Characteristics of Advanced Symmetricblock Ciphers. Placement of Encryption function, Traffic confidentiality, Key distribution, Random Number Generation.

No. of Sessions Planned	Topics	Reference	Teaching Method/ Aids
1	Introduction to Triple DES	R1	BB
2	International Data Encryption algorithm	R1,R2,W2	BB
2	Blowfish,RC5	R1,W3	BB
2	Characteristics of Advanced Symmetric block Ciphers	R1	BB
1	Placement of Encryption function	R1,R2	BB
2	Traffic confidentiality	R2	BB
1	Key Distribution	R1,R2	BB
1	Random Number Generation	R2	BB

Gap beyond syllabus(if any):
Gap within the syllabus(if any)
Course Outcome 1: Student able to design the different combinational logic circuits. Modify and transform one form of Boolean equation to another form and we can simplify the Boolean equation in K-Map.

*Session Duration: 50minutes
*Total Number of Hours/Unit: 12

Course Title: Network Security and Cryptography	Course Code: EC723PE

UNIT – III

Public Key Cryptography: Principles, RSA Algorithm, Key Management, Diffie-Hellman Key exchange, Elliptic Curve Cryptograpy. Number Theory: Prime and Relatively prime numbers, Modular arithmetic, Fermat's and Euler's theorems, Fermat's and Euler's theorems, Euclid's Algorithm, the Chinese remainder theorem, Discrete logarithms

No. of Sessions Planned	Topics	Reference	Teaching Method/ Aids
1	Introduction to public key cryptography	T1	BB
1	Introduction to RSA Algorithm and in detail.	T1	BB
2	Key Management	T1	BB
1	Diffie-Hellman Key exchange	T1	BB
1	Elliptic Curve Cryptograpy	T2	BB
2	Number Theory: Prime and Relatively prime numbers	T1	BB
1	Modular arithmetic	T1	BB
2	Fermat's and Euler's theorems	T1	BB
2	Euclid's Algorithm	T1,R1	BB
2	The Chinese remainder theorem, Discrete logarithms	T1,R2	BB

Gap beyond syllabus(if any):
Gap within the syllabus(if any)
Course Outcome 1: Student able to design the different Sequential circuits. Analyze and compare the flipflops and transform one flipflop to another flipflop.

*Session Duration: 50minutes
*Total Number of Hours/Unit: 15

Course Title: Network Security and Cryptography	Course Code: EC723PE

UNIT – IV

Message Authentication and Hash Functions: Authentication requirements and functions, Message Authentication, Hash functions, Security of Hash functions and MACs. Hash and Mac Algorithms: MD-5, Message digest Algorithm, Secure Hash Algorithm. Digital signatures and Authentication protocols: Digital signatures, Authentication Protocols, Digital signature standards. Authentication Applications: Kerberos, Electronic Mail Security: Pretty Good Privacy, SIME/MIME.

No. of Sessions Planned	Topics	Reference	Teaching Method/ Aids
1	Introduction to Message Authentication and Hash Functions	T1	BB
2	Authentication requirements and functions	T1	BB
1	Message Authentication	T1	BB
1	Hash functions	T1	BB
2	Security of Hash functions and MACs	T1	BB
2	Hash and Mac Algorithms-MD5	T1	BB
1	Message digest Algorithm	T1	BB
1	Secure Hash Algorithm	T1	BB
2	Introduction to Digital signatures and Authentication protocols: Digital signatures	T1	BB
1	Authentication Protocols	T1	BB
1	Digital signature standards	T1	BB
1	Authentication Applications: Kerberos	T1	BB
1	Electronic Mail Security :Pretty Good Privacy	T1	BB
1	SIME/MIME	T1	BB

Gap beyond syllabus(if any):
Gap within the syllabus(if any)
Course Outcome 1: Student able to design synchronous and asynchronous counters. Analyze and differentiate the sequential machines.

*Session Duration: 50minutes
*Total Number of Hours/Unit:18

Course Title: Network Security and Cryptography	Course Code: EC723PE

UNIT - V
IP Security: Overview, Architecture, Authentication, Encapsulating Security Payload, Key Management. Web Security: Web Security requirements, Secure sockets layer and Transport layer security, Secure Electronic Transaction. Intruders, Viruses and Worms: Intruders, Viruses and Related threats. Fire Walls: Fire wall Design Principles, Trusted systems

No. of Sessions Planned	Topics	Reference	Teaching Method/ Aids
2	Introduction to IP Security, overview	T1,	PPT
2	Architecture of IP security	R1	PPT
1	Authentication, Encapsulating Security Payload	R1	PPT
1	Key Management	R1	PPT
1	Introduction to Web Security	R1	PPT
2	Web Security requirements	R1	PPT
2	Secure sockets layer and Transport layer security	R1	PPT
1	Secure Electronic Transaction	R1,T1	PPT
1	Intruders	R1,T1	PPT
1	Viruses and Worms: Intruders	R1	PPT
1	Viruses and Related threats	R1	PPT
1	Fire Walls: Fire wall Design Principles	T1	PPT
1	Trusted systems	R2,T2	PPT

Gap beyond syllabus(if any):
Gap within the syllabus(if any)
Course Outcome 1: Student able to get the knowledge on logic families and realization of basic gates using diodes and transistors

*Session Duration: 50minutes
*Total Number of Hours/Unit:14

TEXT BOOKS:
T1. Cryptography and Network Security: Principles and Practice - William Stallings, Pearson Education.
T2. Network Security: The complete reference, Robert Bragg, Mark Rhodes, TMH,2004.

REFERENCE BOOKS:
R1.Network Security Essentials(Applications and Standards) by William Stallings Pearson Education.
R2.Fundamentals of Network Security by Eric Maiwald(Dreamtech press)
R3. Principles of Information Security, Whitman,Thomson.
R4. Introduction to Cryptography, Buchmann,Springer.

WEB REFERENCES:

W1. https://www.simplilearn.com/what-is-des-article
W2. https://www.educba.com/idea-algorithm/
W3. https://www.geeksforgeeks.org/blowfish-algorithm-with-examples/

SRI INDU INSTITUTE OF ENGINEERING AND TECHNOLOGY

Accredited by NAAC with A+ Grade, Recognized under 2(f) of UGC Act 1956
(Approvedby AICTE, New Delhi and Affiliated to JNTUH, Hyderabad)
Khalsa Ibrahimpatnam, Sheriguda (V), Ibrahimpatnam (M), Ranga Reddy Dist.,
Telangana – 501 510
Website: https://siiet.ac.in/

Lecture notes

Unit 1 link:

https://drive.google.com/file/d/13j3b0HhH0ja3WEuDgBRmxRWX6Z_crg9j/view?usp=sharing

Unit 2 link:

https://drive.google.com/file/d/18tkPU9yObR8KztFWG4lBJjjLXvilyX0D/view?usp=sharing

Unit 3 link:

https://drive.google.com/file/d/1tJFlzWDWYABQ5fw1egFf5vhKYMvCgsuq/ view?usp=sharing

Unit 4 link:

https://drive.google.com/file/d/1C4X3EA7UvjPssJ843WolOVYVBNP3JlhH/view?usp=sharing

Unit 5 link:

https://drive.google.com/file/d/1PsaZqclHMuT-ULZMUKay2oQjmUkyTq9J/view?usp=sharing

Power point presentation

PPT link:

1. https://drive.google.com/file/d/1r47w8tK3hlGwLst23xZn03R-rkpVetOO/view?usp=sharing

2. https://drive.google.com/file/d/1zC5jMcvBq6J83lDuuY3v19YV4F9 m4JPA/view?usp=sharing

3. https://docs.google.com/presentation/d/1z9YkY8xjMVgmvNa2uNjn QF_eS-ldQTCe/edit?usp=sharing&ouid=109450353678166106917&rtpof= true&sd=true

R18

Code No: 157CR

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
B. Tech IV Year I Semester Examinations, February/March - 2022
NETWORK SECURITY AND CRYPTOGRAPHY
(Electronics and Communication Engineering)

Time: 3 Hours **Max. Marks: 75**

Answer any Five Questions
All Questions Carry Equal Marks
- - -

1.a) Write a detailed note on the Conventional Encryption model with an example.
b) Justify how Steganography improves Data Security with an example. [8+7]

2. Demonstrate the working of a Transposition Technique for encryption with an example. [15]

3. Explain the implementation of Triple DES with Two Keys with a neat diagram. [15]

4.a) Illustrate two methods for Traffic Confidentiality with neat diagrams.
b) Explain briefly about Blowfish Algorithm. [8+7]

5.a) Using Fermat's theorem, find 3^{201} mod 11.
b) Use Euler's Theorem to find a number x between 0 and 28 with x^{85} congruent to 6 modulo35. [8+7]

6.a) Write a detailed note on the Chinese Remainder Theorem.
b) Explain briefly the Discrete Logarithms. [8+7]

7.a) Write a detailed note on Kerberos.
b) Explain in detail about Digital Signature Standards. [8+7]

8. Describe in detail the Encapsulating Security Payload with neat diagrams. [15]

---ooOoo---

Code No: 157CR **R18**

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
B. Tech IV Year I Semester Examinations, July/August - 2022
NETWORK SECURITY AND CRYPTOGRAPHY
(Electronics and Communication Engineering)

Time: 3 Hours **Max.Marks:75**

Answer any five questions
All questions carry equal marks
- - -

1.a) Discuss in detail about various Security Services, mechanisms and security attacks.
b) Write a brief note on Block Cipher Principles. [7+8]

2. What is DES? Write a detailed note on the strength of DES. [15]

3. Explain in detail about Triple DES algorithm with an illustration. [15]

4.a) List out the characteristics of advanced Symmetric block Ciphers.
b) Write a detailed note on Blowfish Algorithm. [6+9]

5.a) Define Public Key Cryptography and write its principles.
b) Explain in detail about RSA Algorithm. [7+8]

6.a) Write a brief note on prime and relatively prime numbers in the study of cryptograp y.
b) Explain in detail about Key-Management schemes. [7+8]

7.a) Explain in detail about Hash Functions.
b) Write a detailed note on Kerberos. [8+7]

8.a) Discuss in detail about Secure Electronic Transaction.
b) Write a short note on Trusted Systems. [8+7]

---oo0oo---

Code No: 157CR **R18**

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
B. Tech IV Year I Semester Examinations, January/February - 2023
NETWORK SECURITY AND CRYPTOGRAPHY
(Electronics and Communication Engineering)

Time: 3 Hours **Max.Marks:75**

Note: i) Question paper consists of Part A, Part B.
ii) Part A is compulsory, which carries 25 marks. In Part A, Answer all questions.
iii) In Part B, Answer any one question from each unit. Each question carries 10 marks and may have a, b as sub questions.

PART – A

(25 Marks)

Write about security mechanisms. [2]
b) List the services of security. [3]
c) How a key is generated in IDEA algorithm? [2]
d) Write short notes on Random Number Generation. [3]
e) State the Chinese Remainder Theorem. [2]
f) Define the principles of public key cryptography. [3]
g) Write down requirements for digital signatures. [2]
h) List the services of PGP. [3]
i) Write short notes on scope of ESP. [2]
j) What is a Firewall? Write the need for firewalls. [3]

PART – B

(50 Marks)

2.a) Define Network Security. Explain requirements of network security with examples.
b) Draw the block diagram of DES encryption. Also explain strength of DES in brief. [5+5]

OR

3.a) List and explain types of security attacks with neat diagrams.
b) Discuss in detail about Transposition Techniques with example. [5+5]

4.a) Enumerate in detail about the steps in RC5 Algorithm with a neat diagram.
b) Discuss in detail about location of encryption devices. [5+5]

OR

5.a) Define Key distribution? Illustrate key distribution techniques in detail.
b) Explain the characteristics of advanced symmetric block ciphers. [5+5]

6.a) Illustrate Digital Signature Standard (DSS) an write down the functions of signing and verifying with suitable diagrams.
b) Explain RSA algorithm and illustrate with an example. [5+5]

OR

7.a) What is discrete logarithm and when can we define it for a set of numbers?
b) Enumerate Diffie-Hellman Key exchange for encryption and decryption with suitable examples. [5+5]

SRI INDU INSTITUTE OF ENGINEERING AND TECHNOLOGY

Accredited by NAAC with A+ Grade, Recognized under 2(f) of UGC Act 1956 (Approved by AICTE, New Delhi and Affiliated to JNTUH, Hyderabad)

Khalsa Ibrahimpatnam, Sheriguda (V), Ibrahimpatnam (M), Ranga Reddy Dist., Telangana – 501 510 Website: https://siiet.ac.in/

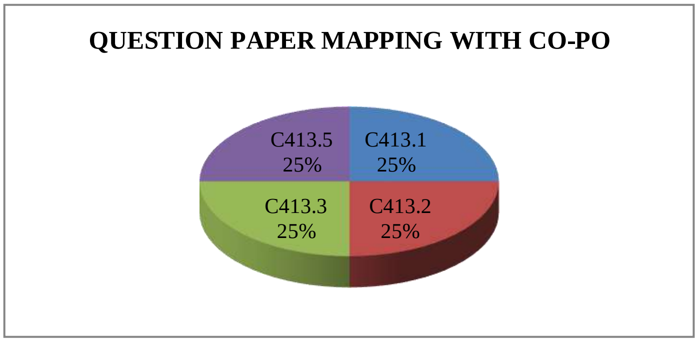
I- Mid Examinations, NOV-2022

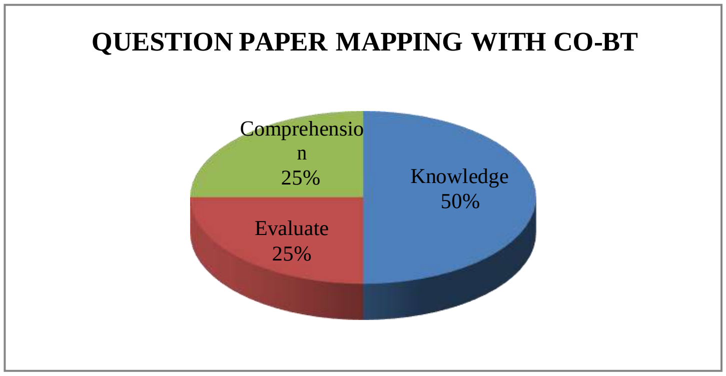
Year &Branch:IVECE Date: 0 3 /11/2022(AN)

Subject:NS&C(A, B&C) Max.Marks: 10 Time:60 mins

Answer any **TWO** Questions. All Question Carry Equal Marks 2*5=10 marks

1. List and briefly define categories of Security Services and attacks.[C413.1]	5	Knowledge
2.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.[C413.2]	5	Evaluate
3.Enumerate Diffie-Hellman Key exchange for encryption and decryption with suitable examples.[C413.3]	5	Knowledge
4.Explain the security constraints of IEEE 802.11i Wireless LAN in detail.[C413.5]	5	Comprehension





SRI INDU INSTITUTE OF ENGINEERING AND TECHNOLOGY

Accredited by NAAC with A+ Grade, Recognized under 2(f) of UGC Act 1956 (Approved by AICTE, New Delhi and Affiliated to JNTUH, Hyderabad)

Khalsa Ibrahimpatnam, Sheriguda (V), Ibrahimpatnam (M), Ranga Reddy Dist.,Telangana – 501 510Website: https://siiet.ac.in/

Set – II

I- Mid Examinations, NOV-2022

Year &Branch:IV ECE   Date: 0 3 /11/2022(AN)

Subject:NS&C(A, B&C)   Max.Marks: 10   Time:60 mins

Answer any **TWO** Questions. All Question Carry Equal Marks   2*5=10 marks]

1. Write any three transposition ciphers with examples.	5	Knowledge
2. Critically analyze the security of RSA	5	Analysis
3. 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.	5	Evaluate
4. What is SSL? Explain about SSL record protocol format.	5	Comprehension

SRI INDU INSTITUTE OF ENGINEERING AND TECHNOLOGY
Accredited by NAAC with A+ Grade, Recognized under 2(f) of UGC Act 1956
(Approved by AICTE, New Delhi and Affiliated to JNTUH, Hyderabad)
Khalsa Ibrahimpatnam, Sheriguda (V), Ibrahimpatnam (M), Ranga Reddy Dist., Telangana – 501 510
Website: https://siiet.ac.in/

B.Tech IV Year I Sem I Mid –Term Examination, NOV-2022
NETWORK SECURITY AND CRYPTOGRAPHY

(Objective Exam)

DATE: 02 /11/2022 (AN) **TIME: 20 Min**

NAME: ____ **ROLL NO:** ____ **MARKS:** ____

I.Choose the Correct Answers

1.Which one of the following is not a RC5 mode of operation? [ ]

a)RC5 block cipher b) RC5-Cipher Block Chaining

c) RC5-Cipher Padding d) RC5-CipherText Stealing

2.Which RC5 mode will have the ciphertext longer than the plaintext by at most the size of a single RC5 block? [ ]

a) RC5 block cipher b) RC5-Cipher Block Chaining

c) RC5-Cipher Block Chaining Pad d) RC5-Cipher Text Stealing

3.Which of these is not a characteristic of block ciphers? [ ]

a) Variable key length / block size / number of rounds

b) Mixed operators, data/key dependent rotation

c) Key independent S-boxes d) More complex key scheduling

4.Which one of the following RC4 algorithm not used in? [ ]

a) SSL b) TLS c) FTP d) WEP

5.What are the allowable values of word size in bit for RC5 algorithm? [ ]

a) 16, 32 b) 16, 32, 64 c) 8, 16, 32 d) 16, 32, 48

6.The total number of subkeys used in the RC5 algorithm is given by the formula (r corresponds to number of rounds)
` [ ]

a) t=2r+4 b) t=2r c) t=2r+2 d) t=2r-2

7.What is the number of possible 3 x 3 affine cipher transformations ? [ ]

a) 168 b) 840 c) 1024 d) 1344

8.Caesar Cipher is an example of [ ]

a) Poly-alphabetic Cipher b) Mono-alphabetic Cipher

c) Multi-alphabetic Cipher d) Bi-alphabetic Cipher

9. In AES the 4×4 bytes matrix key is transformed into a keys of size [ ]

a) 32 words b) 64 words c) 54 words d) 44 words

10.How many modes of operation are there in in DES and AES? [ ]

a) 4 b) 3 c) 2 d) 5

II.Fill in The Blanks:

11.The number of rounds in RC5 can range from 0 to ______________

12.The standard/nominal version of the RC5-w/r/b has parameters w/r/b as______________

13.The value of the base of natural logarithms is ______________

14.AES uses a _____________ bit block size and a key size of ___________ bits.

15.The 4×4 byte matrices in the AES algorithm are called______________

16. XTS-AES mode of operation is a better version of______________

17.______________is the size of the XTS-AES key

18.______________is the maximum size of the key in blowfish algorithm

19.The blowfish algorithm's key expansion converts a key of at most 448 bits into several subkey arrays totaling ____________ bytes.

20.No.of S-boxes are present in the blowfish algorithm______________

NS&C mid 1 descriptive answer key link

https://drive.google.com/file/d/1lwSktRHi5q9lV-KtphvoGbSmeqKmLRI1/view?usp=sharing

SRI INDU INSTITUTE OF ENGINEERING AND TECHNOLOGY

Accredited by NAAC with A+ Grade, Recognized under 2(f) of UGC Act 1956 (
Approvedby AICTE, New Delhi and Affiliated to JNTUH, Hyderabad)
Khalsa Ibrahimpatnam, Sheriguda (V), Ibrahimpatnam (M), Ranga Reddy Dist., Telangana –
501 510Website:https://siiet.ac.in/

B.Tech IV Year ISem I Mid –Term Examination, NOV-2022
NETWORK SECURITY AND CRYPTOGRAPHY
(Objective Exam Key)

Key:

1. C
2. C
3. C
4. C
5. B
6. C
7. D
8. B
9. D
10. D

II. Fill in The Blanks:

11. 255
12. 32/12/16
13. e=2.7183
14. 128.128,192or256
15. States
16. ECB
17. 512
18. 56BYTES
19. 4168
20. 4

SRI INDU INSTITUTE OF ENGINEERING AND TECHNOLOGY

Accredited by NAAC with A+ Grade, Recognized under 2(f) of UGC Act 1956 (
Approvedby AICTE, New Delhi and Affiliated to JNTUH, Hyderabad)
Khalsa Ibrahimpatnam, Sheriguda (V), Ibrahimpatnam (M), Ranga Reddy Dist.,
Telangana –501510
Website:https://siiet.ac.in/

Set – I

II- Mid Examinations, JAN-2023

Year &Branch: IVECE (A,B&C) Date:12-01-2023

Subject: NS&C Marks: 10 Time: 60 min

Answer any **TWO** Questions. All Question Carry Equal Marks 2*5=10 marks

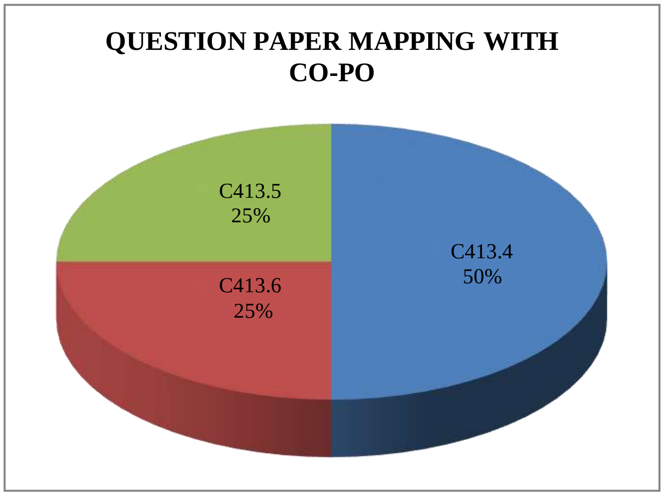
(This question paper is prepared with Course Outcome and BT's mapping)

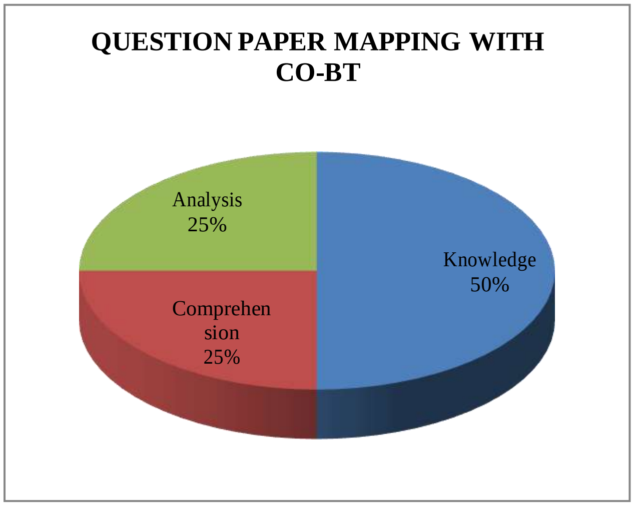
1.Explain Message Authentication Requirements and what are the attacks related to message communication? (**KNOWLEDGE)[C413.4]**

2.Discuss the IEEE 802.11i Wireless LAN Security? **(ANALYSIS)[C413.5]**

3.Explain IP security architecture and also explain basic combinations of securityassociations with a neat diagram? (**COMPREHENSION)[C413.6]**

4. List the main features of SHA-512 cryptographic hash function. What kind of compression function is used in SHA-512? (**KNOWLEDGE)[C413.4]**





SRI INDU INSTITUTE OF ENGINEERING AND TECHNOLOGY
Accredited by NAAC with A+ Grade, Recognized under 2(f) of UGC Act 1956
(Approvedby AICTE, New Delhi and Affiliated to JNTUH, Hyderabad)
Khalsa Ibrahimpatnam, Sheriguda (V), Ibrahimpatnam (M), Ranga Reddy Dist., Telangana –501510
Website: https://siiet.ac.in/

Set – II

II- Mid Examinations, JAN-2023

Year &Branch: IVECE (A,B&C) Date:12-01-2023

Subject: NS&C Marks: 10 Time: 60 min

Answer any **TWO** Questions. All Question Carry Equal Marks 2*5=10 marks

(This question paper is prepared with Course Outcome and BT's mapping)

1.Explain Message Authentication Requirements and what are the attacks related tomessage communication? (**COMPREHENSION)**

2. Discuss the IEEE 802.11i Wireless LAN Security? **(ANALYSIS)**

3.Explain IP security architecture and also explain basic combinations of securityassociations with a neat diagram? (**COMPREHENSION**)

4.List the main features of SHA-512 cryptographic hash function. What kind of compression function is used in SHA-512? (**KNOWLEDGE)**

SRI INDU INSTITUTE OF ENGINEERING AND TECHNOLOGY

Accredited by NAAC with A+ Grade, Recognized under 2(f) of UGC Act 1956 (Approvedby AICTE, New Delhi and Affiliated to JNTUH, Hyderabad)
Khalsa Ibrahimpatnam, Sheriguda (V), Ibrahimpatnam (M), Ranga Reddy Dist., Telangana – 501 510Website:ttps://siiet.ac.in/

B-Tech II - Mid Examinations, JAN-2023

Objective Type Exam

Year &Branch: IV –ECE-A, B&C **Date:12 -01-2023**
Subject: NS &C Max. Marks: 10 Time: 20 mins
Name: ……………………………………………………………Roll No……………………………………

I. Choose the correct alternative:

1. When a hash function is used to provide message authentication, the hash function value is referred to as [ ]
a) Message Field
b) Message Digest
c) Message Score
d) Message Leap

2. Message authentication code is also known as [ ]
a) key code
b) hash code
c) keyed hash function
d) message key hash function

3. Another name for Message authentication codes is [ ]
a) cryptographic code break
b) cryptographic code sum
c) cryptographic check sum
d) cryptographic check break

4. MACs are also called [ ]
a) test word
b) check word
c) test bits
d) none of the mentioned

5. MAC is a [ ]
a) one-to-one mapping
b) many-to-one mapping
c) onto mapping
d) none of the mentioned

6. Wi-Fi stands for [ ]
a) Wireless Fidelity
b) Wireless LAN
c) Wireless FLAN
d) None of the mentioned

7. SSID stands for [ ]
a) Secure Service Identifier
b) Secure Set Independent Device
c) Secure Set Identifier
d) Service Set Independent Device

8. VPN stands for [ ]
a) Visual Performance Node
b) Virtual Private Network
c) Virtual Post Node
d) Virtual Post Network

9. Network layer firewall works as a ___________ [ ]
a) Frame filter
b) Packet filter
c) Content filter
d) Virus filter

10. Which one of the following is not an application hash functions? [ ]
a) One-way password file
b) Key wrapping
c) Virus Detection
d) Intrusion detection

II. Fill in the blanks:

1. A proxy firewall filters at __________
2. ________is a type of software designed to help the user's computer detect viruses and avoid them.
3. It can be a software program or a hardware device that filters all data packets coming through the internet, a network, etc. it is known as the________
4. Code Red is a type of _________
5. Hash functions are extremely useful and appear in almost all--------------------------- applications.
6. There are__________types of computer virus.
7 ---------------------is a most common application of the hash functions.
8. A computer_________is a malicious code which self-replicates by copying itself to other programs.
9. The virus hides itself from getting detected by _______different ways.
10. ________________infects the master boot record and it is challenging and a complex task to remove this virus.

NS&C mid 2 descriptive answer key link

https://drive.google.com/file/d/1DccKXdcez_4BV_9oAiOKmb2RCxTzj4kw/view?usp=sharing

B-Tech II - Mid Examinations, JAN-2023

<u>Objective Type Exam</u>

Year &Branch: IV –ECE-A, B&C **Date:12 -01-2023**

Subject: NS&C Max. Marks: 10 Time:20 mins

Name: ………………………………………………… Roll No……………………………………

ANSWER KEY

I. Choose the correct alternative:

1. B
2. C
3. C
4. D
5. B
6. A
7. C
8. B
9. B
10. B

II. Fill in the blanks:

1. Application layer
2. Antivirus
3. Firewall
4. A computer virus
5. Information security
6. 10
7. Data Integrity check
8. Virus
9. 3
10. Boot Sector Virus

SRI INDU INSTITUTE OF ENGINEERING AND TECHNOLOGY
Accredited by NAAC with A+ Grade, Recognized under 2(f) of UGC Act 1956
(Approvedby AICTE, New Delhi and Affiliated to JNTUH, Hyderabad)
Khalsa Ibrahimpatnam, Sheriguda (V), Ibrahimpatnam (M), Ranga Reddy Dist.,
Telangana – 501 510Website:https://siiet.ac.in/

SUBJECT: NETWORK SECURITY AND CRYPTOGRAPHY

ASSIGNMENT-1

1. Give IP security architecture with neat diagram. (C413.1) (Knowledge)
2. Explain IEEE 802.11 and wireless LAN security. (C413.1) (Knowledge)
3. Explain HMAC algorithm. (C413.1) (Knowledge)
4. What is SSL? Explain about SSL record protocol form. (C413.1) (Knowledge)
5. Write about internet key exchange protocol and list the features and deffie-helman algorithm. (C413.1)(Knowledge)

ASSIGNMENT-1 ANSWER KEY LINK

https://drive.google.com/file/d/1EbDuYnE3eahmmVL8YTcTLWky8D1MUEJ1/view?usp=sharing

SUBJECT:NETWORK SECURITY AND CRYPTOGRAPHY

ASSIGNMENT-2

1. List and explain define the categories of security services and attacks. . (C413.1)(Knowledge)
2. Enumerate Diffie-hellman key exchange for encryption and describe with suitable examples. (C413.1)(Knowledge)
3. Write any three transposition ciphers with examples. . (C413.1)(Knowledge)
4. Critically analyze the security of RSA. . (C413.1) (Knowledge)
5. What is SSL? Explain about SSL record protocol form. . (C413.1)(Knowledge)

ASSIGNMENT –2 ANSWER KEY LINK

https://drive.google.com/file/d/1K8-I4xPEogh5og-Q_-I2aobm8FHmORe0/view?usp=sharing

Result Analysis:

Course Title	NETWORK SECURITY AND CRYPTOGRAPHY
Course Code	EC723PE
Programme	B.Tech
Year & Semester	IV year I-semester, C sec
Regulation	R18
Course Faculty	Dr. T.Rama krishna, Associate Professor, ECE

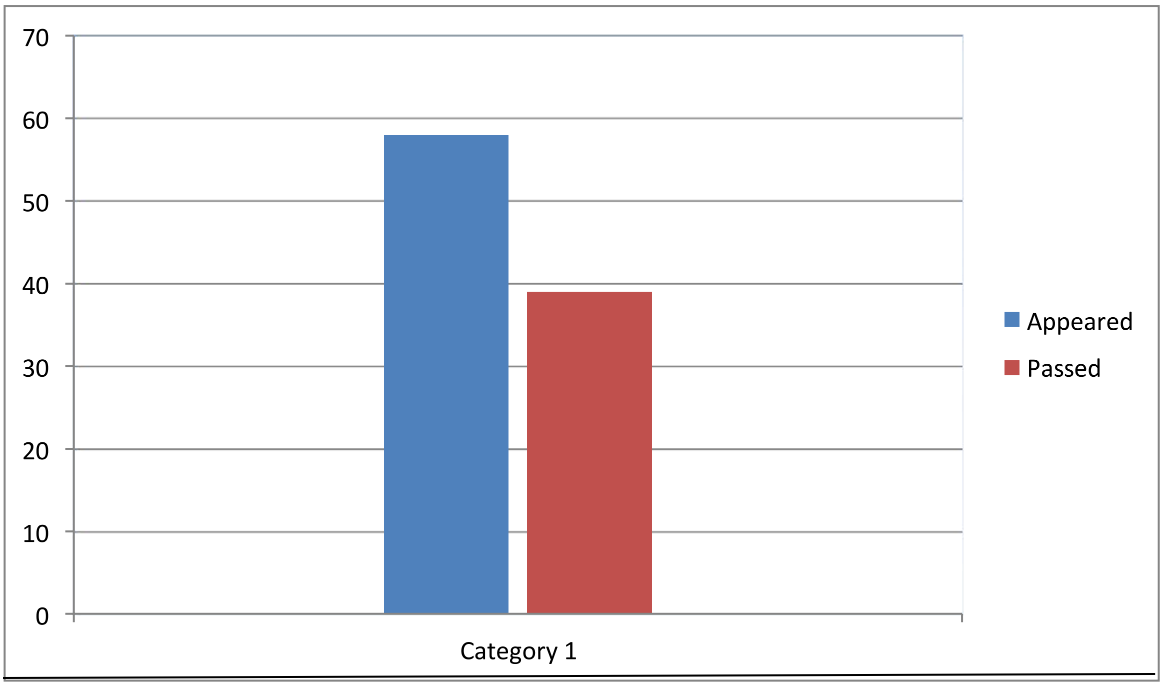
Slow learners:

S No.	Roll no	No of backlogs	Internal-I Status	Internal-II Status
1	18X31A0403	4	14	19
2	18X31A0413	5	15	14
3	18X31A0454	8	14	14
4	18X31A04D4	8	14	15
5	18X31A04F1	5	15	16
6	18X31A04H2	3	21	16
7	18X31A04H7	3	15	22
8	19X31A04B5	3	19	19
9	19X31A04B7	5	18	20
10	19X31A04C3	5	21	16
11	19X31A04D2	4	14	22
12	19X31A04D3	4	20	23
13	19X31A04D8	3	19	23
14	19X31A04E5	5	19	22
15	20X31A0425	4	23	23
16	20X31A0426	5	20	21

BATCH ECE-IV BTECH I SEM ECE-C RESULT ANALYSIS

ACADAMIC YEAR	COURSE NAME	NUMBER OF STUDENTS		QUESTION PAPER SETTING		PASS %
		APPEARED	PASSED	INTERNAL	EXTERNAL	
2022-23	NETWORK SECURITY AND CRYPTOGRAPHY	58	39	COURSE FACULTY	JNTUH	67.24 %

NETWORK SECURITY AND CRYPTOGRAPHY (C413) RESULT ANALYSIS



SRI INDU INSTITUTE OF ENGINEERING AND TECHNOLOGY

(An Autonomous Institution under UGC)
Accredited by NAAC with A+ Grade, Recognized under 2(f) of UGC Act 1956
(Approved by AICTE, New Delhi and Affiliated to JNTUH, Hyderabad)
Khalsa Ibrahimpatnam, Sheriguda (V), Ibrahimpatnam (M), Ranga Reddy Dist., Telangana – 501 510
Website: https://siiet.ac.in/

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

REMEDIAL CLASSES TIME TABLE

A.Y 2022-23 SEMESTER-I

BRANCH/ SEC	MON 4.00 PM-5.00 PM	TUE 4.00 PM-5.00 PM	WED 4.00 PM-5.00 PM	THUR 4.00 PM-5.00 PM	FRI 4.00 PM-5.00 PM
II ECE-A	EDC	NATL	DSD	PTSP	SS
II ECE-B	NATL	DSD	PTSP	SS	EDC
III ECE-A	MPMC	DCCN	CS	BEFA	EMI
III ECE-B	DCCN	CS	BEFA	EMI	MPMC
III ECE-C	CS	BEFA	EMI	MPMC	DCCN
IV ECE-A	MW&OC	DIP	PPLE	NS&C	JAVA
IV ECE-B	DIP	PPLE	NS&C	JAVA	MW&OC
IV ECE-C	PPLE	NS&C	JAVA	MW&OC	DIP

HOD
Head of the Department
Electronics and Communication Engg. Dept.
SRI INDU INSTITUTE OF ENGG & TECH,
Sheriguda(V), Ibrahimpatnam(M), R.R.Dist-501 510.

PRINCIPAL
PRINCIPAL
Sri Indu Institute of Engineering & Tech.
Sheriguda(Vill), Ibrahimpatnam,
R.R Dist Telangana -501 510.

SRI INDU INSTITUTE OF ENGINEERING AND TECHNOLOGY

Department of Electronics and Communication Engineering

Course Outcome Attainment (Internal Examination-1)

Name of the faculty :	Dr.T.Ramakrishna	Academic Year:	2022-23
Branch & Section:	ECE - C	Examination:	I Internal
Course Name:	NS&C	Year: IV	Semester: I

S.No	HT No.	Q1a	Q1b	Q2a	Q2b	Q3a	Q3b	Q4a	Q4b	Obj1	A1
Max. Marks ==>		5		5		5		5		10	5
1	19X31A04A1	4								5	5
2	19X31A04A2	3								9	5
3	19X31A04A3	3								9	5
4	19X31A04A4	3								10	5
5	19X31A04A5	3								10	5
6	19X31A04A6	4		4						9	5
7	19X31A04A7	4		3						9	5
8	19X31A04A8	4		3						10	5
9	19X31A04A9	4		3						9	5
10	19X31A04B0	5								9	5
11	19X31A04B1	3		3						9	5
12	19X31A04B2			3						8	5
13	19X31A04B3			4						9	5
14	19X31A04B4			4						9	5
15	19X31A04B5			4						10	5
16	19X31A04B6	5		4						9	5
17	19X31A04B7	4								9	5
18	19X31A04B8	4		4						9	5
19	19X31A04B9			5						9	5
20	19X31A04C0			4						8	5
21	19X31A04C1			5						8	5
22	19X31A04C2	5		5						8	5
23	19X31A04C3	3		4						9	5
24	19X31A04C4			5		5				10	5
25	19X31A04C5					4		3		10	5
26	19X31A04C6							1		8	5
27	19X31A04C7							5		9	5
28	19X31A04C8					3		2		9	5
29	19X31A04C9			5		4				9	5
30	19X31A04D0	5		3						9	5
31	19X31A04D1	4		3						6	5
32	19X31A04D2			3		2				4	5
33	19X31A04D3					3		3		9	5
34	19X31A04D4					3		4		9	5
35	19X31A04D5					5				9	5
36	19X31A04D6					4		5		9	5
37	19X31A04D7							5		9	5
38	19X31A04D8							5		9	5
39	19X31A04D9					5				9	5
40	19X31A04E0			5		4				9	5
41	19X31A04E1	5		4						9	5
42	19X31A04E2	4		4						8	5
43	19X31A04E3			4						9	5

44	19X31A04E4					5		5		9	5
45	19X31A04E5					2		3		9	5
46	20X35A0421					3		3		9	5
47	20X35A0422					3		3		9	5
48	20X35A0423					5		4		10	5
49	20X35A0424					5		5		9	5
50	20X35A0425	5		4						9	5
51	20X35A0426	3		3						9	5
52	18X31A0403			3						6	5
53	18X31A0413			4						6	5
54	18X31A0454			1						8	5
55	18X31A04D4			5						4	5
56	18X31A04F1			5						5	5
57	18X31A04H2	4		4						8	5
58	18X31A04H7	4								6	5
Target set by the faculty / HoD		3.00	0.00	3.00	0.00	3.00	0.00	3.00	0.00	6.00	3.00
Number of students performed above the target		24	0	32	0	15	0	13	0	54	58
Number of students attempted		24	0	33	0	17	0	15	0	58	58
Percentage of students scored more than target		100%		97%		88%		87%		93%	100%

CO Mapping with Exam Questions:

CO - 1	Y						Y		Y	Y
CO - 2			Y						Y	Y
CO - 3					Y				Y	Y
CO - 4										
CO - 5										
CO - 6										

% Students Scored >Target %	100%		97%		88%		87%		93%	100%

CO Attainment based on Exam Questions:

CO - 1	100%						87%		93%	100%
CO - 2			97%						93%	100%
CO - 3					88%				93%	100%
CO - 4										
CO - 5										
CO - 6										

CO	**Subj**	obj	Asgn	Overall	Level
CO-1	94%	93%	100%	96%	3.00
CO-2	97%	93%	100%	97%	3.00
CO-3	88%	93%	100%	94%	3.00
CO-4					
CO-5					
CO-6					

Attainment Level	
1	40%
2	50%
3	60%

Attainment (Internal 1 Examination) **3.00**

SRI INDU INSTITUTE OF ENGINEERING AND TECHNOLOGY

Department of Electronics and Communication Engineering

Course Outcome Attainment (Internal Examination-2)

Name of the faculty :	Dr.T.Ramakrishna	Academic Year:	2022-23
Branch & Section:	ECE-C	Examination:	II INTERNAL
Course Name:	NS&C	Year: IV	Semester: I

S.No	HT No.	Q1a	Q1b	Q2a	Q2b	Q3a	Q3b	Q4a	Q4b	Obj4	A4
Max. Marks ==>		5		5		5		5		10	5
1	19X31A04A1	5		4						9	5
2	19X31A04A2			4		4				7	5
3	19X31A04A3			4		5				7	5
4	19X31A04A4	5		4						7	5
5	19X31A04A5					5		4		6	5
6	19X31A04A6					5		5		8	5
7	19X31A04A7			5		4				7	5
8	19X31A04A8	5				4				9	5
9	19X31A04A9					4		4		8	5
10	19X31A04B0					5		4		8	5
11	19X31A04B1	5		5						6	5
12	19X31A04B2	4		4						9	5
13	19X31A04B3			5		4				8	5
14	19X31A04B4					4		4		8	5
15	19X31A04B5					4		4		6	5
16	19X31A04B6			5		4				6	5
17	19X31A04B7	3		4						8	5
18	19X31A04B8	4		4						7	5
19	19X31A04B9			5		5				7	5
20	19X31A04C0					4		4		8	5
21	19X31A04C1					5		5		8	5
22	19X31A04C2	5		4						8	5
23	19X31A04C3	5								6	5
24	19X31A04C4	4		4						8	5
25	19X31A04C5			4		4				8	5
26	19X31A04C6					3		5		9	5
27	19X31A04C7					3		3		9	5
28	19X31A04C8			4		3				7	5
29	19X31A04C9	5		5						9	5
30	19X31A04D0	5		5						6	5
31	19X31A04D1			4		5				8	5
32	19X31A04D2					4		4		9	5
33	19X31A04D3	4		5						9	5
34	19X31A04D4			5		5				8	5
35	19X31A04D5					4		5		8	5
36	19X31A04D6					4		5		8	5
37	19X31A04D7			5		4				9	5
38	19X31A04D8	4		5						9	5
39	19X31A04D9	4		5						9	5
40	19X31A04E0			5		5				8	5
41	19X31A04E1			5		5				9	5
42	19X31A04E2			4		4				8	5
43	19X31A04E3					4		5		8	5
44	19X31A04E4					4		5		8	5

45	19X31A04E5			5		4				8	5
46	20X35A0421			4		4				9	5
47	20X35A0422			5		4				9	5
48	20X35A0423	5		5						8	5
49	20X35A0424	5		5						9	5
50	20X35A0425	5		5						8	5
51	20X35A0426			4		4				8	5
52	18X31A0403			3		4				7	5
53	18X31A0413			2						7	5
54	18X31A0454			4						5	5
55	18X31A04D4			4						6	5
56	18X31A04F1	3								8	5
57	18X31A04H2	3								8	5
58	18X31A04H7			5		4				8	5
Target set by the faculty / HoD		3.00	0.00	3.00	0.00	3.00	0.00	3.00	0.00	6.00	3.00
Number of students performed above the target		20	0	38	0	36	0	15	0	57	58
Number of students attempted		20	0	39	0	36	0	15	0	58	58
Percentage of students scored more than target		100%		97%		100%		100%		98%	100%

CO Mapping with Exam Questions:

CO - 1										
CO - 2										
CO - 3										
CO - 4	y		y						y	y
CO - 5					y				y	y
CO - 6							y		y	y

% Students Scored >Target %	100%		97%		100%		100%		98%	100%

CO Attainment based on Exam Questions:

CO - 1										
CO - 2										
CO - 3										
CO - 4	100%		97%						98%	100%
CO - 5					100%				98%	100%
CO - 6							100%		98%	100%

CO	**Subj**	obj	Asgn	Overall	Level
CO-1					
CO-2					
CO-3					
CO-4	99%	98%	100%	99%	3.00
CO-5	100%	98%	100%	99%	3.00
CO-6	100%	98%	100%	99%	3.00

Attainment Level	
1	40%
2	50%
3	60%

Attainment (Internal Examination-2) **3.00**

SRI INDU INSTITUTE OF ENGINEERING AND TECHNOLOGY

Department of Electronics and Communication Engineering

Course Outcome Attainment (University Examinations)

Name of the faculty :	Dr.T.Ramakrishna	Academic Year:	2022-23
Branch & Section:	ECE - C	Year / Semester:	IV/I
Course Name:	NS&C		

S.No	Roll Number	Marks Secured
1	19X31A04A1	33
2	19X31A04A2	34
3	19X31A04A3	30
4	19X31A04A4	28
5	19X31A04A5	26
6	19X31A04A6	29
7	19X31A04A7	36
8	19X31A04A8	37
9	19X31A04A9	26
10	19X31A04B0	26
11	19X31A04B1	27
12	19X31A04B2	26
13	19X31A04B3	38
14	19X31A04B4	30
15	19X31A04B5	5
16	19X31A04B6	32
17	19X31A04B7	1
18	19X31A04B8	28
19	19X31A04B9	26
20	19X31A04C0	26
21	19X31A04C1	26
22	19X31A04C2	26
23	19X31A04C3	0
24	19X31A04C4	32
25	19X31A04C5	29
26	19X31A04C6	27
27	19X31A04C7	6
28	19X31A04C8	17
29	19X31A04C9	26
30	19X31A04D0	42
31	19X31A04D1	47
32	19X31A04D2	11
33	19X31A04D3	19
34	19X31A04D4	27
35	19X31A04D5	26
Max Marks		75

S.No	Roll Number	Marks Secured
36	19X31A04D6	21
37	19X31A04D7	27
38	19X31A04D8	12
39	19X31A04D9	17
40	19X31A04E0	42
41	19X31A04E1	28
42	19X31A04E2	30
43	19X31A04E3	28
44	19X31A04E4	27
45	19X31A04E5	6
46	20X35A0421	26
47	20X35A0422	29
48	20X35A0423	37
49	20X35A0424	45
50	20X35A0425	20
51	20X35A0426	10
52	18X31A0403	0
53	18X31A0413	2
54	18X31A0454	
55	18X31A04D4	
56	18X31A04F1	0
57	18X31A04H2	28
58	18X31A04H7	8

Class Average mark	24
Number of students performed above the target	39
Number of successful students	56
Percentage of students scored more than target	70%
Attainment level	**3**

Attainment Level	% students
1	40%
2	50%
3	60%

SRI INDU INSTITUTE OF ENGINEERING AND TECHNOLOGY

Department of Electronics and Communication Engineering

Course Outcome Attainment

Name of the faculty : Dr.T.Ramakrishna　　Academic Year: 2022-23

Branch & Section: ECE - C

Course Name: NS&C　　Year: IV

Semester: I

Course Outcomes	1st Internal Exam	2nd Internal Exam	Internal Exam	University Exam	Attainment Level
CO1	3.00		3.00	3.00	3.00
CO2	3.00		3.00	3.00	3.00
CO3	3.00		3.00	3.00	3.00
CO4		3.00	3.00	3.00	3.00
CO5		3.00	3.00	3.00	3.00
CO6		3.00	3.00	3.00	3.00
Internal & University Attainment:			3.00	3.00	
Weightage			25%	75%	
O Attainment for the course (Internal, Universit			0.75	2.25	
CO Attainment for the course (Direct Method)			3.00		

Overall course attainment level **3.00**

SRI INDU INSTITUTE OF ENGINEERING & TECHNOLOGY

Department of Electronics and Communication Engineering

Program Outcome Attainment (from Course)

Name of Faculty:	Dr.T.Ramakrishna	Academic Year:	2022-23
Branch & Section:	ECE - C	Year:	IV
Course Name:	NS&C	Semester:	I

CO-PO mapping

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	2	3	3											
CO2												3	2	
CO3	3	2	2								2			
CO4	3	2	3									2	1	
CO5	3		3		2						2			
CO6	2		2	2	2					2				1
Course	**2.60**	**2.33**	**2.60**	**2.00**	**2.00**					**2.00**	**2.00**	**2.50**	**1.50**	**1.00**

CO	**Course Outcome Attainment**
CO1	3.00
CO2	3.00
CO3	3.00
CO4	3.00
CO5	3.00
CO6	3.00
Overall course attainment level	**3.00**

PO-ATTAINMENT

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO Attainment	**2.60**	**2.33**	**2.60**	**2.00**	**2.00**					**2.00**	**2.00**	**2.50**	**1.50**	**1.00**

CO contribution to PO - 33%, 67%, 100% (Level 1/2/3)

IV ECE-C REGISTER

https://drive.google.com/file/d/1o6obrqkC2Q-HvwkFpff6g04sdttWqkX8/view?usp=sharing