



Estd. 2001

Sri Indu

College of Engineering & Technology

UGC Autonomous Institution

Recognized under 2(f) & 12(B) of UGC Act 1956,

NAAC, Approved by AICTE &

Permanently Affiliated to JNTUH



NAAC

NATIONAL ASSESSMENT AND
ACCREDITATION COUNCIL



HANDOUT

IV-CSE(AI&ML)-II Semester

DEPARTMENT OF CSE (ARTIFICIAL INTELLIGENCE & MACHINE LEARNING)

ACADEMIC YEAR 2025-26

**DEPARTMENT OF CSE(ARTIFICIAL INTELLIGENCE & MACHINE
LEARNING)**

HANDOUT-INDEX

SL.NO	CONTENTS
1	VISION, MISSION , PEO's,POs,PSOs,COs
2	Institutional Academic Calendar
3	Department Academic Calendar
4	Subject wise
i)	Lesson Plan
ii)	Question Bank
ii)	Model Question Paper
5	Assignment Questions



SRI INDU COLLEGE OF ENGINEERING & TECHNOLOGY

B.TECH – COMPUTER SCIENCE AND ENGINEERING

VISION OF THE INSTITUTE

To be a premier Institution in Engineering & Technology and Management with competency, values and social consciousness.

MISSION OF THE INSTITUTE

- IM₁** Provide high quality academic programs, training activities and research facilities.
- IM₂** Promote Continuous Industry-Institute interaction for employability, Entrepreneurship, leadership and research aptitude among stakeholders.
- IM₃** Contribute to the economical and technological development of the region, state and nation.

VISION OF THE DEPARTMENT

To be a technologically adaptive centre for computing by grooming the students as top notch professionals.

MISSION OF THE DEPARTMENT

- DM1:** To offer quality education in computing.
- DM2:** To provide an environment that enables overall development to all stakeholders.
- DM3:** To impart training on emerging technologies.
- DM4:** To encourage participation of stakeholders in research and development.

PROGRAM EDUCATIONAL OBJECTIVES (PEOs)

- PEO1: Higher Studies:** Graduate with an ability to pursue higher studies and get employment in reputed institutions and organizations.
- PEO2: Domain Knowledge:** Graduate with an ability to design and develop a product.
- PEO3: Professional Career:** Graduate with excellence by multidisciplinary approach to achieve successful professional career.
- PEO4: Life Long Learning:** Graduate with an ability to learn advanced skills to face professional competence through lifelong learning.

PROGRAM OUTCOMES (POs) & PROGRAM SPECIFIC OUTCOMES (PSOs)

POs	Description
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, review 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 the 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.
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.
PO7	Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
PO8	Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
PO9	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, and give and Receive clear instructions.
PO10	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.
PO11	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.
PROGRAM SPECIFIC OUTCOMES (PSOs)	
PSO1	To develop software projects using standard practices and suitable programming environment.
PSO2	To identify, formulate and solve the real life problems faced in the society, industry and other areas by applying the skills of the programming languages, networks and databases learned.
PSO3	To apply computer science knowledge in exploring and adopting latest technologies in various inter-disciplinary research activities.



SRI INDU COLLEGE OF ENGINEERING AND TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

COURSE OUTCOMES (CO's)

COURSE NAME: INFORMATION SECURITY FUNDAMENTALS (R22INF4233)

Course Outcomes (COs)	
C423.1	Understand the Information security and various Attacks. Analyze the effectiveness of passwords in access control.
C423.2	Understand the basic concepts of Cryptography, encryption and decryption techniques of various communication channels.
C423.3	Understand the Various network security applications, IPSec, Web security, Email security, and Kerberos, X.509 etc.
C423.4	Apply firewall principles, honey pots, IDS,IPS, authentication, mechanisms.
C423.5	Analyze diverse viewpoints to ethical dilemmas in the information technology field and recommend appropriate actions.
C423.6	Understand the role of third-party agents in the provision of authentication services



SRI INDU COLLEGE OF ENGINEERING AND TECHNOLOGY
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Mapping of Course Outcomes(CO's) with PO's / PSO's:

Course Articulation Matrix

COURSE NAME: (R22INF4233) Information Security Fundamentals

POs											
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
C423.1	3	2	-	-	-	-	-	-	-	-	-
C423.2	3	3	3	-	-	-	-	-	-	-	-
C423.3	2	3	3	3	-	-	-	-	-	-	-
C423.4	2	3	2	2	-	-	-	-	-	-	-
C423.5	2	3	3	2	-	-	-	-	-	-	-
C423.6	2	2	3	3	-	-	-	-	-	-	-
C423	2.33	2.67	2.8	2.5	-	-	-	-	-	-	-



SRI INDU COLLEGE OF ENGINEERING AND TECHNOLOGY
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CO-PO/PSO MAPPING

C423.1	Master Able to Understand the need of Security
---------------	--

Mapped POs: PO1, PO2

PO1	Student gains knowledge on cryptography and network security
PO2	Student identifies the advantages of cryptography and network security

C423.2	Master understanding of symmetric and asymmetric encryption systems, various attacks
---------------	--

Mapped POs: PO1, PO2, PO3

PO1	Student gains knowledge about information security Implementation.
PO2	Student analyses the problems related how an application communicates with hardware.
PO3	Student will be able to overcome the problems of security attacks Implementation.

C423.3	Master the role of third-party agents in the provision of authentication services.
---------------	--

Mapped POs: PO1, PO2, PO3, PO4

PO1	Student gains knowledge about the agents, third party criteria
PO2	Analyses problems related to security .
PO3	Student compares various attacks and authentication services
PO4	Designs different problems of security attacks and authentication services

C423.4	Comprehend and apply authentication, email security, web security services and mechanisms.
---------------	--

Mapped POs: PO1, PO2, PO3, PO4

PO1	Student gains knowledge about different securities
PO2	Analyses different services and mechanisms
PO3	Overcomes security attack problems
PO4	Design different email and web securities

C423.5	Master different protocol like SSL, TLS Vis-à-vis their applications
---------------	--

Mapped POs: PO1, PO2, PO3, PO4

PO1	Student gains knowledge about different protocols
PO2	Analyses SSL,TSL applications
PO3	Compares various protocols
PO4	Students are able to Implement different protocols

C423.6	Master the effectiveness of passwords in access control, security services and mechanisms.
---------------	--

Mapped POs: PO1, PO2, PO3, PO4

PO1	Student gains knowledge about effectiveness of passwords
PO2	Student Analyses the problems related to passwords
PO3	Student designs the different passwords and mechanisms
PO4	Provides protection by using security services



Lr.No.SICET/AUTO/DAE/IV B.Tech Academic Calendar/28/2025

B.TECH IV-YEAR I-SEM & II-SEM ACADEMIC CALENDAR
(FOR ACADEMIC YEAR : 2025-26)

Academic Calendar for B.Tech – 4th Year Students (2022 - 23 Batch), BR-22 Regulation.

I – Semester

S.No.	EVENT	PERIOD	DURATION
1.	Commencement of class work.	07.07.2025 (Monday)	
2.	1 st Spell of Instructions for covering First Two and a half Units.	07.07.2025 – 30.08.2025	8 Weeks
3.	I Mid Term Examinations.	01.09.2025 – 03.09.2025	3 Days
4.	Submission of I Mid Term Examination Marks.	10.09.2025	
5.	2 nd Spell of Instructions for Remaining Two and a half Units.	04.09.2025 – 27.09.2025	3 Weeks 2 Days
6.	Continuation of 2 nd Spell of Instructions.	06.10.2025 – 18.11.2025	6 Weeks
7.	II Mid Term Examinations.	19.11.2025 – 21.11.2025	3 Days
8.	Preparation Holidays and Practical Examinations	24.11.2025 – 29.11.2025	1 Week
9.	Submission of II Mid Term Examination Marks.	26.11.2025	
10.	I Semester End Examinations.	01.12.2025 – 13.12.2025	2 Weeks
Commencement of Class-Work for IV B.Tech - II Semester 15.12.2025			

Note: No of Working/instructional days : 91

II – Semester

S.No.	EVENT	PERIOD	DURATION
1.	Commencement of class work.	15.12.2025 (Monday)	
2.	1 st Spell of Instructions for covering First Two and a half Units.	15.12.2025 – 14.02.2026	9 Weeks
3.	I Mid Term Examinations.	16.02.2026 – 18.02.2026	3 Days
4.	Submission of I Mid Term Examination Marks.	24.02.2026	
5.	2 nd Spell of Instructions for Remaining Two and a half Units.	19.02.2026 – 29.04.2026	9 Weeks 3 Days
6.	II Mid Term Examinations.	30.04.2026 – 02.05.2026	3 Days
7.	Preparation Holidays and Project Evaluation.	04.05.2026 – 09.05.2026	1 Week
8.	Submission of II Mid Term Examination Marks.	07.05.2026	
9.	II Semester End Examinations	11.05.2026 – 16.05.2026	1 Week

Note: No of Working/instructional days : 90

ACE

CE

DIRECTOR

PRINCIPAL

Controller of Examination
Sri Indu College of Engineering & Technology
(An Autonomous Institution Under UGC)
Sheriguda (V), Ibrahimpatnam, R.R. Dist-501510

DIRECTOR
Sri Indu College of Engineering & Technology
(An Autonomous Institution Under UGC)
Sheriguda (V), Ibrahimpatnam, R.R. Dist-501510

PRINCIPAL
Sri Indu College of Engineering & Technology
(An Autonomous Institution Under UGC)
Sheriguda (V), Ibrahimpatnam, R.R. Dist-501510

Sign:

Dr. M.V.S.S. Giridhar
Prof. of CEA; JNTUH Nominee

Sign:

Dr. T. Venu Gopal
Prof. of CSE; JNTUH Nominee

Sign:

Dr. D. Ramesh
Prof. of CSE; JNTUH Nominee

(Copy to DAP&E and Copy to all the Dept. Heads)

INFORMATION SECURITY FUNDAMENTALS

SRIINDUCOLLEGE OF ENGINEERING & TECHNOLOGY

(An Autonomous Institution under UGC, New Delhi)

B. Tech.-IV Year– II Semester

OPEN ELECTIVE- III

L	T	P	C
3	0	0	3

(R22INF4233) Information Security Fundamentals

COURSE OBJECTIVES:

1. To provide impeccable knowledge on various technical aspects of Information Security & Computer Security principles
2. To provide foundation for understanding the key issues associated with protecting Computer Systems & Information Assets.
3. To provide competency in designing consistent & reasonable Information security system with appropriate Scanning & Enumeration mechanisms, determining the level of protection and Response to security incidents.

UNIT I: Introduction to Information Security- Introduction to Information Security, Need for Security - Threats to security & Attacks, Computer System Security and Access Controls – System access and data access.

UNIT II: Communication Security- Introduction to cryptography, cryptosystems, encryption and decryption techniques, classical encryption techniques, communication channel used in cryptographic system, various types of ciphers, cryptanalysis, hash function and data integrity, security of hashing function.

UNIT III: Network - Introduction to Network Security, Email Security, IP Security, Web Security, Kerberos, X.509 techniques.

UNIT IV: Scanning & Enumeration Technology- Malicious software, Firewalls, Honeypots, Intrusion Detection system, Intrusion Prevention system

UNIT V: Ethics In Information Security - Implementing Information Security, Legal Ethical & Professional issues in Information Security.

TEXTBOOKS:

1. Matt Bishop, "Computer Security: Art and Science", Addison-Wesley Professional, First Edition, 2003. ISBN: 0201440997.
2. William Stallings, "Cryptography and Network Security", Pearson Education, Fourth Edition, 2006. ISBN: 8177587749

REFERENCES:

1. Michael E. Whitman, Herbert J. Mattord, "Principles of Information Security" Cengage Learning, Fourth Edition, 2010, ISBN: 1111138214
2. Charlie Kaufman, Radia Perlman, Mike Speciner, "Network security: private communication in a public world", Second Edition, ISBN: 0130460192.
3. Dieter Gollmann, "Computer Security", Third Edition, ISBN: 0470741155.



SRI INDU COLLEGE OF ENGINEERING & TECHNOLOGY
LESSON PLAN
(Regulation :R22)
Department of CSE(ARTIFICIAL INTELLIGENCE&MACHINE LEARNING)

Page: 17 -3

Sub. Code & Title

**R22INF4233 INFORMATION SECURITY
FUNDAMENTALS**

Academic Year: 2025-26

Year/Sem./Section

IV-II/A/B

Faculty Name & Designation

Assistant Professor : Mr A.Naresh

Unit/ Item No.	Topic (s)	Book Reference	Page (s)		Teaching Methodolog y	Proposed No. of Periods	Actual Date of Handled	CO/RBT
			From	To				
	UNIT-I							
1	INTRODUCTION - INFORMATION SECURITY					10		
1.1	Introduction to Information Security	T1	1	2	Black board	01		CO1,L2
1.2	Need for Security	T1	3	8	Black board	02		CO1,L6
1.3	Threats to security & Attacks	T1	11,102	14,105	Black board	02		CO1,L1
1.4	Computer System Security	T1	14	18	Black board	01		CO1,L2
1.5	Access Controls	T1	136	140	Black board	02		CO1,L2
1.6	System access and Data access	T1			Black board	02		CO1,L1
	Review	Signature of the HOD/Coordinator						

Unit/ Item No.	Topic (s)	Book Reference	Page (s)		Teaching Methodolog y	Proposed No. of Periods	Actual Date of Handled	CO/RBT
			From	To				
	UNIT-II							
2	COMMUNICATION SECURITY					14		
2.1	Introduction to cryptograph.	T1	288	295	Black board	01		CO2,L1
2.2	Cryptosystems	T1	288	289	Black board	01		CO2,L2
2.3	Encryption & Decryption Techniques	T1	289	290	Black board	02		CO2,L1
2.4	Classical Encryption Techniques	T1			Black board	02		CO2,L2
2.5	Communication channel used in Cryptographic System,	T1	407	408	Black board	02		CO2,L1
2.6	Various types of ciphers	T1	299	305	Black board	02		CO2,L2

2.7	Cryptanalysis	T1	305	306	Black board	01		CO2,L3
2.8	Hash function and Data integrity	T1	311, 378	312, 379	Black board	02		CO2,L4
2.9	Security of Hashing function	T1			Black board	01		CO2,L1
	Review	Signature of the HOD/Coordinator						

Unit/ Item No.	Topic (s)	Book Reference	Page(s)		Teaching Methodology	Proposed No. of Periods	Actual Date of Handled	CO/RBT
			From	To				
	UNIT-III							
3	NETWORK					08		
3.1	Introduction to Network Security	T1	299,322	300,323	Black board	02		CO3,L2
3.2	Email Security	T1			Black board	01		CO3,L3
3.3	IP Security	T3	661	662	Black board	01		CO3,L1
3.4	Web Security	T2	441	443	Black board	01		CO3,L1
3.5	Kerberos	T1,T2	152,32 4	153, 340	Black board	01		CO3,L3
3.6	X.509 techniques	T1	341	349	Black board	02		CO3,L3
	Review	Signature of the HOD/Coordinator						

Unit/ Item No.	Topic (s)	Book Reference	Page (s)		Teaching Methodolog y	Proposed No. of Periods	Actual Date of Handled	CO/RBT
			From	To				
	UNIT-IV							
4	SCANNING & ENUMERATION TECHNOLOGY					08		
4.1	Mallicious Software	T1	99, 355	99, 355	Black board	02		CO4,L2
4.2	Firewalls	T1	108,341	108,344	Black board	01		CO4,L1
4.3	Honey Pots	T1	392	392	Black board	01		CO4,L2
4.4	Intrusion Detection System	T1	234	238	Black board	02		CO4,L1
4.5	Intrusion Prevention System	T1	241	266	Black board	02		CO4,L6
	Review	Signature of the HOD/Coordinator						

Unit/ Item No.	Topic (s)	Book Reference	Page (s)		Teaching Methodolog y	Proposed No. of Periods	Actual Date of Handled	CO/RBT
			From	To				
	UNIT-V							
5	ETHICS IN INFORMATION SECURITY					10		
5.1	Implementing Information Security	T1	456	456	Black board	02		CO5,L2
5.2	Legal Ethical & Professional Issues in Information Security	T1	452	487	Black Board	04		CO5,L2
	Review	Signature of the HOD/Coordinator						

TEXT BOOKS:

- T1. Fundamentals of Information Systems Security: David Kim, Michael G.Solomon, 3rd Edition
T2. Cryptography and Network Security: William Stallings, Pearson Education, 4th Edition
T3. Cryptography and Network Security: William Stallings, Pearson Education, 7th Edition
T4. Cryptography and Network Security: Atul kahate, Mc Graw Hill, 3rdEdition
T5. Cryptography and Network Security: William Stallings, Pearson Education, 2nd Edition

REFERENCE BOOKS:

- R1. Cryptography and Network Security: C K Shyamala, N Harini, Dr. T R Padmanabhan, Wiley India, 1st Edition
R2.Criptography and network Security, Forouzn Mukhopadhyay ,McGraw Hill,2nd edition
R3.Information Security, Principles and Practice: Mark Stamp, Wiley India
R4.Principles of Computer Security: VM Arthur Conklin, Greg White, TMH
R5.Introduction to Network Security: Neal Krawetz, CENGAGE Learning.
R6.Network Security and Cryptography: Bernard Menezes, CENGAGE Learning.

Web Links:

W1:<https://nptel.ac.in/courses/106105031/39>

W2:http://www.cs.wm.edu/~hnw/courses/cs454/notes/lecture17_email.pdf

MID-ASSIGNMENT

	SRI INDU COLLEGE OF ENGINEERING & TECHNOLOGY LESSON PLAN (Regulation :R22) Department of CSE(ARTIFICIAL INTELLIGENCE&MACHINE LEARNING)		Page: 17 -3
	Sub. Code & Title	R22INF4233 INFORMATION SECURITY FUNDAMENTALS	
	Academic Year: 2025-26	Year/Sem./Section	IV/II/ A/B
	Faculty Name & Designation	Assistant Professor : Mr.A.Naresh	

INFORMATION SECURITY FUNDAMENTALS ASSIGNMENT MID-1(CSE-A/B)**Roll Number: 22D41A6601-22D41A6605, 22D41A6665-22D41A6669**

Q.NO	QUESTION	BT Level	Course Outcome
1.	Define Information Security?	1	CO1
2.	Write in detail about security attacks, services, mechanisms?	2	CO1
3.	Define Cryptography	1	CO2
4.	Explain about Communication channel used in Cryptography System?	2	CO2
5.	Define digital signature?	1	CO3

Roll Number: 22D41A6606-22D41A6610, 22D41A6670-22D41A6675

Q.NO	QUESTION	BT Level	Course Outcome
1.	What are the characteristics of Information Security?	1	CO1
2.	Explain inter-network security?	2	CO1
3.	Define plaintext and cipher text?	1	CO2
4.	a. Write about substitution techniques. b. Write about transposition techniques.	2	CO2
5.	Simplify model for Network Security?	4	CO3

Roll Number: 22D41A6611-22D41A6615, 22D41A6676-22D41A6681

Q.NO	QUESTION	BT Level	Course Outcome
1.	What are the multiple layers of Security?	1	CO1
2.	List the types of security attacks with example.	1	CO1
3.	Write about the various Types of ciphers?	2	CO2
4.	Compare encryption and decryption?	2	CO2
5.	What is Email Security?	1	CO3

Roll Number: 22D41A6616-22D41A6620, 22D41A6682-22D41A6686

Q.NO	QUESTION	BT Level	Course Outcome
1.	What are the components of information system?	1	CO1
2.	Explain Information Security and explain its significance in today's world.	5	CO1
3.	Determine a Hash function?	5	CO2
4.	Explain about Security of Hashing Function.	5	CO2
5.	Write about web security considerations?	2	CO3

Roll Number: 22D41A6621-22D41A6625, 22D41A6687-22D41A6691

Q.NO	QUESTION	BT Level	Course Outcome
1S5	List the functions of Information Security?	4	CO1
1L5	Discuss the following terms in detail with relevant examples: a. Interruption b. Interception c. Modification d. Fabrication	6	CO1
2S5	Define cryptanalysis?	1	CO2
2L5	What are applications of public key cryptography? Explain them briefly.	1	CO2
3S5	Explain the basic objectives of network security?	5	CO3

Roll Number: 22D41A6626-22D41A6630, 22D41A6692-22D41A6696

Q.NO	QUESTION	BT Level	Course Outcome
1.	Explain the types of security attacks?	2	CO1
2.	Explain the types of access control? Explain them briefly.	2	CO1
3.	Determine about Data Integrity?	5	CO2
4.	Construct AES encryption and decryption process with neat sketch?	3	CO2
5.	With a neat diagram write about a model for Network security	2	CO3

Roll Number: 22D41A6631-22D41A6635, 22D41A6697-22D41A66A1

Q.NO	QUESTION	BT Level	Course Outcome
1.	List the types of access controls?	4	CO1
2.	Summarize about access control in security PDF?	2	CO1
3.	Explain about various types of ciphers in cryptography?	2	CO2
4.	Discuss briefly about Encryption and Decryption Techniques?	6	CO2
5.	What is X.509 authentication service?	1	CO3

Roll Number: 22D41A6636-22D41A6640, 22D41A66A2-22D41A66A6

Q.NO	QUESTION	BT Level	Course Outcome
1.	What is the need for security?	1	CO1
2.	Discuss the difference between Discretionary Access Control and Mandatory Access Control?	6	CO1
3.	Distinguish encryption and decryption techniques?	4	CO2
4.	Write the importance of secure hash function with relevant examples	2	CO2
5.	Name the different functionalities in the network security?	1	CO3

Roll Number: 22D41A6641-22D41A6645, 22D41A66A7-22D41A66B1

Q.NO	QUESTION	BT Level	Course Outcome
1.	Write about system and data access?	2	CO1
2.	Explain about Computer System Security.	2	CO1
3.	Explain about communication security	2	CO2
4.	Explain briefly how diffusion and confusion increases complexity to the art the Cryptanalyst?	2	CO2
5.	Describe the requirements in web security. Explain the various web security threats.	2	CO3

Roll Number: 22D41A6646-22D41A6650, 22D41A66B3-22D41A66B7

Q.NO	QUESTION	BT Level	Course Outcome
1.	Explain the measures to protect the confidentiality of information?	2	CO1
2.	Explain encapsulating Security Payload?	5	CO1
3.	Define about security in hash function	1	CO2
4.	Explain all the principles of the public key crypto systems?	2	CO2
5.	Describe security association	5	CO3

Roll Number: 22D41A6651-22D41A6655, 22D41A66B8-22D41A66C2

Q.NO	QUESTION	BT Level	Course Outcome
1.	When can a computer be a subject and an object of an attack respectively?	1	CO1
2.	Describe the Critical Characteristics of Information.	2	CO1
3.	Define Cryptosystems	1	CO2
4.	What are the Challenge of Symmetric Key Cryptosystem?	1	CO2
5.	Discuss Kerberos v4 and Kerberos v5?	6	CO3

Roll Number: 22D41A6656-22D41A6660, 22D41A66C3-22D41A66C7

Q.NO	QUESTION	BT Level	Course Outcome
1.	Why is a methodology important in implementing the information security?	1	CO1
2.	Explain the Components of an Information System.	2	CO1
3.	What are the types of Cryptanalytic attacks?	1	CO2
4.	Explain about Diffie-Hellman Key exchange?	2	CO2
5.	Determine how X.509 certificate is revoked?	5	CO3

Roll Number: 22D41A6661-23D45A6601, 22D41A66C8-23D45A6609

Q.NO	QUESTION	BT Level	Course Outcome
1.	Can you explain what the term authorization means in the context of access control?	5	CO1
2.	Which industries could benefit from an access control system?	1	CO
3.	Define SSL?	1	CO2
4.	Explain the Types of Cryptanalytic attacks	2	CO2
5.	Define Information Security?	1	CO1

Roll Number: 23D45A6602-23D45A6606, 23D45A6610-23D45A6613

Q.NO	QUESTION	BT Level	Course Outcome
1.	What is the need for security?	1	CO1
2.	Discuss the difference between Discretionary Access Control and Mandatory Access Control?	6	CO1
3.	Distinguish encryption and decryption techniques?	4	CO2
4.	Write the importance of secure hash function with relevant examples	2	CO2
5.	Name the different functionalities in the network security?	1	CO3

Levels	Bloom's Taxonomy level mapping	Total Marks Covered	%age
L1	Remembering	5	16.66%
L2	Understanding	15	50%
L3	Applying	-	-
L4	Analyzing	10	33.33%
L5	Evaluating	-	-
L6	Creating	-	-

CO & BT Mapping for Assignment-1

	SRI INDU COLLEGE OF ENGG & TECH QUESTION BANK (Regulation :R22) Department of CSE(ARTIFICIAL INTELLIGENCE&MACHINE LEARNING)			Prepared On Rev1: Page:1to27
	Sub.Code& Title	R22INF4233 & Information Security Fundamentals		
	AcademicYear:2025-26	Year/Sem./Section	IV-II/AIML	
	Faculty Name& Designation	Assistant Professor: Mr A.Naresh		

UNIT I: Introduction to Information Security- Introduction to Information Security, Need for Security - Threats to security & Attacks, Computer System Security and Access Controls – System access and data access.

	Multiple choice Questions	BT Level	Course Outcome
1C-1	What is the primary goal of information security? A) Protecting data B) Ensuring availability C) Preventing breaches D) All of the above	I	CO1
1C-2	What type of threat comes from within an organization? A) External B) Internal C) Natural D) Physical	I	CO1
1C-3	Which is a common social engineering attack? A) Phishing B) DDoS C) SQL Injection D) Buffer Overflow	I	CO1
1C-4	What does DDoS stand for? A) Distributed Denial of Service B) Direct Denial of Service C) Dynamic Denial of Service	I	CO1
1C-5	What is the primary goal of access control? A) To grant all users full access B) To restrict access to authorized users C) To remove all security measures D) To increase system complexity	I	CO1

1C-6	Which authentication method uses multiple factors? A) Single-factor B) Multi-factor C) Biometric D) Token-based	I	CO1
1C-7	What does MAC stand for in access control? A) Mandatory Access Control B) Media Access Control C) Maximum Access Control D) Managed Access Control	II	CO1
1C-8	Which model uses roles for access control? A) DAC (Discretionary Access Control) B) MAC (Mandatory Access Control) C) RBAC (Role-Based Access Control) D) ABAC (Attribute-Based Access Control)	I	CO1
1C-9	Which method restricts data access? A) Encryption B) Decryption C) Compression D) Backup	II	CO1
1C-10	What does RBAC stand for? A) Role-Based Access Control B) Rule-Based Access Control C) Resource-Based Access Control D) Risk-Based Access Control	II	CO1
1C-11	Which of the following ensures data confidentiality? A) Encryption B) Hashing C) Encoding D) Compression	I	CO1
1C-12	What does ABAC stand for? A) Attribute-Based Access Control B) Action-Based Access Control C) Access-Based Attribute Control D) Attribute-Based Authentication Control	I	CO1

1C-13	Which attack targets system vulnerabilities? A) Zero-day B) Brute Force C) Dictionary Attack D) Man-in-the-Middle	I	CO1
1C-14	What type of attack overwhelms a system with traffic? A) Phishing B) DDoS C) SQL Injection D) Malware	II	CO1
1C-15	ISF stand for _____ in information security? A) Information Security Framework B) Information Security Fundamentals C) Information Security Function D) Information Security Foundation	II	CO1

Fill in the blanks

1F-1	Info security protects _____ assets.	I	CO1
1F-2	The CIA triad includes Confidentiality, Integrity, and _____	I	CO1
1F-3	_____ threats come from within an organization.	II	CO1
1F-4	Security involves _____ and procedures.	I	CO1
1F-5	Security is needed to protect against _____	I	CO1
1F-6	_____ threats target system vulnerabilities.	I	CO1
1F-7	Phishing is a common _____ attack.	I	CO1
1F-8	Organizations face _____ threats from insiders.	II	CO1
1F-9	System security involves controlling _____ access.	I	CO1

1F-10	_____ authentication uses multiple factors.	I	CO1
1F-11	Access control models include _____ I	I	CO1
1F-12	System logs help with _____ activities.	I	CO1

1F-13	Access controls ensure only _____ users can access data.	I	CO1
1F-14	_____ controls limit system access.	I	CO1
1F-15	_____ is a method to restrict data access.	I	CO1
Match the following			
1M-1	(i) CIA Triad A) Potential for harm to assets (ii) Security Threat B) Identify, assess, mitigate risks (iii) Security Control C) Confidentiality, Integrity, Availability (iv) Risk Management D) Safeguard or countermeasure	I	CO1
1M-2	(i) Asset Value A) Regulations, threats, business needs (ii) Threat Impact B) Restricting resource access (iii) Security Drivers C) Potential harm to assets (iv) Access Control D) Determines security level needed	IV	CO1
1M -3	(i) Malware A) Deceptive trick to steal info (ii) Phishing B) Software designed to harm (iii) Denial of Service-DOS C) Attacks database queries (iv) SQL Injection D) Overwhelms system resources	II	CO1
1M -4	(i) Authentication A) Protecting data confidentiality (ii) Data Encryption B) Handling security breaches (iii) System Hardening C) Verifying user identity (iv) Incident Response D) Reducing vulnerabilities	II	CO1
1M -5	(i) Authorization A) Enforcing strict access rules (ii) Mandatory Access Control-MAC B) Risk from authorized users (iii) Role-Based Access Control-RBAC C) Determining access rights (iv) Insider Threat D) Assigning access by role	IV	CO1

UNIT I

PART-B

1.	Write in detail about security attacks, services, mechanisms?	VI	CO1
2.	With a neat diagram write about a model for Network security. (R16-MAR21 & R16- OCT20 & R16-DEC19)	II	CO1
3.	Write the types of security attacks with example?	II	CO1
4.	Distinguish between symmetric key and asymmetric key cryptography.	II	CO1

5.	Difference between substitution techniques and transposition techniques.	II	CO1
6.	Define Caesar cipher? And calculate the encryption and decryption for the following plain text P="COME TO MY HOME" by using caser cipher with Key k=3?	II	CO1
7.	Construct all kinds of cipher techniques in the cryptography?	II	CO1
8.	Classify the following plain text message P="come to my home today using Row Transposition.	II	CO1
9.	Classify the following plain text P="TRUST MEE" into cipher text by Caesar cipher with key k= 4.	II	CO1
10.	Classify the following plain text message P=0110111 into cipher text by using one- time pad cipher with key K=1011001.calculate both encryption and decryption for the above message.	VI	CO1
11.	a) List briefly categories of security mechanisms? b) What is meant by authentication and availability?	II	CO1
12.	Define plaintext, cipher text and Cryptography?	I	CO1
13.	a)Define encryption and decryption and Information Security?	I	CO1
14.	a) Simplify model for Network Security? b) What are the types of security attacks?	II	CO1
15.	Define steganography and cryptanalysis?	II	CO1

UNIT II - Communication Security-Introduction to cryptography, cryptosystems, encryption and decryption techniques, classical encryption techniques, communication channel used in cryptographic system, various types of ciphers, cryptanalysis, hash function and data integrity, security of hashing function.

Multiple choice Questions			
2C-1	What is the main difference between symmetric and asymmetric cryptography? A) Key usage B) Speed C) Algorithm type D) Block size	II	CO2
2C-2	_____ is a symmetric encryption technique? A) RSA B) AES C) Hash function D) Digital signature	II	CO2
2C-3	Which of the following is NOT a type of cryptosystem? A) Symmetric-key B) Asymmetric-key C) Hash function D) Compression algorithm	II	CO 2

2C-4	Which type of cipher encrypts data in fixed-length blocks? A) Stream cipher B) Block cipher C) Hash function D) Digital signature	III	CO 2
2C-5	What is cryptosystem? A) A type of encryption algorithm B) A secure communication system C) A type of hash function D) A decryption technique	I	CO 2
2C-6	The hash function's output is called ____? A) Digest B) Block C) Stream D) Key	I	CO 2
2C-7	Which of the following is an example of a hash function? A) SHA-256 B) AES C) RSA D) SSL/TLS	I	CO 2
2C-8	What is the process of decryption A) Converting plaintext to ciphertext B) Converting ciphertext to plaintext C) Creating a hash function D) Breaking a cipher	I	CO2
2C-9	What happens if a hash function is vulnerable to collisions? A) Data integrity is compromised B) Data is encrypted C) Computation is fast D) Data is compressed	II	CO2

2C-10	Why is collision resistance important in hash functions? A) For fast computation B) For data compression C) For data integrity D) For encryption	II	CO2
2C-11	Which attack tries to find two inputs with the same hash output? A) Preimage attack B) Collision attack C) Brute-force attack D) Dictionary attack	II	CO2
2C-12	"preimage resistance" means in hash functions? A) Hard to find original data from hash B) Hard to find two inputs with same hash C) Fast computation D) High entropy	I	CO2
2C-13	A primary security goal of a hash function is ? A) Speed B) Compression C) Collision resistance D) Encryption	II	CO2
2C-14	Which of the following is a technique used in cryptanalysis? A) Frequency analysis B) Differential cryptanalysis C) Linear cryptanalysis D) All of the above	I	CO2
2C-15	Which of the following is a type of encryption algorithm? A) Block cipher B) Stream cipher C) Hash function D) Both A and B	II	CO2

Fill in the blanks			
2F-1	Cryptography involves transforming plaintext into _____ using algorithms.	I	CO2
2F-2	_____ cryptography uses the same key for encryption and decryption.	I	CO2
2F-3	A cryptosystem typically involves _____ and decryption processes.	I	CO2
2F-4	_____ encryption uses a pair of keys for encryption and decryption.	I	CO2
2F-5	The _____ cipher is a simple substitution technique.	I	CO2
2F-6	Data is transmitted through a _____ channel in a crypto system.	I	CO2
2F-7	_____ ciphers encrypt data bit by bit.	I	CO2
2F-8	A hash function ensures _____ of data.	I	CO2
2F-9	_____ attack involves trying all possible keys.	I	CO2
2F-10	A hash function vulnerable to _____ that attacks can be broken.	II	CO2
2F-11	_____ is a key property of a good hash function.	I	CO2
2F-12	_____ mechanisms ensure data isn't modified unauthorized.	I	CO2
2F-13	_____ is a type of symmetric encryption algorithm.	II	CO2
2F-14	1The process of _____ involves converting ciphertext to plaintext.	I	CO2
2F-15	Hash functions help verify _____ of data.	I	CO2
MATCH THE FOLLOWING:			
2M-1	(i) Cipher Type A) Fixed length, Continuous (ii) Cipher Operation B) AES, RC4 (iii) Cipher Example C) Interception, Encryption (iv) Channel Concern D) Block, Stream	I	CO 2
2M-2	(i) AES A) Rivest-Shamir-Adleman ii) RSA B) File Transfer Protocol (iii) FTP C) HyperText Transfer Protocol (iv) HTTP D) Advanced Encryption Standard	I	CO 2
2M-3	(i) Symmetric encryption A) 64 bits (ii) Asymmetric encryption B) 128,192 or 256 bits (iii) AES Block size C) 2048 bits or more (iv) DES key size D) 128-bits	II	CO 2

2M-4	(i) Encryption (ii) Hashing, (iii) Compress (iv) Decryption	A) Converting data size into fixed string size B) Ciphertext to plaintext C) Plaintext to ciphertext D) Reduces data size	II	CO 2
2M-5	(i) Substitution (ii) Transposition (iii) Monoalphabetic (iv) Polyalphabetic	A) one fixed map B) replace letters C) multiple changing maps D) rearrange the order of letters	III	CO 2

UNIT II

PART-B

1.	Discuss Feistel's cipher structure with a neat diagram?	II	CO2
2	Write in detail about simple-DES and AES.	II	CO2
3.	Write about the various key distribution methods?	II	CO2
4	Prove encryption and decryption using RSA algorithm for a) $p=3, q=11, e=7, m=5$ b) $p=11, q=13, e=11, m=7$. (R16-MAR21 & R16-OCT20)	III	CO2
5.	Discuss the RSA and Diffie Hellman algorithm.	IV	CO2
6	Show AES encryption and decryption process with neat sketch?	III	CO2
7.	Explain briefly about RSA algorithm and IDEA in a detail manner?	II	CO2
8.	Explain about Blowfish Algorithm with example	IV	CO2
9.	Explain briefly how diffusion and confusion increases complexity to thwart the cryptanalyst?	II	CO2
10	Explain all the principles of the public key crypto systems? (R14-NOV/DEC 17)	II	CO2
11	What are the components of conventional encryption principles? What are the conventional encryption algorithms?	II	
12	What are public key cryptosystems algorithms? What are applications of public key cryptography?	II	CO2
13	Define product cipher? Explain RC4 Location?	I	CO2
14	a) Determine session key and master key? b) Determine link and end-to-end encryption?	II	CO2
15	a) Simplify the design criteria of block cipher? b) Explain Advantages of counter mode ?	II	CO2

	UNIT III: Network - Introduction to Network Security, Email Security, IP Security, Web Security, Kerberos, X.509 techniques.		
	PART - A Multiple choice Questions	BT Level	Course Outcome
3C.1	Which device filters network traffic? A) Router B) Switch C) Firewall D) Hub	II	CO3
3C.2	What does VPN stand for? A) Virtual Private Network B) Virtual Public Network C) Verified Private Network D) Value Private Network	I	CO3
3C.3	Network security threats include? A) Malware B) DoS attacks C) Unauthorized access D) All of the above	II	CO3
3C.4	What protects network data in transit? A) Encryption B) Compression C) Authentication D) Firewalls	I	CO3
3C-5	What protects email content? A) Encryption B) Compression C) Hashing D) Encoding	II	CO3

3C.6	Email authentication methods include? A) SPF B) DKIM C) DMARC D) All of the above	II	CO3
3C.7	IPsec provides security at which layer? A) Application B) Transport C) Network D) Data Link	I	CO3
3C.8	What are the two main IPsec protocols? A) AH and ESP B) TCP and UDP C) HTTP and FTP D) DNS and DHCP	II	CO3
3C-9	What protects against XSS attacks? A) Input validation B) Output encoding C) Both A and B D) Firewalls	IV	CO3
3C-10	What is Kerberos primarily used for? A) Network encryption B) Authentication C) Data compression D) Firewall configuration	II	CO3
3C-11	Which protocol does Kerberos use for authentication? A) Ticket-based B) Token-based C) Password-based D) Biometric-based	I	CO3
3C-12	What are the three main components of Kerberos? A) Client, Server, KDC B) Client, Server, Firewall C) User, Server, Database D) Client, Router, Switch	I	CO3

3C-13	What does TGT stand for in Kerberos? A) Ticket Granting Ticket B) Token Granting Ticket C) Ticket Granting Token D) Target Granting Ticket	II	CO3
3C-14	What is the role of the KDC in Kerberos? A) Key Distribution Center B) Key Decision Center C) Key Data Center D) Key Domain Center	III	CO3
3C-15	What is a key component of an X.509 certificate? A) Public key B) Private key C) Password D) IP address	II	CO3
	FILL IN THE BLANKS		Course Outcome
3F.1	Network security protects _____ from unauthorized access.	II	CO3
3F.2	Key goals include ensuring _____ of data.	II	CO3
3F.3	Common threats are _____ and malware.	I	CO3
3F.4	Firewalls help with _____ control.	II	CO3
3F.5	Email security protects against _____	II	CO3
3F.6	_____ is used to encrypt email content.	II	CO3
3F.7	Phishing attacks often use _____ emails.	II	CO3
3F-8	SPF, DKIM help with _____	II	CO3
3F-9	Web security protects against _____ attacks.	II	CO3
3F-10	HTTPS uses _____ to secure data.	II	CO3
3F-11	_____ attacks target user input fields.	II	CO3
3F-12	Firewalls help with _____ control.	II	CO3
3F-13	The _____ grants access to services.	III	CO3

3F-14	Kerberos relies on _____ for encryption.	III	CO3
3F-15	IPsec provides _____ for IP packets.	I	CO3
	MATCH THE FOLLOWING		
3M-1	(i) X.509 standards for _____ A) includes public key (ii) X.509 certificates _____ B) digital certificates (iii) Certificate Authority-CA _____ C) revoked certs (iv) Certificate Revocation Lists tracks _____ D) validates certificate authenticity	II	CO3
3M-2	(i) Kerberos _____ A) Key Distribution Center to issue tickets. (ii) Kerberos used for _____ B) grants access to services. (iii) Ticket Granting Service-TGS _____ C) symmetric key for encryption (iv) Kerberos relies _____ D) network authentication protocol.	II	CO3
3M-3	(i) HTTPS _____ A) XSS or SQL injection (ii) Cross-Site Scripting-XSS _____ B) Validate user input (iii) Web Security Measure _____ C) Injects malicious scripts (iv) Web Threat _____ D) Encrypts web traffic	I	CO3
3M-4	(i) SPF _____ A) Hypertext Transfer Protocol Secure (ii) DKIM _____ B) Virtual Private Networks (iii) VPNs _____ C) Domain Keys Identified Mail (iv) HTTPS _____ D) Sender Policy Framework	II	CO3
3M-5	(i) Firewall Function _____ A) Multiple layers of defenses (ii) Network Security Layer _____ B) Control incoming/outgoing traffic (iii) Email Encryption _____ C) Transport or Tunnel (iv) IPSec Mode _____ D) Protects email content	III	CO3

UNIT-III			
PART-B			
1.	Write in detail about Digital signature? (R16-DEC 19 & R14 NOV/DEC 17)	II	CO3
2	What is X.509 authentication service? (R16-DEC 19)	II	CO3
3.	Write short notes on message authentication code?	IV	CO3
4	Write the importance of secure hash function with relevant examples? Differentiate between direct digital signature and arbitrated digital signature?	I	CO3
5.	Discuss Kerberos v4 and Kerberos v5?	I	CO3
6	Determine how X.509 certificate is revoked?	I	CO3
7.	Describe briefly what are the different kinds of the authentication requirements are there for message authentication?	I	CO3
8.	Describe why Kerberos is more secure than the other security mechanisms? (R16-MAR21 & R16-OCT20)	I	CO3
9.	Describe the message digest function in digital signatures and explain with an example?	III	CO3
10	Write in detail about Digital Signature?	IV	CO3
11	a) What are advantages and disadvantages of Kerberos? b) What is Hash function?	II	CO3
12	a) What are the parameters of HMAC algorithms? b) Discuss HMAC and CMAC?	II	CO3
13	Define Message Authentication code and Extend key principles of Biometric Authentication?.	II	CO3
14	Enumerate uses of public key cryptography?	I	CO3
15.	Explain the rules of public and private key?	I	

UNIT-IV- Scanning&EnumerationTechnology-Malicioussoftware,Firewalls,Honeypots,Intrusion Detection system, Intrusion Prevention system			
MULTIPLE CHOICE QUESTIONS			
4C-1	What type of malware encrypts data for ransom? A) Ransomware B) Adware C) Spyware D) Rootkit	I	CO4
4C-2	What does ransomware typically demand? A) Payment for decryption B) Payment for removal C) Software updates D) System reboot	I	CO4
4C-3	What spreads malware via infected websites? A) Drive-by download	I	CO4

	B) Phishing C) SQL injection D) DDoS		
4C-4	Which kind of firewall filters traffic is based on IP addresses and ports? A) Packet filtering firewall B) Stateful inspection firewall C) Application layer firewall D) Proxy firewall	II	CO4
4C-5	What is a stateful inspection firewall? A) Tracks connection states B) Filters based on IP addresses C) Blocks all incoming traffic D) Encrypts data	IV	CO4
4C-6	Which type of firewall is acts as an intermediary? A) Proxy firewall B) Packet filtering firewall C) Stateful inspection firewall D) Application layer firewall	I	CO4
4C-7	What is a honey pot in cybersecurity? A) A decoy system to attract attackers B) A secure server for sensitive data C) A type of firewall D) A malware removal tool	IV	CO4
4C-8	Honey pot is designed as a _____ to mimic a real system? A) High-interaction honey pot B) Low-interaction honey pot C) Medium-interaction honey pot D) Production honey pot	I	CO4
4C-9	What is a honeypot used for? A) Detecting intrusions B) Attracting attackers C) Blocking malware D) Encrypting data	V	CO4
4C-10	What does IDS primarily do? A) Blocks intrusions B) Detects and alerts on intrusions	I	CO4

	C) Encrypts data D) Authenticates users		
4C-11	What type of IDS monitors network traffic? A) NIDS B) HIDS C) AIPS D) SIDS	I	CO4
4C-12	1A disadvantage of IDS is ____? A) Generates false positives B) Blocks all attacks C) Encrypts data slowly D) Authenticates users weakly	IV	CO4
4C-13	How does an IPS differ from an IDS? A) IPS only detects, IDS blocks B) IPS blocks, IDS only detects C) IPS is software, IDS is hardware D) IPS is for networks, IDS for hosts	I	CO4
4C-14	What does a Trojan typically do? A) Replicates itself B) Encrypts data C) Disguises as legitimate software D) Deletes files	I	CO4
4C-15	Firewalls can be ____? A) Hardware-based B) Software-based C) Both A and B D) None of the above	I	CO4
	FILL IN THE BLANKS	BT	
4F-1	Malware includes viruses, worms, and _____	I	CO4
4F-2	_____ malware self-replicates.	III	CO4
4F-3	Ransomware typically demands a _____	I	CO4

4F-4	Spyware aims to steal _____	I	CO4
4F-5	Firewalls control incoming and outgoing _____	I	CO4
4F-6	_____ firewalls filter traffic by ports/IPs.	I	CO4
4F-7	Stateful firewalls track _____ connections.	I	CO4
4F-8	Next-gen firewalls include _____ inspection.	I	CO4
4F-9	_____ IDS analyses network packets.	III	CO4
4F-10	IDS can be configured to alert on _____ thresholds.	I	CO4
4F-11	A false positive in IDS means _____ alert.	II	CO4
4F-12	IPS can operate in _____ mode.	II	CO4
4F-13	IDS monitors network traffic for _____ activities.	II	CO4
4F-14	Honeypots are _____ systems to lure attackers.	I	CO4
4F-15	IPS uses signatures to detect known _____	II	CO4
	MATCH THE FOLLOWING		
4M-1	(i) Virus A) Demands payment for data (ii) Trojan Horse B) Secretly monitors activity (iii) Ransomware C) Self-replicating malware (iv) Spyware D) Disguised malicious code .	I	CO4
4M-2	(i) Packet Filtering A) Tracks connection states (ii) Stateful Inspection B) Examines packet headers (iii) Proxy Firewall C) Includes advanced features like IPS (iv) Next-Gen Firewall D) Acts as intermediary	I	CO4
4M-3	(i) Network Firewall A) Detect and block attacks (ii) Worm B) Low-interaction or high-interaction (iii) Honeypot Type C) Self-spreading malware (iv) IPS Function D) Protects network perimeter	I	CO4
4M-4	a) process automation i) focuses on a particular market or function b) Line of Business Organization ii) measure and control industrial processes c) Process Instrumentation iii) metrics or measures used to evaluate process d) Quality indicators iv) Automating business workflows	I	CO4
5M-5	(i) IPS Technique A) IPS blocks, IDS alerts (ii) IPS vs IDS B) Network-based or host-based (iii) IDS Technique C) Signature-based detection (iv) IDS Type D) Signature-based or anomaly-based		
	PART-B		

4D-1	Explain about web security considerations?	II	CO4
4D-2	What is secure socket layer ,briefly explain about it?	VI	CO4
4D-3	Write down differences between SSL and TLS?	IV	CO4
4D-4	Explain about transport layer security?	IV	CO4
4D-5	Explain about IEEE802.11 with neat diagram?	III	CO4
4D-6	Write about HTTPS detail?	III	CO4
4D-7	Explain about secure shell?	VI	CO4
4D-8	Write a short notes on wireless LAN	IV	CO4
4D-9	Explain about IEEE802.11?	VI	CO4
4D-10	Write about web security requirements?	I	CO4
4D-11	Define SSL and TLS?	II	CO4
4D-12	Define HTTPS and SSH ?	I	CO4
4D-13	Write about mobile device security and 4 properties of HTTP?	II	CO4
4D-14	Write about wireless LAN and Where we use wireless LAN?	I	CO4

UNIT-V- CCPDS-R Case Study and Future Software Project Management Practices Modern Project Profiles, Next-Generation software Economics, Modern Process Transitions.

MULTIPLE CHOICE QUESTIONS			
5C-1	What is a key step for implementing info security? A) Conduct risk assessment B) Install antivirus software C) Block all internet access D) Hire a security team	I	CO5
5C-2	What does a risk assessment identify? A) Vulnerabilities and threats B) Security policies C) Network topology D) Employee roles	II	CO5
5C-3	Security policies should be __? A) Documented and communicated B) Kept secret C) Changed daily D) Ignored if outdated	II	CO5
5C-4	What is a benefit of security awareness training? A) Reduces human error risks	II	CO5

	B) Increases network speed C) Blocks malware D) Encrypts data		
5C-5	_____ protects the encryption? A) Data confidentiality B) Network speed C) System availability D) User passwords	II	CO5
5C-6	What is a security metric? A) Measure of security effectiveness B) Type of firewall C) Encryption algorithm D) Network protocol	III	CO5
5C-7	What does GDPR stand for? A) General Data Protection Regulation B) Global Data Privacy Rule C) General Digital Rights Act D) Government Data Protection Regime	II	CO5
5C-8	What is a key ethical principle in info security? A) Respect for privacy B) Maximize data collection C) Share data freely D) Prioritize business needs	II	CO5
5C-10	HIPAA regulated for _____? A) Healthcare data privacy B) Financial data security C) Network security rules D) Software patents	II	CO5
5C-11	What is a professional responsibility?	III	CO5

	A) Protecting sensitive data B) Sharing passwords C) Ignoring updates D) Disabling security controls		
5C-12	Security professionals often need? A) Continuous learning B) Fixed skillsets C) No certifications D) Minimal training	II	CO5
5C-13	What is a key professional issue in info security? A) Balancing security and usability B) Ignoring user needs C) Focusing only on tech D) Outsourcing all security	II	CO5
5C-14	security professional faces ____ issues? A) Conflicting priorities B) Clear-cut decisions C) No budget constraints D) Full user cooperation	I	CO5
5C-15	Which can leads to insider threats? A) Disgruntled employees B) Strong security controls C) Happy workforce D) Outsourced security	II	CO5
	FILL IN THE BLANKS	BT Level	Course Outcome
5F-1	Information security involves protecting _____	I	CO5
5F-2	A key principle is the _____ model.	I	CO5
5F-3	Security measures include access _____	II	CO5
5F-4	Incident _____ is crucial for security.	I	CO5
5F-5	Information security professionals must follow _____ laws.	II	CO5

5F-6	Ethical hacking is done with _____ permission.	III	CO5
5F-7	_____ deals with data privacy regulations.	II	CO5
5F-8	Professionals must adhere to a _____ of conduct.	III	CO5
5F-9	Organizations must comply with _____ laws.	III	CO5
5F-10	Ethical decisions involve considering _____	II	CO5
5F-11	Professionals should adhere to a _____ of ethics.	III	CO5
5F-12	Info security pros must maintain _____	II	CO5
5F-13	_____ is key to building trust.	II	CO5
5F-14	Pros should stay updated with _____ advancements.	I	CO5
5-15	Handling incidents requires _____ skills.	II	CO5
	MATCH THE FOLLOWING		
5M-1	(i) GDPR (ii) HIPAA (iii) Continuous Learning (iv) Communicating Risks	A) Informing stakeholders effectively B) Data protection regulation C) Healthcare data privacy D) Updating security skills	I CO5
5M-2	(i) Responsible Disclosure (ii) Intellectual Property (iii) Compliance (iv) Professional Ethics	A) Following legal requirements B) Acting responsibly and transparently C) Protecting software rights D) Ethical vulnerability reporting	I CO5
5M-3	(i) Respect for Privacy (ii) Transparency (iii) Confidentiality (iv) Ethical Hacking	A) Testing security with permission B) Protecting sensitive info C) Protecting personal data D) Clear security practices	II CO5
5M-4	(i) Insider Threats guidelines (ii) Security Policies (iii) Security Awareness (iv) Balancing Security and Usability	A) Documented security B) Finding the right trade-off C) Risks from employees D) Training users on security	I CO5

5M-5	(i) Ethical Issue A) Follow laws and policies (ii) Ethics Guideline B) Report security breaches (iii) Ethical Behavior C) Respect privacy (iv) Ethical Principle D) Data breach disclosure	III	CO5
	PART B		CO5
5D-1	Write clearly about public key management in PGP?	II	CO5
5D-2	Describe how Authentication and Confidentiality are handled in S/MIME?	IV	CO5
5D-3	Draw a neat diagram and write about IP Security Architecture? (R16-DEC 19)	V	CO5
5D-4	Write about Authentication header?	II	CO5
5D-5	Write briefly about Encapsulating security payload format? (R16-DEC 19)	V	CO5
5D-6	Enumerate all services of PGP and explain with neat sketch. (R16-MAR21 & R16-OCT20)	II	CO5
5D-7	Justify why S/MIME is a security enhancement to MIME internet email format standard?	III	CO5
5D-8	Describe how encapsulating security payload is defined?	V	CO5
5D-9	Describe and explain how the security will be provided in Email?	III	CO5
5D-10	Define payload? And discuss about encapsulating security payload?	IV	CO5
5D-11	What is Email Security and cookie?	I	CO5
5D-12	What are authentication and, confidentiality? What is tunnel mode?	II	CO5
5D-13	What are benefits of IPsec and List out notations used in PGP?	II	CO5
5D-14	Explain about Email compatibility? List MIME content Type?	II	CO5
5D-15	Define Authentication Header? Explain encapsulating Security Payload?	I	CO5

QUESTION PAPERS



SRI INDU COLLEGE OF ENGINEERING & TECHNOLOGY

(An Autonomous Institution under UGC, New Delhi) - Recognized under 2(f) and 12(B) of UGC Act 1956

IV B.Tech. II Semester (REGULAR and SUPPL.) End Examinations, June - 2023.

(R18INF4295) INFORMATION SECURITY FUNDAMENTALS

05/06/2023

(For CSE and IT)

Day- 3 (FN)

Duration: 3 Hrs

Maximum Marks: 70M

Blooms Taxonomy : (I-Remembering, II-Understanding, III-Applying, IV-Analyzing, V-Evaluating and VI-Creating)

Course Outcome : CO

PART - A

Answer all the following questions.

(5Qx 4M = 20M)

1. Define information security and describe its key concepts.
2. What is symmetric key cryptography? Discuss its advantages.
3. What is Web security and why is it important?
4. What is Malware? How to Stay Protected from Malware Attacks?
5. Justify the impact of Law and Ethics in Information Security.

II	CO1
VI	CO2
I	CO3
III	CO4
V	CO5

PART - B

Answer FIVE questions choosing at least one from each unit

(5Qx10M = 50M)

UNIT-I

6. a) Enumerate the types of attacks.
- b) Explain the need and principles of security.

II	CO1
I	CO1

OR

7. Describe the critical characteristics of information. How are they used in the study of computer security?

II	CO1
----	-----

UNIT-II

8. With a neat diagram explain how encryption and decryption are done using Blowfish algorithm?

III	CO2
-----	-----

OR

9. a) Compare and contrast linear and differential cryptanalysis.
- b) Describe block cipher modes of operation.

VI	CO2
II	CO2

UNIT-III

10. a) Explain the model for Network Security.
- b) Compare and contrast Kerberos version 4 and 5.

I	CO3
VI	CO3

OR

11. Give the general structure of IP security authentication header. Describe how anti-replay service is supported?

III	CO3
-----	-----

UNIT-IV

12. What is a firewall? List the characteristics of a good firewall implementation. How is circuit gateway different from application gateway?

IV	CO4
----	-----

OR

13. What is Intrusion? What are the measures used for intrusion detection? Discuss Intrusion detection system with neat diagram.

II	CO4
----	-----

UNIT-V

4. Interpret the importance of Legal, Ethical and Professional issues during the security investigation.

IV	CO5
----	-----

OR

5. What are the steps do we need to know in implementing the information security program? Explain the approaches to implementing information security.

II	CO5
----	-----

BR-18

SRI INDU COLLEGE OF ENGINEERING & TECHNOLOGY
IV B.Tech - II Semester - I Mid Term Examination, March - 2023
(R18INF4295) INFORMATION SECURITY FUNDAMENTALS

D4

Duration: 90 Mins

Dt: 27-03-2023, Day-3 (AN)

Max Marks: 25M

Section - AAnswer All the questions

* (I-Remembering, II-Understanding, III-Appling, IV-Analyzing, V-Evaluating, and VI-Creating.)

Marks: 5Qx1M = 5M

1. What are the characteristics of Information Security?
2. Explain the types of security attacks.
3. Define Cryptography.
4. Explain about communication security.
5. What is Email Security?

* Bloom's Taxonomy Level	Course Outcomes
I	CO1
II	CO2
I	CO3
II	CO3
I	CO4

Section - BAnswer any FOUR questions

Marks: 4Qx5M = 20M

6. Write in detail about security attacks, services, mechanisms.
7. Explain about Computer System Security.
8. a) Write about substitution techniques.
b) Write about transposition techniques.
9. Construct AES encryption and decryption process with neat sketch.
10. Explain briefly how diffusion and confusion increases complexity to the art the Cryptanalyst.
11. What is X.509 authentication service?

II	CO2
II	CO2
II	CO3
II	CO3
III	CO3
II	CO3
I	CO4

BR-18

SRI INDU COLLEGE OF ENGINEERING & TECHNOLOGY
IV B.Tech - II Semester - II Mid Term Examination, May - 2023
(R18INF4295) INFORMATION SECURITY FUNDAMENTALS

D4

Duration: 90 Mins

Dt: 23-05-2023, Day-2 (FN)

Max Marks: 25M

Section - AAnswer All the questions

* (I-Remembering, II-Understanding, III-Appling, IV-Analyzing, V-Evaluating, and VI-Creating.)

Marks: 5Qx1M = 5M

1. What is VPN?
2. Explain about Honey pots.
3. Explain about the types of virus.
4. Explain about policy. How does it differ from a law?
5. What is the difference between law and ethics?

* Bloom's Taxonomy Level	Course Outcomes
II	CO4
V	CO5
II	CO5
V	CO3
I	CO3

Section - BAnswer any FOUR questions

Marks: 4Qx5M = 20M

6. Determine how X.509 certificate is revoked.
7. Describe why Kerberos is more secure than the other security mechanisms.
8. How does Scanning Works?
9. How to prevent attackers to stealing our information?
10. What are the three general categories of unethical and illegal behavior?
11. Justify why S/MIME is a security enhancement to MIME internet email format Standard.

V	CO4
VI	CO4
I	CO5
I	CO5
I	CO3
V	CO3

ASSIGNMENT QUESTIONS

SRI INDU COLLEGE OF ENGG & TECH

Department of CSE(ARTIFICIAL INTELLIGENCE&MACHINE LEARNING) INFORMATION SECURITY FUNDAMENTALS

ASSIGNMENT QUESTION

1. What are the types of security attacks?
2. Simplify model for Network Security?
3. Distinguish between symmetric key and asymmetric key cryptography
4. Classify the following
plain text P= "TRUST MEE" into cipher text by Caesar cipher with key k= 4.
5. What are applications of public key cryptography?
6. Simplify the design criteria of block cipher?
7. Show AES encryption and decryption process with neat sketch?
8. Discuss HMAC and CMAC?
9. Explain the rules of public and private key?
10. Define Message Authentication code?
11. Write the importance of secure hash function with relevant examples?
12. Differentiate between direct digital signature and arbitrated digital signature?

13. Describe briefly what are the different kinds of the authentication requirements are there for message authentication?
14. Write about web security considerations?
15. Define IEEE802.11?
16. Where we use wireless LAN?
17. What is secure socket layer, briefly explain about it?
18. What are authentication and confidentiality?