K L Deemed to be University
Department of Computer Science and Engineering-Honors -- KLVZA
Course Handout
2023-2024, Odd Sem

Course Title	:CRYPT ANALYSIS AND CYBER DEFENCE
Course Code	:21CS3041A
L-T-P-S Structure	: 3-0-4-4
Pre-requisite	:
Credits	: 6
Course Coordinator	:Ruth Ramya Kalangi
Team of Instructors	:
Teaching Associates	:

Syllabus : Introduction to Security: Security Concepts, Security Attacks, A Security Model, Security , Services and Mechanisms, Antivirus bypassing, Password Attacks and Web browser exploitation. Block Ciphers: DES, DES Example, Strength of DES, Differential and Linear Cryptanalysis., AES: Finite Field Arithmetic, AES Structure, AES Transformation Functions, AES Example. Multiple Encryption and Triple DES. Modes of Operation. Pseudorandom Number Generation: Principles and Pseudorandom Number, Generators, Pseudorandom Number Generation using a Block Cipher, Stream Ciphers. Stream Ciphers: RC4.. Public-key Cryptography: RSA algorithm, Diffie-Hellman Key Exchange, ElGamal Cryptosystem, Elliptic Curve Arithmetic, Elliptic Curve Cryptography. . Cryptographic. Hash Functions: Applications of Cryptographic Hash functions, Two Simple Hash Functions, Requirements and Security, SHA 512, MD5. Performing Incident Response: Introduction to Incident Response Process, Cyber Incident Response Team, Communication Plan and Stakeholder Management, Incident Response Plan, Cyber Kill Chain Attack Framework, Incident Response, Disaster Recovery, and Retention Policy

Text Books :1. Cryptography and Network Security Principles and Practice, William stallings, 5th Edition, Pearson, 2011 2. Applied Cryptography: Protocols, Algorthms, and Source Code in C, Bruce Schneier, John Wiley & Sons, Second Edition, 1996. 3. Cyber Security Incident Management Guide, Gerard Johansen, Packt Publishing Ltd, 2017. 4.Digital Forensics & Incident Response, Gerard Johnson, Packt Publishing Ltd.2017

Reference Books :1. Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering, Hamid R. Nemati and Li Yang, IGI Global, 2011. 2. Cryptography and Network Security , Forouzon B, Indian Edition, TMH (2010)..

Web Links :1. https://www.linkedin.com/learning/cybersecurity-awareness-cybersecurity-terminology/welcome-to-cybersecurity-terminology-. 2.https://www.linkedin.com/learning/symmetric-cryptography-essential-training/cryptography-is-everywhere? 3. https://www.linkedin.com/learning/cybersecurity-foundations-22006082. 4. https://www.linkedin.com/learning/cybersecurity-foundations-security-architecture?trk=learning-path&upsellOrderOrigin=default_guest_learning .

MOOCS :1.https://onlinecourses.nptel.ac.in/noc23_cs127/preview 2. https://onlinecourses.nptel.ac.in/noc23_cs75/preview. 3. https://onlinecourses.nptel.ac.in/noc23_cs127/preview 4. https://www.coursera.org/learn/introduction-to-applied-cryptography. 5.https://www.coursera.org/learn/crypto-hashing. 6. https://www.coursera.org/learn/palo-alto-networks-network-security-fundamentals

Course Rationale : This course introduces the fundamental principles of cryptography and its applications on the network security domain. Students will become familiar with cryptographic techniques for secured communication over an unsecured channel; verification of the authenticity of the source of a message; verification of the integrity of the messages transmitted via an unsecured channel and unique identification of the originator of any message. Cryptanalysis attacks against the cryptographic techniques, and attack

models will be presented. Furthermore, it will be illustrated on how network security and management mechanisms employ cryptography to prevent, detect, and mitigate security threats against the network.

Course Objectives : The course aims to provide a comprehensive understanding of the fundamental principles of cryptography, including encryption, decryption, key management, and authentication. This course also covers various cryptographic algorithms such as symmetric key algorithms (e.g., AES, DES), asymmetric key algorithms (e.g., RSA, ECC), and hash functions (e.g., SHA-256). The objective is to understand the strengths, weaknesses, and applications of different algorithms. Vulnerabilities of cryptographic systems and defense mechanisms and countermeasures to mitigate these attacks are also analyzed in this course.

COURSE OUTCOMES (COs):

CO NO	Course Outcome (CO)	PO/PSO	Blooms Taxonomy Level (BTL)
CO1	Apply Classical Encryption Techniques and Symmetric Encryption algorithms to convert a given Plaintext to Cipher text.	PSO1,PO1,PO5	3
CO2	Apply RC4, Block Cipher Modes of Operation and Multiple Encryption for given plaintext	PSO1,PO1,PO5	3
CO3	Apply Public Key Crypto Systems which uses number theory to ensure Secure communication of data.	PSO1,PO1,PO5	3
CO4	Apply Hash, MAC algorithms, Digital Signatures and Incident Response concepts to achieve Message Authentication, Integrity and Incident Response	PO5,PSO1,PO1	3
CO5	Analyze social engineering, Ethical Hacking & Incident Responses using various tools and implement Encryption algorithms and Integrity algorithms.	PSO2,PO1,PO5	4

COURSE OUTCOME INDICATORS (COIs)::

Outcome No.	Highest BTL	COI-2	COI-3	COI-4
CO1	3	**Btl-2** Compare and Contrast Passive and Active Attacks.	**Btl-3** Apply Classical Encryption Techniques and DES algorithm with suitable examples and interpret attacks on them.	
CO2	3	**Btl-2** Summarize block cipher modes of operation & multiple encryption	**Btl-3** Apply RC4 algorithm for a given plaintext.	
CO3	3	**Btl-2** Illustrate Public Key Cryptosystem	**Btl-3** Apply RSA, Diffie-Hellman, Elgamal, Elliptic Curve Arithmetic and Cryptography to ensure data security.	
CO4	3	**Btl-2** Understand Hash Functions	**Btl-3** Apply two Simple Hash Functions and SHA 512 and	

		& MAC and their applications	MAC algorithm and forensics for a given message to Generate Hash Code and also for Incident Response	
CO5	4	**Btl-2** Summarize all security concepts like Confidentiality, Integrity and Authentication	**Btl-3** Implement various Encryption & Hash algorithms.	**Btl-4** Analyze social engineering, Ethical Hacking & Incident Responses using various tools

PROGRAM OUTCOMES & PROGRAM SPECIFIC OUTCOMES (POs/PSOs)

Po No.	Program Outcome
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 analyse 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 for complex problems that cannot be solved by straightforward application of knowledge, theories and techniques applicable to the engineering discipline.
PO5	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.
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	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
PO8	Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice
PO9	Individual and Team Work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
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, and 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 lifelong learning in the broadest context of technological change.
PSO1	An ability to design and develop software projects as well as Analyze and test user requirements.
PSO2	An Ability to gain working Knowledge on emerging software tools and technologies.

Lecture Course DELIVERY Plan:

Sess.No.	CO	COI	Topic	Book No[CH No][Page No]	Teaching-Learning Methods	EvaluationComponents
1	CO1	COI-2	Course Handout, Introduction to Security	T1, CH 1, Pg, {8,9]	Chalk,PPT,Talk	End Semester Exam,SEM-EXAM1
2	CO1	COI-2	Security Attacks, Services & Mechanisms, Model for Network Security	T1,CH[1], PG[15-25]	Chalk,PPT,Talk	End Semester Exam,SEM-EXAM1
3	CO1	COI-3	Substitution & Transposition Techniques	T1, CH[2] ,Pg [33-53]	Chalk,PPT,Talk	ALM,End Semester Exam,SEM-EXAM1
4	CO1	COI-3	SDES Algorithm	T1, CH[3],Pg[66-88]	Chalk,PPT,Talk	End Semester Exam,SEM-EXAM1
5	CO1	COI-2	DES Algorithms & Attacks	T1, CH[3], PG[68-89]	Chalk,PPT,Talk	ALM,End Semester Exam,SEM-EXAM1
6	CO1	COI-3	SAES Algorithms	T1, CH[5],Pg [148-174]	Chalk,PPT,Talk	End Semester Exam,MOOCs Certification,SEM-EXAM1
7	CO1	COI-2	AES Algorithm	T1, CH[5],Pg [148-174]	Chalk,PPT,Talk	End Semester Exam,SEM-EXAM1
8	CO1	COI-2	Block Cipher Design Principles	T1, CH [6], Pg[193]	Chalk,PPT,Talk	End Semester Exam,MOOCs Review,SEM-EXAM1
9	CO2	COI-2	Block Cipher Modes of Operation	T1, CH [6], Pg[198-201]	Chalk,PPT,Talk	End Semester Exam,SEM-EXAM1
10	CO2	COI-2	Block Cipher Modes of Operation	T1, CH[6],Pg[201-206]	Chalk,PPT,Talk	ALM,End Semester Exam,SEM-EXAM1
11	CO2	COI-3	Random Number Generators	T1,CH[7], Pg {219-226]	Chalk,PPT,Talk	End Semester Exam,SEM-EXAM1
12	CO2	COI-3	Random Number Generators	T1,CH[7], Pg[226]	Chalk,PPT,Talk	End Semester Exam,SEM-EXAM1
13	CO2	COI-2	Psuedorandom Number Generators using Block Ciphers.	T1,CH[7], Pg. [229]	Chalk,PPT,Talk	End Semester Exam,MOOCs Review,SEM-EXAM1
14	CO2	COI-3	Steam Ciphers & SRC4	T1, CH[7[, Pg, {232]	Chalk,PPT,Talk	ALM,End Semester Exam,MOOCs

Sess.No.	CO	COI	Topic	Book No[CH No][Page No]	Teaching-Learning Methods	EvaluationComponents
						Certification,SEM-EXAM1
15	CO2	COI-2	RC4 Algorithm	T1,CH[7], Pg [234]	Chalk,PPT,Talk	End Semester Exam,SEM-EXAM1
16	CO2	COI-2	Cryptanalysis on RC4	T1,CH[7], Pg [234]	Chalk,PPT,Talk	End Semester Exam,SEM-EXAM1
17	CO3	COI-2	Public Key Cryptography	T1, CH[269]	Chalk,PPT,Talk	End Semester Exam,SEM-EXAM2
18	CO3	COI-3	RSA Algorithm	T1, CH[10],Pg. [305]	Chalk,PPT,Talk	ALM,End Semester Exam,SEM-EXAM2
19	CO3	COI-3	Diffie-Hellman Key Exchange	T1, CH[10], PG. [301]	Chalk,PPT,Talk	End Semester Exam,MOOCs Review,SEM-EXAM2
20	CO3	COI-3	Elgamal Algorithm	T1, CH[10], pg. [305]	Chalk,PPT,Talk	ALM,End Semester Exam,SEM-EXAM2
21	CO3	COI-3	Elliptic Curve Arithmetic	T1, CH[10,pg. [308]	Chalk,PPT,Talk	End Semester Exam,SEM-EXAM2
22	CO3	COI-3	Elliptic Curve Arithmetic	T1, CH[10,PG, [308-317]	Chalk,PPT,Talk	End Semester Exam,MOOCs Certification,SEM-EXAM2
23	CO3	COI-2	Elliptic Curve Cryptography	T1, CH[10,PG, [308-317]	Chalk,PPT,Talk	End Semester Exam,SEM-EXAM2
24	CO4	COI-2	Hash Functions	T1, CH[11], PG.[329]	Chalk,PPT,Talk	End Semester Exam,SEM-EXAM2
25	CO4	COI-2	Hash Functions	T1, CH[11], PG.[329]	Chalk,PPT,Talk	End Semester Exam,SEM-EXAM2
26	CO4	COI-3	Hash Functions	T1,CH [11], PG. [333]	Chalk,PPT,Talk	End Semester Exam,SEM-EXAM2
27	CO4	COI-2	Cryptanalysis of Hash Functions	T1, CH[11[, PG[335].	Chalk,PPT,Talk	End Semester Exam,MOOCs Review,SEM-EXAM2
28	CO4	COI-2	SHA-512	T1, CH[11], PG[342]	Chalk,PPT,Talk	ALM,End Semester Exam,SEM-EXAM2
29	CO4	COI-	MD5	T1, CH[11],	Chalk,PPT,Talk	End Semester

Sess.No.	CO	COI	Topic	Book No[CH No][Page No]	Teaching-Learning Methods	EvaluationComponents
		2		PG.[342]		Exam,MOOCs Certification,SEM-EXAM2
30	CO4	COI-2	MAC Algorithms	T1, CH[12], PG. [362-372]	Chalk,PPT,Talk	ALM,End Semester Exam,SEM-EXAM2
31	CO4	COI-2	Introduction to Incident Response Process	T3	Chalk,PPT,Talk	End Semester Exam,SEM-EXAM2
32	CO4	COI-2	Cyber Incident Response Team	T3	Chalk,PPT,Talk	End Semester Exam,SEM-EXAM2
33	CO4	COI-2	Communication Plan and Stakeholder Management,	T3	Chalk,PPT,Talk	End Semester Exam,SEM-EXAM2
34	CO4	COI-2	Cyber Kill Chain Attack Framework	T3	Chalk,PPT,Talk	End Semester Exam,SEM-EXAM2
35	CO4	COI-2	Disaster Recovery	T3	Chalk,PPT,Talk	End Semester Exam,SEM-EXAM2
36	CO4	COI-2	Retention Policy	T3	Chalk,PPT,Talk	End Semester Exam,SEM-EXAM2
37	CO4	COI-2	REVISION	T3	Chalk,PPT,Talk	End Semester Exam,SEM-EXAM2
38	CO4	COI-2	REVISION	T1	Chalk,PPT,Talk	End Semester Exam,SEM-EXAM1,SEM-EXAM2
39	CO4	COI-2	REVISION	T1	Chalk,PPT,Talk	End Semester Exam,SEM-EXAM2

Lecture Session wise Teaching – Learning Plan

SESSION NUMBER : 1

Session Outcome: 1 Defines Security Concepts.

Session Outcome: 2 Demonstrates CIA Triangle

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---

20	Course Handout	2	Chalk	--- NOT APPLICABLE ---
20	Security Concepts & CIA Triangle	2	PPT	--- NOT APPLICABLE ---
5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 2

Session Outcome: 1 Define Security Attacks, Services & Mechanisms

Session Outcome: 2 Demonstrate Model for Network Security

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---
10	Security Attacks	2	PPT	--- NOT APPLICABLE ---
10	Security Services	2	Chalk	--- NOT APPLICABLE ---
10	Security Mechanisms	2	PPT	--- NOT APPLICABLE ---
10	Model for Network Security	2	PPT	--- NOT APPLICABLE ---
5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 3

Session Outcome: 1 Compare & Contrast substitution and transposition techniques.

Session Outcome: 2 Apply substitution and transposition techniques on a given plaintext.

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---
20	Substitution Techniques	3	Chalk	Puzzle, Enigma, Contradiction
20	Transposition Techniques	3	PPT	--- NOT APPLICABLE

5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 4

Session Outcome: 1 Demonstrate Symmetric Cipher Model

Session Outcome: 2 Apply SDES algorithm to generate ciphertext

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---
20	SDES Key Generation	3	Chalk	--- NOT APPLICABLE ---
20	SDES Encryption	3	PPT	--- NOT APPLICABLE ---
5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 5

Session Outcome: 1 Demonstrate DES Algorithm

Session Outcome: 2 Understand attacks on DES Algorithm

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---
20	DES Key Generation	2	PPT	--- NOT APPLICABLE ---
20	DES Encryption	2	PPT	Immediate feedback
5	Viva Voice	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 6

Session Outcome: 1 Apply SAES Algorithm to Generate Ciphertext

Session Outcome: 2 Demonstrate AES Algorithm

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---
20	SAES Algorithm	3	Chalk	--- NOT APPLICABLE ---
20	AES Algorithm	2	PPT	--- NOT APPLICABLE ---
5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 7

Session Outcome: 1 Demonstrate AES Algorithm

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---
20	AES Key Generation	2	PPT	--- NOT APPLICABLE ---
20	AES Encryption	2	PPT	--- NOT APPLICABLE ---
5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 8

Session Outcome: 1 Summarize Block Cpher Design Principles

Session Outcome: 2 Illustrate Double DES & Triple DES Algorithms

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---
20	Block Cipher Design Principles	2	PPT	--- NOT APPLICABLE ---
20	Double DES & Triple DES	2	PPT	--- NOT APPLICABLE ---

5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 9

Session Outcome: 1 Define Block Cipher

Session Outcome: 2 Summarize Block Cipher Modes of Operation

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---
20	Electronic Code Book	2	PPT	--- NOT APPLICABLE ---
20	Cipher Block Chaining Mode	2	Chalk	--- NOT APPLICABLE ---
5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 10

Session Outcome: 1 Define Block Cipher

Session Outcome: 2 Demonstrate CFB, OFB & Counter Block Cipher Modes of Operation

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---
20	Cipher Feedback Mode, Output Feedback Mode	2	PPT	Immediate feedback
20	Counter Mode	2	PPT	--- NOT APPLICABLE ---
5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 11

Session Outcome: 1 List Principles of Random Number Generation

Session Outcome: 2 Demonstrate types of Random Number Generators

Time(min)	Topic	BTL	Teaching-Learning	Active Learning

			Methods	Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---
20	Principles of Random Number Generation	3	Talk	--- NOT APPLICABLE ---
20	Types of Random Number Generation	3	PPT	--- NOT APPLICABLE ---
5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 12

Session Outcome: 1 Demonstrate types of Random Number Generators.

Session Outcome: 2 Apply Psuedorandom Number Generators.

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---
20	LCG	3	Chalk	--- NOT APPLICABLE ---
20	BBS	3	PPT	--- NOT APPLICABLE ---
5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 13

Session Outcome: 1 Demonstrate Psuedorandom Number Generators using Block Ciphers.

Session Outcome: 2 Demonstrate X9.17 ANSI Ring

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---
20	Psuedorandom Number Generators using Block Ciphers.	2	PPT	--- NOT APPLICABLE ---
20	X9.17 ANSI Ring	2	Chalk	--- NOT APPLICABLE ---

5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 14

Session Outcome: 1 Summarize the concepts of Stream Cipher.

Session Outcome: 2 Apply SRC4 cipher to a given plaintext.

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---
20	Stream Ciphers	3	PPT	Quiz/Test Questions
20	SRC4	3	Chalk	--- NOT APPLICABLE ---
5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 15

Session Outcome: 1 Demonstrate RC4 cipher to a given plaintext

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---
20	RC4 Key Generation	2	PPT	--- NOT APPLICABLE ---
20	RC4 Encryption	2	PPT	--- NOT APPLICABLE ---
5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 16

Session Outcome: 1 Illustrate attacks Possible on RC4

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---

20	Attacks on RC4	2	PPT	--- NOT APPLICABLE ---
20	Attacks on RC4	2	PPT	--- NOT APPLICABLE ---
5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 17

Session Outcome: 1 Define Public Key Cryptosystems

Session Outcome: 2 List out applications of Principles of Public Key Cryptosystems

Session Outcome: 3 Summarize Principles of Public Key Cryptosystems

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---
10	Principles of Publickey Cryptoystem	2	PPT	--- NOT APPLICABLE ---
10	Publickey Cryptosystem -Confidentiality	2	PPT	--- NOT APPLICABLE ---
10	Publickey Cryptosystem -Authentication	2	PPT	--- NOT APPLICABLE ---
10	Publickey Cryptosystem -Confidentiality & Authentication	2	Chalk	--- NOT APPLICABLE ---
5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 18

Session Outcome: 1 Apply RSA Algorithm for a given value of plaintext.

Session Outcome: 2 Summarize attacks on RSA Algorithm

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---
20	RSA Algorithm	3	PPT	--- NOT APPLICABLE ---

20	Attacks on RSA	3	Chalk	Quiz/Test Questions
5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 19

Session Outcome: 1 Apply Diffie-Hellman Key Exchange Algorithms on different plaintexts.

Session Outcome: 2 Summarize Man-in-the-Middle attack on Diffie-Hellman Algorithm

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---
20	Diffie-Hellman Key Exchange Algorithm	3	PPT	--- NOT APPLICABLE ---
20	Man-in-the-Middle Attack	3	Chalk	--- NOT APPLICABLE ---
5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 20

Session Outcome: 1 Apply Elgamal Algorithms to generate ciphertext.

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---
20	Elgamal Algorithm	3	PPT	--- NOT APPLICABLE ---
20	Example on Elgamal Algorithm	3	Chalk	Quiz/Test Questions
5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 21

Session Outcome: 1 Summarizes properties of Abelian Group.

Session Outcome: 2 Differentiates Prime Curves and Binary Curves

Session Outcome: 3 Apply Elliptic Curve Arithmetic over Prime Curves

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---
20	Abelian Group	3	PPT	--- NOT APPLICABLE ---
20	Elliptic Curve Arithmetic Over Prime Curves	3	Chalk	--- NOT APPLICABLE ---
5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 22

Session Outcome: 1 Apply Elliptic Curve Arithmetic Binary Curves

Session Outcome: 2 Illustrates Elliptic Curve Diffie-Hellman Key Exchange Algorithm.

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---
20	Elliptic Curve Arithmetic Binary Curves	3	PPT	--- NOT APPLICABLE ---
20	Elliptic Curve Cryptography	3	Chalk	--- NOT APPLICABLE ---
5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 23

Session Outcome: 1 Demonstrate Elliptic Curve Cryptography

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---
20	Elliptic Curve Cryptography- Introduction	2	PPT	--- NOT APPLICABLE ---
20	Elliptic Curve Cryptography-Diffie Hellman Key Exchange	2	PPT	--- NOT APPLICABLE ---

5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 24

Session Outcome: 1 Define Hash Functions

Session Outcome: 2 List Properties of Hash Functions

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---
20	Hash Functions Introduction	2	PPT	--- NOT APPLICABLE ---
20	Properties of Hash Functions	2	Chalk	--- NOT APPLICABLE ---
5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 25

Session Outcome: 1 Define Hash Functions

Session Outcome: 2 List applications of Hash Functions

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---
20	Message Authentication	2	PPT	--- NOT APPLICABLE ---
20	Digital Signature & Other Application	2	Chalk	--- NOT APPLICABLE ---
5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 26

Session Outcome: 1 Apply simple Hash Functions

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods

5	Attendance	1	Talk	--- NOT APPLICABLE ---
20	Hash Function 1	3	PPT	--- NOT APPLICABLE ---
20	Hash Function 2	3	PPT	--- NOT APPLICABLE ---
5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 27

Session Outcome: 1 Summarize cryptanalysis of hash functions

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---
10	Brute Force Attack	2	PPT	--- NOT APPLICABLE ---
10	Birthday Paradox	2	PPT	--- NOT APPLICABLE ---
10	Birthday Attack	2	Chalk	--- NOT APPLICABLE ---
10	Meet-in-the-Middle-Attcak	2	PPT	--- NOT APPLICABLE ---
5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 28

Session Outcome: 1 Demonstrate SHA-512 hash algorithm.

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---
20	SHA-512 Block Diagram	2	PPT	--- NOT APPLICABLE ---
20	SHA-512 Single Round Operations	2	Chalk	One minute paper

5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 29

Session Outcome: 1 Demonstrate MD5 Hash Algorithm.

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---
20	MD5 Block Diagram	2	PPT	--- NOT APPLICABLE ---
20	MD5 Single Round Operation	2	PPT	--- NOT APPLICABLE ---
5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 30

Session Outcome: 1 List Applications of Illustrate MAC a

Session Outcome: 2 Illustrate MAC algorithms

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---
10	Applications of MAC	2	Talk	--- NOT APPLICABLE ---
10	HMAC	2	PPT	--- NOT APPLICABLE ---
10	DAA	2	PPT	--- NOT APPLICABLE ---
10	CMAC	2	Chalk	One minute paper
5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 31

Session Outcome: 1 Define Incident Response Process

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---
20	Introduction to Incident Response	2	PPT	--- NOT APPLICABLE ---
20	Introduction to Incident Response Process	2	PPT	--- NOT APPLICABLE ---
5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 32

Session Outcome: 1 Summarize Cyber Incident Response Team

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---
20	Cyber Incident Response Team	2	PPT	--- NOT APPLICABLE ---
20	Cyber Incident Response Team	2	PPT	--- NOT APPLICABLE ---
5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 33

Session Outcome: 1 Illustrate Communication Plan

Session Outcome: 2 Demonstrate Stakeholder Management,

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---
20	Communication Plan	2	PPT	--- NOT APPLICABLE ---
20	Stakeholder Management,	2	PPT	--- NOT APPLICABLE ---

5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 34

Session Outcome: 1 Demonstrate Cyber Kill Chain Attack Framework

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---
20	Cyber Kill Chain Attack Framework	2	PPT	--- NOT APPLICABLE ---
20	Cyber Kill Chain Attack Framework	2	PPT	--- NOT APPLICABLE ---
5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 35

Session Outcome: 1 Illustrate Disaster Recovery

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---
20	Disaster Recovery	2	PPT	--- NOT APPLICABLE ---
20	Disaster Recovery	2	PPT	--- NOT APPLICABLE ---
5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 36

Session Outcome: 1 Retention Policy

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---

20	Retention Policy	2	PPT	--- NOT APPLICABLE ---
20	Retention Policy	2	PPT	--- NOT APPLICABLE ---
5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 37

Session Outcome: 1 Recall Concepts of CO1

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---
20	REVISION	2	PPT	--- NOT APPLICABLE ---
20	REVISION	2	PPT	--- NOT APPLICABLE ---
5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 38

Session Outcome: 1 Revision of CO2 & CO3

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---
20	REVISION CO2	2	Talk	--- NOT APPLICABLE ---
20	REVISION CO3	2	Talk	--- NOT APPLICABLE ---
5	Summary	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 39

Session Outcome: 1 REVISION CO4

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
5	Attendance	1	Talk	--- NOT APPLICABLE ---
20	REVISION CO4	2	Talk	--- NOT APPLICABLE ---
20	REVISION CO4	2	Talk	--- NOT APPLICABLE ---
5	Summary	1	Talk	--- NOT APPLICABLE ---

Tutorial Course DELIVERY Plan: NO Delivery Plan Exists

Tutorial Session wise Teaching – Learning Plan

No Session Plans Exists

Practical Course DELIVERY Plan:

Tutorial Session no	Topics	CO-Mapping
1	Implementation of Caesar Cipher and Vigenère Cipher.	CO5
2	Implementation of Playfair Cipher substitution technique	CO5
3	Implementation of Railfence Transposition and Columnar Techniques	CO5
4	Implementation of Simplified Data Encryption Standard Algorithm	CO5
5	Implementation of AES Key Generation	CO5
6	Implementation of Substitute bytes and Shift rows operations in AES.	CO5
7	Implementation LCG and Blum-Blum Sub generators	CO5
8	Implementation of RSA Algorithm	CO5
9	Implementation of Diffie-Hellman Algorithm	CO5
10	Implementation a Two Simple Hash Functions	CO5
11	Implementation of SHA-512 Algorithm	CO5
12	Implementation of MD5 Algorithm	CO5

Tutorial Session no	Topics	CO-Mapping
13	Implementation of One Time Pad and Hill Cipher substitution technique	CO5
14	Implementation of simplified RC4	CO5
15	Implementation of Elgamal Cryptosystem Algorithm	CO5
16	Implement IPsec Site-to-Site	CO5
17	Detecting different attacks using Wireshark	CO5
18	Mounting Forensic Images for Scanning and Recovering Files from Forensic Image	CO5
19	Demonstration on security mechanism incorporated in router	CO5
20	Demonstration of security mechanism incorporated in switches.	CO5

Practical Session wise Teaching – Learning Plan

SESSION NUMBER : 1

Session Outcome: 1 Apply Caesar Cipher on a given Plaintext

Session Outcome: 2 Apply Vigenere Cipher on a given Plaintext

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Implementation of Caesar Cipher	3	LTC	--- NOT APPLICABLE ---
30	Implementation of Vigenere Cipher	3	LTC	--- NOT APPLICABLE ---
30	Viva Voice	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 2

Session Outcome: 1 Apply Playfair Cipher to encrypt the given Plaintext

Session Outcome: 2 Apply Playfair Cipher to decrypt the given Ciphertext

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods

10	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Implementation of Playfair Cipher - Encryption	3	LTC	--- NOT APPLICABLE ---
30	Implementation of Playfair Cipher - Decryption	3	LTC	--- NOT APPLICABLE ---
30	Viva Voice	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 3

Session Outcome: 1 Apply Railfence Transposition on a given Plaintext

Session Outcome: 2 Apply Columnar Transposition on a given Plaintext

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Implementation of Railfence Transposition	3	LTC	--- NOT APPLICABLE ---
30	Implementation of ColumnarTransposition	3	LTC	--- NOT APPLICABLE ---
30	Viva Voice	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 4

Session Outcome: 1 Implementation of Simplified Data Encryption Standard Key Generation Algorithm

Session Outcome: 2 Implementation of Simplified Data Encryption Standard Encryption Algorithm

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Implementation of Simplified Data Encryption Standard Key Generation Algorithm	3	LTC	--- NOT APPLICABLE ---
30	Implementation of Simplified Data Encryption Standard Encryption Algorithm	3	LTC	--- NOT APPLICABLE ---
30	Viva Voice	1	Talk	--- NOT APPLICABLE

SESSION NUMBER : 5

Session Outcome: 1 Apply AES Key Generation Algorithm to Generate Keys

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Implementation of AES Key Generation	3	LTC	--- NOT APPLICABLE ---
30	Results & Documentation	3	LTC	--- NOT APPLICABLE ---
30	Viva Voice	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 6

Session Outcome: 1 Apply AES Substitute Byte Operation on the Plaintext

Session Outcome: 2 Apply AES Shift Row Operation on the Plaintext

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Implementation of Substitute bytes in AES.	3	LTC	--- NOT APPLICABLE ---
30	Implementation of Shift rows operations in AES.	3	LTC	--- NOT APPLICABLE ---
30	Viva Voice	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 7

Session Outcome: 1 Apply LCG to generate random numbers

Session Outcome: 2 Apply BBS to generate random numbers

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE

30	Implementation LCG	3	LTC	--- NOT APPLICABLE ---
30	Implementation Blum-Blum Sub generators	3	LTC	--- NOT APPLICABLE ---
30	Viva Voice	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 8

Session Outcome: 1 Apply RSA Algorithm on given Plaintext

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Implementation of RSA Algorithm	3	LTC	--- NOT APPLICABLE ---
30	Results & Documentation	3	LTC	--- NOT APPLICABLE ---
30	Viva Voice	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 9

Session Outcome: 1 Apply Diffie-Hellman Algorithm

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Implementation of Diffie-Hellman Algorithm	3	LTC	--- NOT APPLICABLE ---
30	Results & Documentation	3	LTC	--- NOT APPLICABLE ---
30	Viva Voice	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 10

Session Outcome: 1 Apply Two Simple Hash Functions to Generate Hash Code

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Implementation a Two Simple Hash Functions	3	LTC	--- NOT APPLICABLE ---
30	Results & Documentation	3	LTC	--- NOT APPLICABLE ---
30	Viva Voice	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 11

Session Outcome: 1 Apply Implementation of SHA-512 Algorithm to Generate Hash Code

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Implementation of SHA-512 Algorithm	3	LTC	--- NOT APPLICABLE ---
30	Results & Documentation	3	LTC	--- NOT APPLICABLE ---
30	Viva Voice	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 12

Session Outcome: 1 Apply MD5 Algorithm to Generate Hash Code

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Implementation of MD5 Algorithm	3	LTC	--- NOT APPLICABLE ---
30	Results & Documentation	3	LTC	--- NOT APPLICABLE ---
25	Viva Voice	1	Talk	--- NOT APPLICABLE

SESSION NUMBER : 13

Session Outcome: 1 Apply One Time Pad on a given Plaintext

Session Outcome: 2 Apply Hill Cipher on a given Plaintext

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Implementation of One Time Pad substitution technique	3	LTC	--- NOT APPLICABLE ---
30	Implementation of Hill Cipher substitution technique	3	LTC	--- NOT APPLICABLE ---
30	Viva Voice	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 14

Session Outcome: 1 Apply SRC4 Algorithm to Generate Ciphertext

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Implementation of simplified RC4	3	LTC	--- NOT APPLICABLE ---
30	Results & Documentation	3	LTC	--- NOT APPLICABLE ---
30	Viva Voice	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 15

Session Outcome: 1 Apply Elgamal Cryptosystem Algorithm on a Given Plaintext

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE ---

30	Implementation of Elgamal Cryptosystem Algorithm	3	LTC	--- NOT APPLICABLE ---
30	Results & Documentation	3	LTC	--- NOT APPLICABLE ---
30	Viva Voice	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 16

Session Outcome: 1 Apply IPsec Site-to-Site

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Implement IPsec Site-to-Site	3	LTC	--- NOT APPLICABLE ---
30	Results & Documentation	3	LTC	--- NOT APPLICABLE ---
30	Viva Voice	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 17

Session Outcome: 1 Apply Wireshark and detect attacks

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Detecting different attacks using Wireshark	3	LTC	--- NOT APPLICABLE ---
30	Results & Documentation	3	LTC	--- NOT APPLICABLE ---
30	Viva Voice	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 18

Session Outcome: 1 Apply Forensic Images for Scanning and Recovering Files

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Mounting Forensic Images for Scanning and Recovering Files from Forensic Image	3	LTC	--- NOT APPLICABLE ---
30	Results & Documentation	3	LTC	--- NOT APPLICABLE ---
30	Viva Voice	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 19

Session Outcome: 1 Apply security mechanism on Router

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Demonstration on security mechanism incorporated in router	3	LTC	--- NOT APPLICABLE ---
30	Results & Documentation	4	LTC	--- NOT APPLICABLE ---
30	Viva-Voice	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 20

Session Outcome: 1 Apply security mechanism on Switches

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Demonstration of security mechanism incorporated in switches.	3	LTC	--- NOT APPLICABLE ---
30	Results & Documentation	4	LTC	--- NOT APPLICABLE ---
30	Viva Voice	1	Talk	--- NOT APPLICABLE

Skilling Course DELIVERY Plan:

Skilling session no	Topics/Experiments	CO-Mapping
1	Installation of virtual box and Kali Linux.	CO5
2	Implementation of Packet Capturing Using Airodump-ng	CO5
3	Implementation of Social Engineering Using Ghost Phisher	CO5
4	Implementation of Password Cracking Using John The Ripper	CO5
5	Implementation of Wifi Hacking Using Reaver	CO5
6	Implementation of NMAP Tool	CO5
7	Implementation of Man in the Middle Attack(Ettercap Tool)	CO5
8	Implementation of Mobile Security Using APK Tool.	CO5
9	analyze of Web Application Security	CO5
10	Implementation of SQL Injection Using SQLMap	CO5
11	Implementation of Cross Site Scripting Attack.	CO5
12	Exploiting Windows Machine using Metasploit	CO5
13	Implementation of Social Engineering Using Maltego	CO5
14	Analyze Vulnerability Analysis Using Wireshark	CO5
15	Implementation of Web Application Security (Paros)	CO5
16	Analyze Processing Crime and Incident Scenes	CO5
17	Working with file systems	CO5
18	Virtual Machine Forensics, Live Acquisitions & Network Forensics	CO5
19	Implementation of Various Attacks on RSA	CO5
20	Implementation of various Attacks on ECC	CO5

Skilling Session wise Teaching – Learning Plan

SESSION NUMBER : 1

Session Outcome: 1 To install Kali Linux

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Experimentation on Kali Linux Installation	4	LTC	--- NOT APPLICABLE ---
30	Result Documentation and Submission	4	LTC	--- NOT APPLICABLE ---
30	Viva	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 2

Session Outcome: 1 To analyzePacket Capturing Using Airodump-ng.

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Experimentation on Packet Capturing	4	LTC	--- NOT APPLICABLE ---
30	Result Documentation and Submission	4	LTC	--- NOT APPLICABLE ---
10	Viva	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 3

Session Outcome: 1 To implement social engineering attacks using Ghost Phisher.

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Experimentation on Social Engineering Attacks	3	LTC	--- NOT APPLICABLE ---
30	Result Documentation and Submission	3	LTC	--- NOT APPLICABLE ---

30	Viva	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 4

Session Outcome: 5 To analyzepassword cracking using John the Ripper tool.

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Experimentation on Password cracking	3	LTC	--- NOT APPLICABLE ---
30	Result Documentation and Submission	3	LTC	--- NOT APPLICABLE ---
30	Viva	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 5

Session Outcome: 1 To analyzet Wi-Fi hacking using Reaver.

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Experimentation on Wi-Fi Hacking.	3	LTC	--- NOT APPLICABLE ---
30	Result Documentation and Submission	3	LTC	--- NOT APPLICABLE ---
30	Viva	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 6

Session Outcome: 1 Analyze NMAP Scanning

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE ---

30	Experimentation on NMAP.	3	LTC	--- NOT APPLICABLE ---
30	Result Documentation and Submission	3	LTC	--- NOT APPLICABLE ---
30	Viva	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 7

Session Outcome: 1 To implement Man-in-the Middle attack using Ettercap.

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Experimentation on Ettercap.	3	LTC	--- NOT APPLICABLE ---
30	Result Documentation and Submission	4	LTC	--- NOT APPLICABLE ---
30	Viva	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 8

Session Outcome: 1 To implement mobile security using Apk tool.

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Experimentation on Mobile security	3	LTC	--- NOT APPLICABLE ---
30	Result Documentation and Submission	4	LTC	--- NOT APPLICABLE ---
30	Viva	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 9

Session Outcome: 1 To analyzeWeb Application Security.

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Experimentation on Web Application Security.	4	LTC	--- NOT APPLICABLE ---
30	Result Documentation and Submission	4	LTC	--- NOT APPLICABLE ---
30	Viva	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 10

Session Outcome: 1 To implement SQL Injection Using SQLMap.

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Experimentation on SQL Injection.	3	LTC	--- NOT APPLICABLE ---
30	Result Documentation and Submission	4	LTC	--- NOT APPLICABLE ---
30	Viva	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 11

Session Outcome: 1 To implement Cross site scripting attack.

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Experimentation on cross site scripting.	4	LTC	--- NOT APPLICABLE ---
30	Result Documentation and Submission	3	LTC	--- NOT APPLICABLE ---
30	Viva	1	Talk	--- NOT APPLICABLE

SESSION NUMBER : 12

Session Outcome: 1 To ianalyze Windows Metasploit.

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Experimentation on Windows Metasploit.	3	LTC	--- NOT APPLICABLE ---
30	Result Documentation and Submission	4	LTC	--- NOT APPLICABLE ---
30	Viva	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 13

Session Outcome: 1 Apply Maltego Tool to do Social Engineering

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Implementation of Social Engineering Using Maltego	3	LTC	--- NOT APPLICABLE ---
30	Analysis of Results & Documentation	4	LTC	--- NOT APPLICABLE ---
30	Viva Voice	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 14

Session Outcome: 1 Analyze Vulnerabilities Using Wireshark

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Analyze Vulnerability Analysis Using Wireshark	3	LTC	--- NOT APPLICABLE ---

30	Analysis of Results & Documentation	4	LTC	--- NOT APPLICABLE ---
30	Viva Voice	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 15

Session Outcome: 1 Apply Web Application Security using Paros

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Implementation of Web Application Security (Paros)	3	LTC	--- NOT APPLICABLE ---
30	Analysis of Results & Documentation	4	LTC	--- NOT APPLICABLE ---
30	Viva Voice	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 16

Session Outcome: 1 To Analyze Incident Scenes

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
20	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Analyze Processing Crime and Incident Scenes	3	LTC	--- NOT APPLICABLE ---
30	Analysis of Results & Documentation	4	LTC	--- NOT APPLICABLE ---
30	Viva Voice	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 17

Session Outcome: 1 Demonstrate Working with file systems

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods

10	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Working with file systems	3	LTC	--- NOT APPLICABLE ---
30	Analysis of Results & Documentation	4	LTC	--- NOT APPLICABLE ---
30	Viva Voice	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 18

Session Outcome: 1 Analyze Virtual Machine Forensics, Live Acquisitions & Network Forensics

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Analyze Virtual Machine Forensics, Live Acquisitions & Network Forensics	4	LTC	--- NOT APPLICABLE ---
30	Analysis of Results & Documentation	4	LTC	--- NOT APPLICABLE ---
30	Viva Voice	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 19

Session Outcome: 1 Implementation of Various Attacks on RSA

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Implementation of Various Attacks on RSA	3	LTC	--- NOT APPLICABLE ---
30	Analysis of Results & Documentation	3	LTC	--- NOT APPLICABLE ---
30	Viva Voice	1	Talk	--- NOT APPLICABLE ---

SESSION NUMBER : 20

Session Outcome: 1 Demonstrate various Attacks on ECC

Time(min)	Topic	BTL	Teaching-Learning Methods	Active Learning Methods
10	Attendance	1	Talk	--- NOT APPLICABLE ---
30	Implementation of various Attacks on ECC	3	LTC	--- NOT APPLICABLE ---
30	Analysis of Results & Documentation	4	LTC	--- NOT APPLICABLE ---
30	Viva Voice	1	Talk	--- NOT APPLICABLE ---

WEEKLY HOMEWORK ASSIGNMENTS/ PROBLEM SETS/OPEN ENDEDED PROBLEM-SOLVING EXERCISES etc:

Week	Assignment Type	Assignment No	Topic	Details	co

COURSE TIME TABLE:

	Hour	1	2	3	4	5	6	7	8	9
Day	Component									
Mon	Theory	--	--	--	--	--	--	--	--	--
	Tutorial	--	--	--	--	--	--	--	--	--
	Lab	--	--	--	--	--	--	--	--	--
	Skilling	--	--	--	--	--	--	--	--	--
Tue	Theory	--	--	--	--	--	--	--	--	--
	Tutorial	--	--	--	--	--	--	--	--	--
	Lab	--	--	--	--	--	--	--	--	--
	Skilling	--	--	--	--	--	--	--	--	--
Wed	Theory	--	--	--	--	--	--	--	--	--
	Tutorial	--	--	--	--	--	--	--	--	--
	Lab	--	--	--	--	--	--	--	--	--

	Skilling	--	--	--	--	--	--	--	--	--
Thu	Theory	--	--	--	--	--	--	--	--	--
	Tutorial	--	--	--	--	--	--	--	--	--
	Lab	--	--	--	--	--	--	--	--	--
	Skilling	--	--	--	--	--	--	--	--	--
Fri	Theory	---	---	---	---	V-S52	V-S52	---	---	---
	Tutorial	---	---	---	---	--	--	---	---	---
	Lab	---	---	---	---	V-S51,V-S51,V-S51	V-S51,V-S51,V-S51	---	---	---
	Skilling	---	---	---	---	V-S53,V-S53,V-S54,V-S54	V-S53,V-S53,V-S54,V-S54	---	---	---
Sat	Theory	V-S53	V-S53	V-S54	V-S54	---	---	---	---	---
	Tutorial	--	--	--	--	---	---	---	---	---
	Lab	V-S51,V-S51,V-S51,V-S54,V-S54,V-S54	V-S51,V-S51,V-S51,V-S54,V-S54,V-S54	V-S52,V-S52,V-S52,V-S53,V-S53,V-S53	V-S52,V-S52,V-S52,V-S53,V-S53,V-S53	---	---	---	---	---
	Skilling	V-S52,V-S52	V-S52,V-S52	V-S51,V-S51	V-S51,V-S51	---	---	---	---	---
Sun	Theory	--	--	--	--	--	--	--	--	--
	Tutorial	--	--	--	--	--	--	--	--	--
	Lab	--	--	--	--	--	--	--	--	--
	Skilling	--	--	--	--	--	--	--	--	--

REMEDIAL CLASSES:

Supplement course handout, which may perhaps include special lectures and discussions that would be planned, and schedule notified according

SELF-LEARNING:

Assignments to promote self-learning, survey of contents from multiple sources.

S.no	Topics	CO	ALM	References/MOOCS

DELIVERY DETAILS OF CONTENT BEYOND SYLLABUS:

Content beyond syllabus covered (if any) should be delivered to all students that would be planned, and schedule notified accordingly.

S.no	Advanced Topics, Additional Reading, Research papers and any	CO	ALM	References/MOOCS

EVALUATION PLAN:

Evaluation Type	Evaluation Component	Weightage/Marks		Assessment Dates	Duration (Hours)	CO1	CO2	CO3	CO4	CO5
End Semester Summative Evaluation Total= 40 %	Skill Sem-End Exam	Weightage	10		90					10
		Max Marks	50							50
	End Semester Exam	Weightage	20		90	5	5	5	5	
		Max Marks	100			25	25	25	25	
	Lab End Semester Exam	Weightage	10		90					10
		Max Marks	50							50
In Semester Formative Evaluation Total= 24 %	Skilling Continuous Evaluation	Weightage	6		90					6
		Max Marks	50							50
	ALM	Weightage	6		90	1.5	1.5	1.5	1.5	
		Max Marks	40			10	10	10	10	
	Continuous Evaluation - Lab Exercise	Weightage	6		90					6
		Max Marks	50							50
	MOOCs Review	Weightage	6		90	1.5	1.5	1.5	1.5	
		Max Marks	40			10	10	10	10	
In Semester Summative Evaluation Total= 36 %	Semester in Exam-I	Weightage	10		90	5	5			
		Max Marks	50			25	25			
	Semester in Exam-II	Weightage	10		90			5	5	
		Max Marks	50					25	25	
	Lab In Semester Exam	Weightage	5		90					5
		Max Marks	50							50
	Leaderboard ranking for Global Challenges	Weightage	6		90					6
		Max Marks	50							50
	Skill In-Sem Exam	Weightage	5		90					5
		Max Marks	50							50

ATTENDANCE POLICY:

Every student is expected to be responsible for regularity of his/her attendance in class rooms and laboratories, to appear in scheduled tests and examinations and fulfill all other tasks assigned to him/her in

every course
In every course, student has to maintain a minimum of 85% attendance to be eligible for appearing in Semester end examination of the course, for cases of medical issues and other unavoidable circumstances the students will be condoned if their attendance is between 75% to 85% in every course, subjected to submission of medical certificates, medical case file and other needful documental proof to the concerned departments

DETENTION POLICY :

In any course, a student has to maintain a minimum of 85% attendance and In-Semester Examinations to be eligible for appearing to the Semester End Examination, failing to fulfill these conditions will deem such student to have been detained in that course.

PLAGIARISM POLICY :

Supplement course handout, which may perhaps include special lectures and discussions

COURSE TEAM MEMBERS, CHAMBER CONSULTATION HOURS AND CHAMBER VENUE DETAILS:

Supplement course handout, which may perhaps include special lectures and discussions

Name of Faculty	Delivery Component of Faculty	Sections of Faculty	Chamber Consultation Day (s)	Chamber Consultation Timings for each day	Chamber Consultation Room No:	Signature of Course faculty:
Arumugham Roshini	P	53-B	-	-	-	-
Chandol Mohan Kumar	S	53-B	-	-	-	-
Motilal Singh Khoirom	L	51-MA	-	-	-	-
Motilal Singh Khoirom	P	51-A	-	-	-	-
Motilal Singh Khoirom	S	51-A	-	-	-	-
Jalaluddin Khan	P	51-B	-	-	-	-
Jalaluddin Khan	S	51-B	-	-	-	-
Jagjit Dhatterwal	S	52-B	-	-	-	-
Arpit Jain	S	53-B	-	-	-	-
Jagadish Gurrala	L	53-MA	-	-	-	-
Jagadish Gurrala	P	53-A	-	-	-	-
Jagadish Gurrala	S	53-A	-	-	-	-
Ravi Rastogi	L	54-MA	-	-	-	-
Ravi Rastogi	P	54-A	-	-	-	-
Ravi Rastogi	S	54-A	-	-	-	-

Khalim Meerja	P	51-B	-	-	-	-
Sameer Bhat	S	52-B	-	-	-	-
DESETTI TULASI	P	53-C	-	-	-	-
SOLLETI PHANI KUMAR	L	52-MA	-	-	-	-
SOLLETI PHANI KUMAR	P	52-A	-	-	-	-
SOLLETI PHANI KUMAR	S	52-A	-	-	-	-
DASARI SAILAJA	P	54-C	-	-	-	-
DASARI SAILAJA	S	51-B	-	-	-	-
Tejo Gudipalli	P	52-B	-	-	-	-
BOYAPATI RANI	P	54-B	-	-	-	-
BOYAPATI RANI	S	54-B	-	-	-	-
DASARI KUMAR	P	52-B	-	-	-	-
Bhabendu Mohanta	P	51-C,52-C	-	-	-	-

GENERAL INSTRUCTIONS

Students should come prepared for classes and carry the text book(s) or material(s) as prescribed by the Course Faculty to the class.

NOTICES

Most of the notices are available on the LMS platform.

All notices will be communicated through the institution email.

All notices concerning the course will be displayed on the respective Notice Boards.

Signature of COURSE COORDINATOR

(Ruth Ramya Kalangi)

Signature of Department Prof. Incharge Academics & Vetting Team Member

Department Of CSE-Honors

HEAD OF DEPARTMENT:

Approval from: DEAN-ACADEMICS
(Sign with Office Seal) [object HTMLDivElement]