MANIPAL SCHOOL OF INFORMATION SCIENCES
MANIPAL
(A constituent unit of MAHE, Manipal)

Master of Engineering - ME (Cyber Security)

Course File

Course Name	:	Cryptology
Course Code	:	CYS 5101
Academic Year	:	2024 - 25
Semester	:	I
Name of the Course Coordinator	:	Mrs. Keerthana B
Name of the Program Coordinator	:	Mrs. Keerthana B

Signature of Program Coordinator **with Date**	**Signature of Course Coordinator** **with Date**

MANIPAL SCHOOL OF INFORMATION SCIENCES
MANIPAL
(A constituent unit of MAHE, Manipal)

Table of Contents

Program Education Objectives (PEOs)

The overall objectives of the Learning Outcomes-based Curriculum Framework (LOCF) for **ME (Cyber Security)**, program are as follows.

PEO No.	Education Objective
PEO 1	To prepare students with the technical knowledge and skills needed to protect and defend computer systems, mobile devices, and networks.
PEO 2	To develop students' skills who can plan, implement, and monitor cyber security mechanisms to help ensure the protection of information technology assets.
PEO 3	To develop students who can identify, analyse and remediate IT security breaches within the limits of cyber laws and ethical practices.
PEO 4	Possess analytical, communicative and leadership skills, and demonstrate the ability to work in multidisciplinary and multi-cultural environments.
PEO 5	Be Self-motivated and remain continuously employable by engaging in lifelong learning.

Program Outcomes (POs)

By the end of the postgraduate program in **ME (Cyber Security)**, graduates will be able to:

PO1	Independently carry out research /investigation and development work to solve practical problems.
PO2	Write and present a substantial technical report/document.
PO3	Demonstrate a degree of mastery over the area as per the specialization of the program. The mastery should be at a level higher than the requirements in the appropriate bachelor program.
PO4	Identify, Analyze and evaluate the cybersecurity needs of an organization.
PO5	Develop knowledge in Cybersecurity to Monitor, Prevent, Predict and Detect and countermeasure cyberattacks using tools and techniques using appropriate Security tools.

1. Course Plan

1.1 Primary Information

Course Name	**:**	Cyber Security [CYS 5101]
L-T-P-C	**:**	3-0-0-3
Contact Hours	**:**	36 Hours
Pre-requisite	**:**	Basic of foundation in computer science, programming, networking, modular arithmetic
Core/ PE/OE	**:**	Core

1.2 Course Outcomes (COs), Program outcomes (POs) and Bloom's Taxonomy Mapping

CO	At the end of this course, the student should be able to:	No. of Contact Hours	Program Outcomes (PO's)	BL
CO1	**Apply** the CIA triad to assess the security of information systems and data.	4	PO3	3
CO2	**Evaluate** the strengths and weaknesses of conventional encryption algorithms.	20	PO4	4
CO3	**Apply** the techniques to analyze and break different type of ciphers.	12	PO4	5

1.3 Assessment Plan

Components	Internal Test 1	Flexible Assessments (2 – 3 in number)	End semester/ Makeup examination
Duration	90 minutes	To be decided by the faculty.	180 minutes
Weightage	0.3	0.2	0.5
Typology of questions	Applying; Analyzing.	Applying; Implementing, Evaluating.	Applying; Analyzing; Evaluating.
Pattern	Answer all 5 questions of 10 marks each. Each question may have 2 to 3 parts of 3/4/5/6/7 marks.	**Assignment:** Solving problems by applying and implementing encryption and decryption using ciphers.	Answer all 10 full questions of 10 marks each. Each question may have 2 to 3 parts of 3/4/5/6/7 marks.
Schedule	As per academic calendar.	**Assignment submission:** November 2024	As per academic calendar.
Topics covered	Introduction – Components of Cryptosystem Types of Attacks Cipher - Cryptography.	Quantum computing Steganography	Comprehensive examination covering the full syllabus. Students are expected to answer all questions.

1.4 Lesson Plan

L. No.	TOPICS	Course Outcome Addressed
L0	Course delivery plan, Course assessment plan, Course outcomes, Program outcomes, CO-PO mapping, reference books	---
L1	Need for Security, Security Models, Principles of Security	CO1
L2	Types of Attacks, Preventive Measure & Remedial Measure	CO1
L3	Components of Cryptosystem, Characteristics of Cryptographic Systems	CO1
L4	Substitution - Ceaser Cipher Affine Cipher	CO1
L5	Breaking substitution cipher	CO1
L6	Transposition - Rail fence, Transposition cipher	CO1
L7	Modular arithmetic	CO1
L8	Kerckhoffs Principle - Symmetric cryptography,	CO2
L9	Stream and Block cipher,	CO2
L10	Double Transposition Cipher	CO2
L11	Product cipher	CO2
L12	Breaking Transposition	CO2

L13	Classification of Cryptanalysis	CO2
L14	Kasiski Test	CO2
L15	Block Vs Stream Cipher	CO3
L16	RC4	CO3
L17	Breaking RC4	CO3
L18	LFSR	CO3
L19	DES	CO3
L20	DES Breaking	CO3
IT1	Internal test 1	CO1 CO2 & CO3
L21	AES	CO3
L22	Modes of Operation	CO4
L23	Kanpsack	CO4
L24	RSA	CO4
L25	Breaking RSA	CO4
L26	DH ECC	CO4
L27	PKI	CO4
L28	Hashing	CO4
L29	Attacks on Hashing	CO4
L30	Authentication	CO4
L31	MAC	CO5

L32	Digital signature	CO5
L33	kerberos	CO5
L34	Zkp	CO5
L35	Sieve Algorithm	CO5
L36	Security Validation	CO5

1.5 References

1. Cryptography and Network Security, William Stallings, Pearson Education, 6th Edition, 2013.
2. Cryptography and Network Security, AtulKahate, McGraw Hill Education India (Pvt. Ltd), 2nd edition, 2009.
3. Network Security: Private Communication in a Public World, Charlie Kaufman Radia Pertman, Mike Speciner. Prentice Hall, 2nd Edition 2002
4. Security in Computing, Charles Pfleeger, Prentice Hall, 4th Edition, 2006.
5. Algorithmic Cryptanalysis, Antoine Joux, Taylor and Francis Group, CRC Press, 2009.
6. Post Quantum Cryptography, Daniel J. Bernstein, Johannes Buchmann, Erik Dahmen, Sprinegr Publication, 2009.
7. https://nptel.ac.in/courses/106105031 (last accessed on 01.03.2022)

1.6 Other Resources (Online, Text, Multimedia, etc.)

1. Web Resources: Blog, Online tools and cloud resources.
2. Journal Articles.

1.7 Course Timetable

1st Semester Cyber Security				Room: LG1 LH 12				
	9-10	10-11	11-12	12-1	1-2	2-3	3-4	4-5
MON		Crypt						
TUE								
WED		Crypt				Crypt Lab		
THU								
FRI		Crypt						
SAT								

1.8 Assessment Plan

COs		**Marks & Weightage**			
CO No.	CO Name	IT-1 (Max. 50)	Assignment (Max. 20)	End Semester (Max. 100)	CO wise Weightage
CO1	**Apply** the CIA triad to assess the security of information systems and data.	10	10	10	**0.1**
CO2	**Evaluate** the strengths and weaknesses of conventional encryption algorithms.	25		20	**0.2**
CO3	**Apply** the techniques to analyze and break different type of ciphers.	15	10	20	**0.2**
	Marks (weightage)	**0.3**	**0.2**	**0.5**	**1.0**

Note:

- In-semester Assessment is considered as the Internal Assessment (IA) in this course for 50 marks, which includes the performances in class participation, assignment work, class tests, mid-term tests, quizzes etc.
- End-semester examination (ESE) for this course is conducted for a maximum of 100 and the same will be scaled down to 50.
- End-semester marks for a maximum of 50 and IA marks for a maximum of 50 are added for a maximum of 100 marks to decide upon the grade in this course.

Weightage for CO1 = (IT1 marks for CO1 / 2.5 + IT2 marks for CO1 / 2.5 + Assignment marks for CO1 + ESE marks for CO1 / 2)/100
= (25/2.5 + 0 + 0 + 20/ 2)/100 = 0.2

1.9 Assessment Details

The assessment tools to be used for the Current Academic Year (CAY) are as follows:

SI. No.	Tools	Weightage	Frequency	Details of Measurement (Weightage/Rubrics/Duration, etc.)
1	Internal Test	0.3	2	• Performance is measured using internal test attainment level. • Reference: question paper and answer scheme. • Each internal test is assessed for a maximum of 50 marks and scaled down to 40 marks.
2	Assignments	0.2	5	• Performance is measured using assignments/quiz attainment level. • Assignments/quiz are evaluated for a maximum of 10 marks.
3	End Semester	0.5	1	• Performance is measured using ESE attainment level. • Reference: question paper and answer scheme. • ESE is assessed for a maximum of 100 marks and scaled down to 50 marks.

1.10 Course Articulation Matrix

CO	PO1	PO2	PO3	PO4	PO5
CO1			**Y**		
CO2				**Y**	
CO3				**Y**	
Average Articulation Level			Y	Y	Y