



MANIPAL SCHOOL OF INFORMATION SCIENCES



MANIPAL

(A constituent unit of MAHE, Manipal)

Master of Engineering - ME (Cyber Security)

Course File

Course Name	:	Cryptology Lab
Course Code	:	CYS 5151
Academic Year	:	2023 - 24
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

1. Course Plan	5
1.1 Primary Information	5
1.2 Course Outcomes (COs)	6
1.3 Assessment Plan	6
1.4 Lesson Plan	8
1.5 References	9
1.6 Other Resources (Online, Text, Multimedia, etc.)	10
1.7 Course Timetable	11
1.8 Assessment Plan	12
1.9 Assessment Details	13
1.10 Course Articulation Matrix	13



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.



MANIPAL SCHOOL OF INFORMATION SCIENCES

MANIPAL

(A constituent unit of MAHE, Manipal)

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.



MANIPAL SCHOOL OF INFORMATION SCIENCES

MANIPAL

(A constituent unit of MAHE, Manipal)

1. Course Plan

1.1 Primary Information

Course Name	:	Cryptology Lab [CYS 5151]
L-T-P-C	:	0-0-3-1
Contact Hours	:	36 Hours
Pre-requisite	:	Programming with Python
Core/ PE/OE	:	Core



MANIPAL SCHOOL OF INFORMATION SCIENCES

MANIPAL

(A constituent unit of MAHE, Manipal)

1.2 Course Outcomes (COs)

CO	At the end of this course, the student should be able to:	No. of Contact Hours	Program Outcomes (PO's)	BL
CO1	Identify the Threat, vulnerabilities and attacks in the network.	1	PO3	3
CO2	Implement the encryption and decryption concepts.	6	PO3	3
CO3	Implement the cryptanalysis using mono alphabetic and Polyalphabetic cipher	5	PO4	4

1.3 Assessment Plan

Components	Lab Test	Flexible Assessments (2 – 3 in number)	End semester/ Makeup examination
------------	----------	---	-------------------------------------



MANIPAL SCHOOL OF INFORMATION SCIENCES

MANIPAL

(A constituent unit of MAHE, Manipal)

Duration	90 minutes	To be decided by the faculty.	180 minutes
Weightage	0.3	0.2	0.5
Typology of questions	Applying; Analyzing.	Applying; Analyzing. Evaluating.	Applying; Analyzing; Evaluating.
Pattern	Answer all the questions. Maximum marks 30.	Assignment: Use different library functions to apply, analyze and evaluate the performances of the cryptographic algorithms: AES algorithm, RSA algorithm, DES algorithm, DSA algorithm, RC4 algorithm, Diffie-Hellman key exchange method. Maximum 20 marks. [To be decided by the faculty members. May be Assignments, Problem solving, etc.]	Answer all the questions. Maximum marks 50.
Schedule	As per academic calendar.	Assignment submission: November 2023	As per academic calendar.



MANIPAL SCHOOL OF INFORMATION SCIENCES

MANIPAL

(A constituent unit of MAHE, Manipal)

Topics covered	Fernet, hashlib, symmetric and asymmetric algorithms.		Comprehensive examination covering the full syllabus.
-----------------------	---	--	---

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	---
Lab1	Basic Python	
Lab2	Python File handling	
Lab3	Performing Arithmetic operating – prime numbers, calculating inverse	CO2



MANIPAL SCHOOL OF INFORMATION SCIENCES

MANIPAL

(A constituent unit of MAHE, Manipal)

Lab4	Encrypt and decrypt Caesar cipher	CO2
Lab5	Break the Caesar Cipher	CO3
Lab6	Implement RSA	CO3
IT1	Internal lab test	CO1, CO2, CO3
Lab7	Implement RC4	CO4
Lab8	Explore openssl tools	CO4
Lab9	Explore hashing algorithms	CO4
Lab10	Implement DH	CO5
Lab11	Doing Kasiksi Test	CO5
Lab12	Simulate DES	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 Perlman, Mike Speciner, Prentice Hall, 2nd edition, 2002.
4. Security in computing, Charles Pfleeger, Shari Lawrence 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, Springer Publication,2009.
7. <https://nptel.ac.in/courses/106105031> (last accessed on 01.03.2022)



MANIPAL SCHOOL OF INFORMATION SCIENCES

MANIPAL

(A constituent unit of MAHE, Manipal)

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

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



MANIPAL SCHOOL OF INFORMATION SCIENCES

MANIPAL

(A constituent unit of MAHE, Manipal)

1.7 Course Timetable

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



MANIPAL SCHOOL OF INFORMATION SCIENCES

MANIPAL

(A constituent unit of MAHE, Manipal)

1.8 Assessment Plan

COs		Marks & weightage			
CO No.	CO Name	Lab Test (Max. 30)	Assignment (Max. 20)	End Semester (Max. 50)	CO wise Weightage
CO1	Identify the Threat, vulnerabilities and attacks in the network.	5	5	-	0
CO2	Implement the encryption and decryption concepts.	5	10	25	0.25
CO3	Implement the cryptanalysis using mono alphabetic and Polyalphabetic cipher	20	5	25	0.25
	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 lab participation, assignment work, lab work, lab tests, quizzes etc.
- End-semester examination (ESE) for this course is conducted for a maximum of 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.



MANIPAL SCHOOL OF INFORMATION SCIENCES

MANIPAL

(A constituent unit of MAHE, Manipal)

$$\begin{aligned}\text{Weightage for CO1} &= (\text{Lab Test marks for CO1} + \text{Assignment marks for CO1} + \text{ESE marks for CO1}) / 100 \\ &= (5 + 2 + 5) / 100 = 0.12\end{aligned}$$

1.9 Assessment Details

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

Sl. No.	Tools	Weightage	Frequency	Details of Measurement (Weightage/Rubrics/Duration, etc.)
1	Lab Test	0.3	1	<ul style="list-style-type: none">• Performance is measured using lab internal test attainment level.• Reference: question paper and answer scheme.• Lab internal test is assessed for a maximum of 30 marks.
2	Assignments	0.2	1	<ul style="list-style-type: none">• Performance is measured using assignments attainment level.• Assignment is evaluated for a maximum of 20 marks.
3	ESE	0.5	1	<ul style="list-style-type: none">• Performance is measured using ESE attainment level.• Reference: question paper and answer scheme.• ESE is assessed for a maximum of 50 marks.

1.10 Course Articulation Matrix



MANIPAL SCHOOL OF INFORMATION SCIENCES

MANIPAL

(A constituent unit of MAHE, Manipal)

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