MANIPAL INSTITUTE OF TECHNOLOGY
MANIPAL
(A constituent unit of MAHE, Manipal)

COURSE PLAN

Department :	**Information and Communication Technology**			
Course Name & code :	**Information Security**		**ICT 3121**	
Semester & branch :	**V**	**Information Technology / Computer and Communication Engineering**		
Name of the faculty :	**Dr. Raghavendra Ganiga**			
No of contact hours/week:	**L**	**T**	**P**	**C**
	3	**0**	**0**	**3**

COURSE OUTCOMES (COS) to PO,PSO,BL Mapping

At the end of this course, the student should be able to:		**No. of Contact Hours**	**Marks**	**Program Outcomes (POs)**	**PSO**	**BL (Recommended)**
CO1	Articulate the security attacks and various services for data security.	2	6	1		3
CO2	Analyze various symmetric data encryption techniques in cryptography.	8	24	1,2,3	1	4
CO3	Implement solution for security issues problem using asymmetric key encryption algorithm.	8	24	1,2,3	1	4
CO4	Choose appropriate integrity and authentication techniques for security challenges	9	26	1,2,3	1	4
CO5	Apply the knowledge of security concepts for providing solutions to computer systems and networks	9	20	1,2,3	1	3
	Total	**36**	**100**			

Course Articulation Matrix

CO	Engineering knowledge	Problem analysis	Design/development of solutions	Conduct investigations of complex problems	Engineering tool usage	The Engineer and the world	Ethics	Individual and team work	Communication	Project management and finance	Life-long learning					
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3	PSO4
CO1	2	2	2	2									2			
CO2	2	2	2	2									2			
CO3	2	2	2	2									2			
CO4	2	2	2	2									2			
CO5	2	2	2	2									2			
Average Articulation Level	2	2	2	2									2			

ICT Tools used in delivery and assessment

Sl. No	Name of the ICT tool used	Details of how it is used
1	LMS	To upload materials and for conducting assignments.
2	MSTeam	To communicate with students.

Typical tools including LMS, Smart Boards, MS Teams, etc

Course Outcomes (Cos) to PO, PSO, BL Mapping

At the end of this course, the student should be able to:		No. of Contact Hours	Marks	Program Outcomes(POs)	Learning Outcomes (LOs)	BL (Recommended)
CLO1	Articulate the security attacks and various services for data security.	2	6	1	1	3
CLO2	Analyze various symmetric data encryption techniques in cryptography	8	24	1,2,3	1,2,3	4
CLO3	Implement solution for security issues problem using asymmetric key encryption algorithm.	8	24	1,2,3	2,3	4
CLO4	Choose appropriate integrity and authentication techniques for security challenges	9	26	1,2,3	2,3	4
CLO5	Apply the knowledge of security concepts for providing solutions to computer systems and networks	**9**	**20**	1,2,3	3	3
	Total	**36**	**100**			

# Applicable to IET Accredited Courses (modules) Only

Delivery and Assessment Plan of LOs

<u>Learning Outcome (LO) mapped to the course</u>		**Delivery and assessment Plan**
LO	**LO statement**	
LO1	Apply knowledge of mathematics, statistics, natural science and engineering principles to the solution of complex problems. Some of the knowledge will be at the forefront of the particular subject of study.	
LO2	Analyse complex problems to reach substantiated conclusions using first principles of mathematics, statistics, natural science and engineering principles.	
LO3	Select and apply appropriate computational and analytical techniques to model complex problems, recognising the limitations of the techniques	

	employed	
LO6	Apply an integrated or systems approach to the solution of complex problems	

# Applicable to IET Accredited Programs Only

Assessment Plan (As communicated from o/o AD-A, in every odd semester)

IN – SEMESTER ASSESSMENTS

S. No.	Assessment Mode		Assessment Method	Time Duration	Marks	Weightage	Typology of Questions (Recommended)	Schedule	**Topics Covered
1	**MISAC**	**1**	**Surprise Assignment**	**20 Mins**	**5**	1 Question × 5M = 5 marks (Minimum 5 questions to be given)	Bloom's taxonomy (BT) level of the question should be L3 and above.	Aug 12th to 20th 2024	L1-L7
		2	**In-semester Exam**	**120 Mins**	**30**	**Objective:** 5M 10 MCQs × ½ = 5 marks **Descriptive:** 25 M (2 Questions of 4 Marks + 5 Questions of 3 Marks+1 Question of 2 Marks)	Bloom's taxonomy (B) level of the question should be L3 and above.	Sep 23rd -28th, 2024	L1-L19, SDL1-4
		3	**Quiz**	**15 Mins**	**5**	10 MCQs × ½ = 5	Bloom's taxonomy (BT) level of the question should be L3 and above.	Sep-2nd -9th 2024	L20-L22
2	**FISAC**	**1**	**Group Assignment**	*******	**10**	*******	Bloom's taxonomy (BT) level of the question should	Oct-21th-26th-2024	Quiz based on the concepts from L6-L36 and SDL 4-7

							be L3 and above.		
END – SEMESTER ASSESSMENT									
1	**Regular/Make–Up Exam**			180 Mins	**50**	Answer all 5 full questions of 10 marks each. Each question can have 3 parts of 2/3/4/5/6 marks.	Bloom's taxonomy (BT) level of the question should be L3 and above.		L1-L36, SDL1-SDL6

***** Individual faculty will be entering the topics***

****** Individual faculty must identify the assessment method from table 3 and fill in the details.***

***NOTE:* Information provided in the table is as per the In-semester assessment plan and schedule of V and VII semester B. Tech provided from Academic Section.**

LESSON PLAN

L No	TOPICS	Course Outcome Addressed
0	Introduction to the course	
1	Introduction, Computer Security Concepts, Security Goals, Security Attacks	CO1
2	Security Services, Security Mechanisms, Security Techniques	CO1
3	Kerckhoff’s principle, Substitution ciphers	CO2
4	Substitution ciphers (contd)	CO2
5	Transposition ciphers,Stream & Block ciphers.	CO2
6	DES	CO2
7	DES (contd)	CO2
8	AES	CO2
9	AES (contd)	CO2
10	Use of modern block ciphers.	CO2
11	Asymmetric cryptosystems	CO3
12	Asymmetric cryptosystems (contd)	CO3
13	RSA	CO3
14	RSA (contd)	CO3
15	Rabin cryptosystem	CO3
16	Elgamal encryption system	CO3
17	Elgamal encryption system (contd)	CO3
18	Diffie Hellman Key exchange	CO3
19	Message Integrity, Random Oracle Model	CO4
20	Message Authentication	CO4
21	Hash function, SHA 512	CO4
22	Whirlpool	CO4
23	Digital Signatures schemes: RSA	CO4
24	Elgamal Scheme, Shnorr	CO4
25	ECDS, Digital Signature Standards	CO4
26	Attacks on digital signatures	CO4
27	Entity authentication- Passwords & challenge response, Zero knowledge & biometrics	CO4
28	Key management-KDC &Kerberos	CO5
29	Public key distribution: Certification Authority	CO5
30	Public Key Infrastructure	CO5
31	Transport layer Security- SSL/TLS	CO5
32	Architecture, Protocols, Message formats	CO5
33	System Security- Firewalls	CO5
34	System Security- Firewalls (contd)	CO5
35	Network Intrusion Detection and Prevention Systems	CO5
36	Network Intrusion Detection and Prevention Systems (contd)	CO5
SDL1	Cryptanalysis- Traditional and Modern Cryptography	CO3
SDL2	Elliptic curve cryptosystem (ECC) and Digital Signature ECC	CO4
SDL3	Multimedia Encryption	CO5
SDL4	Introduction to Homomorphic Encryption	CO5
SDL5	Searchable Encryption	CO4
SDL6	Digital rights management issues	CO4

Faculty Members Teaching the Course (If Multiple Sections Exist):

Faculty	Section	Faculty	Section
Dr. Nisha	IT A	Dr. Nisha	CCE A
Dr. Raghavendra Ganiga	IT B	Dr. Divya Rao	CCE B
Mr. Akshay K C	IT C	Mr. Sudhina Kumar G K	CCE C

References:

Textbooks	• William Stallings, Cryptography and Network Security: Principles and Practice ,7th edition,Pearson Publications, 2016. • Charles P. Pfleeger, Shari Lawrence Pfleeger , Jonathan Margulies, Security in Computing, 5th edition, Prentice Hall, 2015.. • Michael E. Whitman and Herbert J. Mattord, Principles of Information Security ,5th edition,Cengage Learning, 2015. • Mark Stamp, Information Security: Principles and Practice,2nd edition, John Wiley & Sons, 2011. • Behrouz A. Forouzan, Debdeep Mukhopadhyay, Cryptography and Network Security ,2nd Edition (Revised), Tata McGraw-Hill Education India, 2010. • Borko Furht, Darko Kirovski, Multimedia Encryption and Authentication Techniques and Applications ,1st edition, Taylor and Francis,2019.
Self-Directed Learning	
Research Literature/ Case Studies	• Cheon, J.H., Costache, A., Moreno, R.C., Dai, W., Gama, N., Georgieva, M., Halevi, S., Kim, M., Kim, S., Laine, K. and Polyakov, Y., 2021. Introduction to homomorphic encryption and schemes. Protecting Privacy through Homomorphic Encryption, pp.3-28. • Ren, Kui, and Cong Wang. Searchable Encryption: From Concepts to Systems. Springer, 2023. • Kulkarni, Nidhi S., Balasubramanian Raman, and Indra Gupta. "Multimedia encryption: a brief overview." Recent advances in multimedia signal processing and communications (2009): 417-449.
NPTEL/Coursera/any MOOC-based material	• Cryptography and Network Security - (Computer Science and Engineering course from IIT Kharagpur) NPTEL Lecture Videos by Dr. Debdeep Mukhopadhyay from IIT Kharagpur. Link: • https://www.nptelvideos.com/course.php?id=398

	• **Foundations of Cryptography** **By Prof. Ashish Choudhury , IIIT Bangalore Link:** **https://onlinecourses.nptel.ac.in/noc24_cs01/preview**

Submitted by:

(Signature of the faculty)

Date:

Approved by:

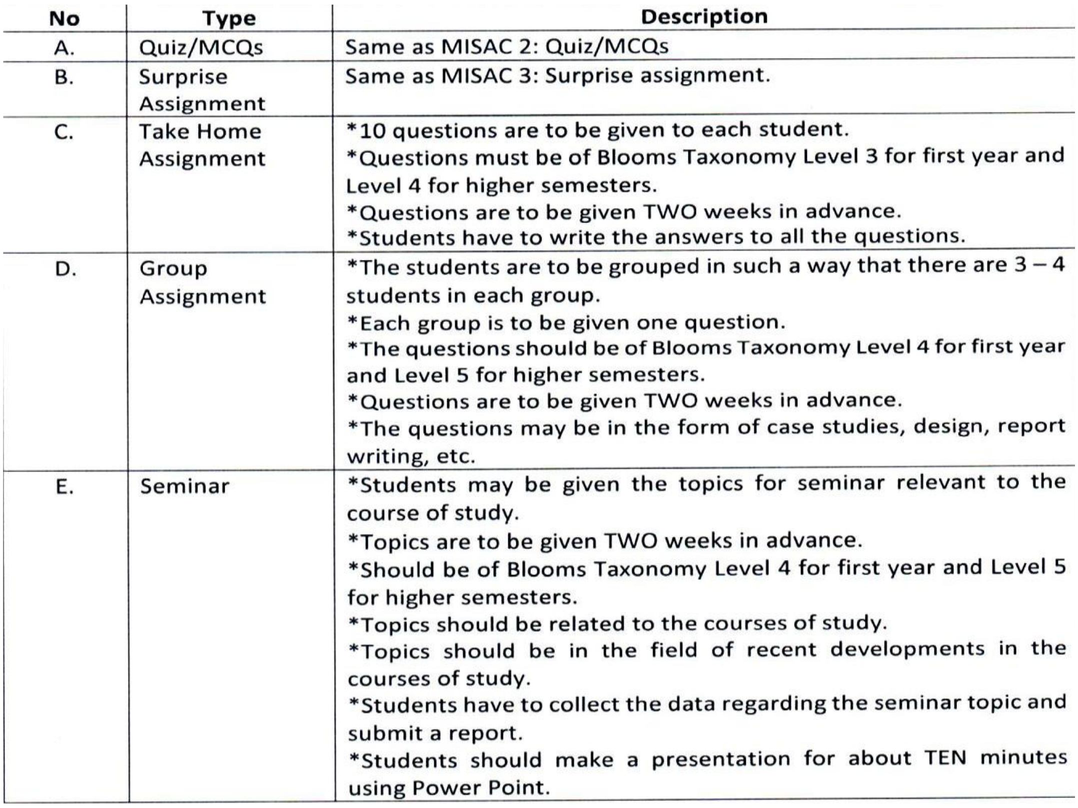
(Signature of HOD)

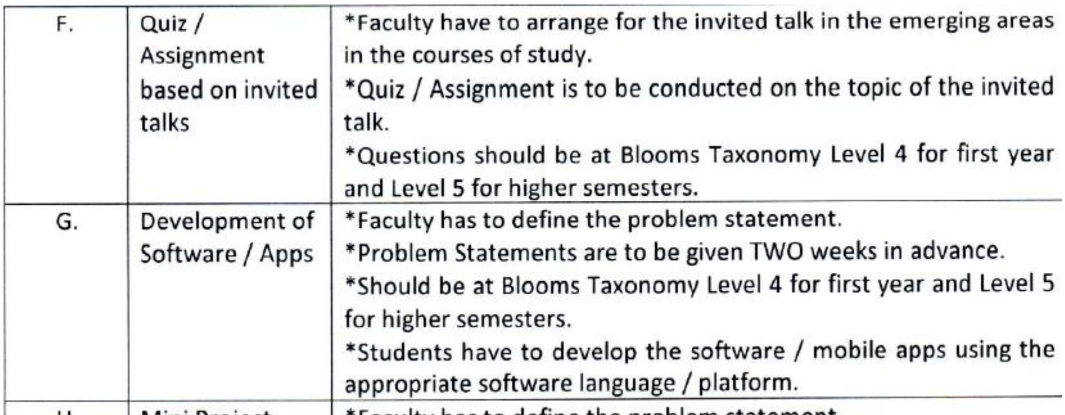
Flexible In-semester Assessment Component (FISAC):

i) The FISAC 1 may be any of the types given in Table 1. However, the two components should be of different type.

ii) The type of assessment should be informed to the students well in advance.

Table 1: Flexible In-semester Assessment Component (FISAC)





No	Type	Description
A.	Quiz/MCQs	Same as MISAC 2: Quiz/MCQs
B.	Surprise Assignment	Same as MISAC 3: Surprise assignment.
C.	Take Home Assignment	*10 questions are to be given to each student. *Questions must be of Blooms Taxonomy Level 3 for first year and Level 4 for higher semesters. *Questions are to be given TWO weeks in advance. *Students have to write the answers to all the questions.
D.	Group Assignment	*The students are to be grouped in such a way that there are 3 – 4 students in each group. *Each group is to be given one question. *The questions should be of Blooms Taxonomy Level 4 for first year and Level 5 for higher semesters. *Questions are to be given TWO weeks in advance. *The questions may be in the form of case studies, design, report writing, etc.
E.	Seminar	*Students may be given the topics for seminar relevant to the course of study. *Topics are to be given TWO weeks in advance. *Should be of Blooms Taxonomy Level 4 for first year and Level 5 for higher semesters. *Topics should be related to the courses of study. *Topics should be in the field of recent developments in the courses of study. *Students have to collect the data regarding the seminar topic and submit a report. *Students should make a presentation for about TEN minutes using Power Point.
F.	Quiz / Assignment based on invited talks	*Faculty have to arrange for the invited talk in the emerging areas in the courses of study. *Quiz / Assignment is to be conducted on the topic of the invited talk. *Questions should be at Blooms Taxonomy Level 4 for first year and Level 5 for higher semesters.
G.	Development of Software / Apps	*Faculty has to define the problem statement. *Problem Statements are to be given TWO weeks in advance. *Should be at Blooms Taxonomy Level 4 for first year and Level 5 for higher semesters. *Students have to develop the software / mobile apps using the appropriate software language / platform.
H.	Mini Project	*Faculty has to define the problem statement.