

ACADEMIC CURRICULA

POST GRADUATE DEGREE PROGRAMMES

Master of Technology

(Choice Based Flexible Credit System)

Regulations 2021

Volume – 21 Curriculum



SRM

INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

(Deemed to be University u/s 3 of UGC Act, 1956)

Kattankulathur, Chengalpattu District 603203,

Tamil Nadu, India

22 M.Tech in Cyber Security

22. (a) Department Vision Statement

Stmt - 1	<i>To Nurture as globally recognizable department in imparting the students high quality education and providing high confidence, unique knowledge and research experience in the field of networking, cyber security, forensics, information technology, cognitive computing and internet of things.</i>
----------	---

22. (b) Department Mission Statement

Stmt - 1	<i>To provide world-class IT professionals with appropriate industry and research-based curriculum.</i>
Stmt - 2	<i>To train the students, that leads to entrepreneurship and develop societal need-based industries.</i>
Stmt - 3	<i>To nourish the students as socially responsible professionals by providing them training in personality development, ethics, and leadership program.</i>

22. (c) Program Education Objectives (PEO)

PEO - 1	<i>Graduates will be able to demonstrate their knowledge and skills acquired in Computer Science and Engineering domain</i>
PEO - 2	<i>Graduates will be able to successfully pursue their research in reputed institutions</i>
PEO - 3	<i>Graduates will have the proficiency to adapt, contribute and innovate new technologies and systems in their job domains with appropriate professional skills</i>
PEO - 4	<i>Graduates will be ethically and socially responsible solution providers and entrepreneurs in Computer Science and other engineering disciplines.</i>
PEO - 5	<i>Graduates will have the ability to excel in their career producing outstanding contribution in Computer Science with cybersecurity domain.</i>

22. (d) Consistency of PEO's with Mission of the Department

	Mission Stmt. - 1	Mission Stmt. - 2	Mission Stmt. - 3
PEO - 1	3	3	-
PEO - 2	2	3	2
PEO - 3	3	2	2
PEO - 4	2	2	3
PEO - 5	3	2	2

22. (e) PO – Program Outcomes

PO - 1	<i>An ability to independently carry out research /investigation and development work to solve practical problems.</i>
PO - 2	<i>An ability to write and present a substantial technical report/document.</i>
PO - 3	<i>Students should be able to 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.</i>

22. (f) Consistency of PEO's with Program Outcomes (PO)

	Program Outcomes (PO)		
	1	2	3
PEO - 1	3	2	3
PEO - 2	3	3	2
PEO - 3	2	2	2
PEO - 4	2	2	2
PEO - 5	2	2	3

3 – High Correlation, 2 – Medium Correlation, 1 – Low Correlation

22. (g) Programme Structure: M.Tech in Cyber Security

Professional Core Courses (C)						
Course	Course	Hours/Week				
Code	Title	L	T	P	C	
21MAC504T	Number Theory	3	1	0	4	
21CSC503T	Security Service Management	3	1	0	4	
21CSC572J	Applied Malware Analysis	3	0	2	4	
21CSC546J	Understanding Cyber Attacks	3	0	2	4	
21CSC547J	Designing Security Controls, Governance and Compliance	3	0	2	4	
21IPC501J ²	Research Methodology	2	1	2	4	
21CSC601T ¹	Case Studies	3	0	0	3	
Total Credits					27	

Project Work, Internship In Industry / Higher Technical Institutions (P)						
Course	Course	Hours/Week				
Code	Title	L	T	P	C	
21CSP501L	Specialization Project (OR)	0	0	40	20	
21CSP502L	Specialization Project	0	0	30	15	
21CSP503L	Domain Internship	0	0	10	5	
Total Credits					20	

Course Delivery by online mode (³)						
Course	Course	Hours/Week				
Code	Title	L	T	P	C	
21CSE596T ³	Security Operations and Incident Management	3	0	0	3	
21CSE597T ³	Containers and Cloud DevOps	3	0	0	3	
21CSE598T ³	Big Data Analytics and Microservices	3	0	0	3	
21CSE599T ³	Security and Architecture	3	0	0	3	
21CSE626T ³	Hacker Techniques and Incident Handling	3	0	0	3	
21CSE628T ³	Cyber Law and Ethics	3	0	0	3	
21CSE629T ³	Wireless Security	3	0	0	3	
21CSE630T ³	Operating System Internals	3	0	0	3	
21CSE650T ³	Penetration Testing	3	0	0	3	
21CSE651T ³	InfoSec Leadership	3	0	0	3	
21CSE651T ³	InfoSec Leadership	3	0	0	3	

Professional Elective Courses (E) (Any 7 Courses)						
Course	Course	Hours/Week				
Code	Title	L	T	P	C	
21CSE596T ³	Security Operations and Incident Management	3	0	0	3	
21CSE597T ³	Containers and Cloud DevOps	3	0	0	3	
21CSE598T ³	Big Data Analytics and Microservices	3	0	0	3	
21CSE599T ³	Security and Architecture	3	0	0	3	
21CSE531T	Cyber Security Operations	2	1	0	3	
21CSE532T	Network Management and Protocols	2	1	0	3	
21CSE533T	Firewalls and Access Controls	2	1	0	3	
21CSE534T	Network Programming and Management	2	1	0	3	
21CSE535T	Network Intrusions and Computer Forensics	2	1	0	3	
21CSE536T	Mobile Forensics	2	1	0	3	
21CSE537T	Digital Forensics	2	1	0	3	
21CSE538T	Security Scripting and Analysis	2	1	0	3	
21CSE539T	Principles of Secure Coding Principles	2	1	0	3	
21CSE540T	Android Security and Design Internals	2	1	0	3	
21CSE626T ³	Hacker Techniques and Incident Handling	3	0	0	3	
21CSE628T ³	Cyber Law and Ethics	3	0	0	3	
21CSE629T ³	Wireless Security	3	0	0	3	
21CSE630T ³	Operating System Internals	3	0	0	3	
21CSE650T ³	Penetration Testing	3	0	0	3	
21CSE651T ³	InfoSec Leadership	3	0	0	3	
21CSE600T ¹	Journal Publication	0	0	0	3	
Total Credits					21	

Open Elective Courses (O)						
Course	Course	Hours/Week				
Code	Title	L	T	P	C	
21CSO621T	Cyber Security	3	0	0	3	
21CSO622T	Big Data Analytics	3	0	0	3	
21CSO623T	Data Sciences	3	0	0	3	
Total Credits					3	

Assessment by Open Book Examination (²)						
Course	Course	Hours/Week				
Code	Title	L	T	P	C	
21IPC501J ²	Research Methodology	2	1	2	4	

100% assessment by the Department (¹)						
Course	Course	Hours/Week				
Code	Title	L	T	P	C	
21CSC601T ¹	Case Studies	3	0	0	3	
21CSE600T ¹	Journal Publication	0	0	0	3	

All elective courses may be studied under MOOC platform

¹ 100% assessment by the Department

² Assessment by Open Book Examination

³ Course Delivery through online mode

22. (h) Implementation Plan: M.Tech in Cyber Security

Semester - I						
Code	Course Title	Hours/ Week				
		L	T	P	C	
21MAC504T	Number Theory	3	1	0	4	
21CSC503T	Security Service Management	3	1	0	4	
21CSC572J	Applied Malware Analysis	3	0	2	4	
21IPC501J ²	Research Methodology	2	1	2	4	
					3	
Total Credits					16/19	

Semester - II						
Code	Course Title	Hours/ Week				
		L	T	P	C	
21CSC546J	Understanding Cyber Attacks	3	0	2	4	
21CSC547J	Designing Security Controls, Governance and Compliance	3	0	2	4	
	Professional Elective-1				3	
					3	
					3	
Total Credits					11/17	

Semester - III						
Code	Course Title	Hours/ Week				
		L	T	P	C	
21CSC601T ¹	Case Studies	3	0	0	3	
	Professional Elective-2				3	
					3	
					3	
					3	
Total Credits					6/15	

Semester - IV						
Code	Course Title	Hours/ Week				
		L	T	P	C	
21CSP501L	Specialization Project (OR)	0	0	40	20	
21CSP502L	Specialization Project	0	0	30	15	
21CSP503L	Domain Internship	0	0	10	5	
					3	
					3	
Total Credits					20/26	

Students must register either 21CSP501L or 21CSP502L and 21CSP503L both in fourth semester

Offered and can be enrolled in both ODD & EVEN semester					
Code	Course Title	Hours/Week			C
		L	T	P	
	Professional Elective-3				3
	Professional Elective-4				3
	Professional Elective-5				3
	Professional Elective-6				3
21CSE600T ¹	Journal Publication	0	0	0	3
	Professional Elective-7				3
	Open Elective	3	0	0	3

22. (i) Program Articulation Matrix: M.Tech in Cyber Security

Course Code	Course Name	Programme Outcomes		
		1	2	3
21MAC504T	Number Theory	3	3	-
21CSC503T	Security Service Management			
21CSC572J	Applied Malware Analysis	1	2	3
21CSC546J	Understanding Cyber Attacks	2	2	3
21CSC547J	Designing Security Controls, Governance and Compliance	1.3	2	3
21CSC601T	Case Studies			
21CSE596T	Security Operations and Incident Management	1.3	2	2.6
21CSE597T	Containers and Cloud DevOps	2	2.6	3
21CSE598T	Big Data Analytics and Microservices	2	2.6	3
21CSE599T	Security and Architecture	2	2.6	3
21CSE531T	Cyber Security Operations			
21CSE532T	Network Management and Protocols			
21CSE533T	Firewalls and Access Controls			
21CSE534T	Network Programming and Management			
21CSE535T	Network Intrusions and Computer Forensics			
21CSE536T	Mobile Forensics			
21CSE537T	Digital Forensics			
21CSE538T	Security Scripting and Analysis			
21CSE539T	Principles of Secure Coding Principles			
21CSE540T	Android Security and Design Internals			
21CSE626T	Hacker Techniques and Incident Handling	2	2	3
21CSE628T	Cyber Law and Ethics	1.6	3	1.3
21CSE629T	Wireless Security	1.8	2.6	1.8
21CSE630T	Operating System Internals	1.8	2.2	1.8
21CSE650T	Penetration Testing	2	2.6	3
21CSE651T	InfoSec Leadership	2	2.6	3
21CSE600T	Journal Publication			
21IPC501J	Research Methodology	3	2.6	
	Open Elective			
21CSP501L	Specialization Project			
21CSP502L	Specialization Project			
21CSP503L	Domain Internship			
Program Average				

3 – High Correlation, 2 – Medium Correlation, 1 – Low Correlation



SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

(Deemed to be University u/s 3 of UGC Act, 1956)

Kattankulathur, Chengalpattu District 603203, Tamil Nadu, India