

M.Tech. in Computer Science & Engineering (Networking & Cyber Security)

University-Style Syllabus (2 Years / 4 Semesters)

Programmer Duration: 2 Years (4 Semesters)

Programmer Level: Postgraduate (M.Tech.)

Semester I

Subject Code	Subject	L	T	P	Credits
CNS101	Advanced Computer Networks	3	1	0	4
CNS102	Applied Cryptography and Network Security	3	1	0	4
CNS103	Advanced Operating Systems	3	0	2	4
CNS104	Research Methodology	2	0	2	3
CNS105	Cyber Security Laboratory	0	0	4	2
CNS106	Seminar-I	0	0	2	1

Total Credits: 18

Semester II

Subject Code	Subject	L	T	P	Credits
CNS201	Wireless and Mobile Networks	3	1	0	4
CNS202	Ethical Hacking and Penetration Testing	3	0	2	4
CNS203	Cloud Security	3	0	2	4

Subject Code	Subject	L	T	P	Credits
CNS204	Internet of Things Security	3	0	2	4
CNS205	Advanced Networking Laboratory	0	0	4	2
CNS206	Seminar-II	0	0	2	1

Total Credits: 19

Semester III

Subject Code	Subject	L	T	P	Credits
CNS301	Artificial Intelligence in Cyber Security	3	1	0	4
CNS302	Digital Forensics	3	0	2	4
CNS303	Block chain Security	3	0	2	4
CNS304	Elective-I	3	0	0	3
CNS305	Dissertation Phase-I	0	0	12	8

Elective-I (Choose One)

- CNS311 – Big Data Security
- CNS312 – Malware Analysis
- CNS313 – Software Defined Networking
- CNS314 – Secure Software Engineering
- CNS315 – Data Privacy and Protection

Total Credits: 23

Semester IV

Subject Code	Subject	L	T	P	Credits
--------------	---------	---	---	---	---------

Subject Code	Subject	L	T	P	Credits
CNS401	Dissertation Phase-II	0	0	24	16
CNS402	Viva Voce	0	0	2	2
CNS403	Industrial Internship	0	0	8	4

Total Credits: 22

Laboratory Courses

Code	Laboratory
CNS105	Cyber Security Lab
CNS205	Advanced Networking Lab
CNS305	Research and Dissertation Lab
CNS401	Dissertation Work

Detailed Unit-Wise Syllabus

CNS101 Advanced Computer Networks

Unit I

- Network Architecture
- TCP/IP Advanced Concepts
- IPv6

Unit II

- Routing Protocols
- MPLS
- VPN

Unit III

- QoS
- SDN
- NFV

Unit IV

- Data Center Networks
- Cloud Networking

Unit V

- Future Internet Technologies
-

CNS102 Applied Cryptography & Network Security

Unit I

- Classical Cryptography

Unit II

- AES
- DES
- RSA

Unit III

- Digital Signature
- Hash Functions

Unit IV

- PKI
- SSL/TLS

Unit V

- Block chain Cryptography
-

CNS202 Ethical Hacking

Unit I

- Reconnaissance

Unit II

- Vulnerability Assessment

Unit III

- Web Security Testing

Unit IV

- Wireless Security

Unit V

- Reporting and Countermeasures
-

CNS203 Cloud Security

- Cloud Architecture
 - Identity Management
 - Secure Virtualization
 - Cloud Risk Management
 - Compliance
-

CNS302 Digital Forensics

- Computer Forensics
 - Mobile Forensics
 - Memory Analysis
 - Network Forensics
 - Incident Response
-

Practical List

Students should perform practical exercises such as:

- Cisco Router Configuration

- Firewall Configuration
 - VPN Implementation
 - Penetration Testing using Kali Linux
 - Wire shark Packet Analysis
 - Snort IDS Configuration
 - Meta spoilt Framework
 - Digital Evidence Collection
 - Linux Server Hardening
 - Cloud Security Configuration
 - Vulnerability Assessment
 - Secure Network Design
-

Examination Scheme

Component	Marks
End Semester Examination	70
Internal Assessment	30
Practical	100
Seminar	100
Dissertation	300
Viva Voce	100

Recommended Reference Books

- Computer Networking: A Top-Down Approach
- Cryptography and Network Security
- Hacking: The Art of Exploitation
- Computer Security: Principles and Practice
- Digital Forensics and Incident Response

Programmer Outcomes

On successful completion of the programmed, graduates will be able to:

1. Design secure enterprise networks.
2. Apply advanced cyber security techniques to detect and mitigate threats.
3. Develop secure cloud and distributed systems.
4. Perform digital forensic investigations.
5. Conduct research in networking and cyber security.
6. Design and implement industry-standard security solutions.
7. Manage large-scale information security projects.
8. Pursue doctoral research or advanced professional careers in networking and cyber security.