NIRMA UNIVERSITY
Institute of Technology
B.Tech. Computer Science and Engineering
Semester-VI
Department Elective-I

L	T	P	C
2	0	2	3

Course Code	2CSDE54
Course Title	Information and Network Security

Course Outcomes:

At the end of the course, students will be able to –

1. illustrate principles and problems of cryptosystems for encryption, digital signing and authentication
2. apply methods to create core cryptographic algorithms
3. evaluate techniques to protect as well as attack a network.

Syllabus

Teaching Hours:30

Unit I

Security Overview: Significance of Information and network security, what are the hurdles in achieving the same, introduction to Cryptography — **02**

Unit II — **16**

Information Security: Classical Encryption Techniques, Block Ciphers and DES, Advanced Encryption Standard (AES), Block Cipher Operations, Pseudo Random Number Generation and Stream Ciphers, Mathematical Background(Fermat's Little Theorem, Euler Totient Function , Euler's Theorem Chinese Remainder Theorem etc.), Public Key Cryptography

Unit III — **12**

Network Security: Firewall, Secure Socket Layer (SSL) Architecture and working, Transport Level Security (TLS) including HTTPS, HTTPS Use, Secure Shell SSH Protocol, port forwarding, Wireless Network Security: IEEE 802.11 Architecture IEEE 802.11 Services Wired Equivalent Privacy (WEP), 802.11i Wireless LAN Security, Electronic Mail Security: Email Security Enhancements, Pretty Good Privacy (PGP), S/MIME, IP Security, IPSec, IPSec key management, Intrusion Detection: Concepts, Intrusion vs. Extrusion Detection Examples of Intrusion Categories of Intruders Hacker Behaviour, Insider Behaviour, Intrusion Techniques, Password Guessing and Capture Notification Alarms, Types of IDS.

Self-Study:

The self-study contents will be declared at the commencement of semester. Around 10% of the questions will be asked from self-study contents.

Laboratory Work:

Laboratory work will be based on the above syllabus with minimum 6 experiments to be incorporated.

Suggested Readings^:

1. William Stallings, "Cryptography and Network Security: Principles and Practice, Pearson
2. D. R. Stinson: Cryptography: Theory and Practice (Discrete Mathematics and Its Applications), CRC Press.
3. B. Schneier: Applied cryptography: protocols, algorithms, and source code in C, John Wiley & Sons.
4. Bernard Menezes: Network Security & Cryptography, 1st Edition, Cengage Learning, Delhi

L=Lecture, T=Tutorial, P=Practical, C=Credit

^this is not an exhaustive list