INDIAN INSTITUTE OF TECHNOLOGY ROORKEE

NAME OF DEPT./CENTRE: **Electronics and Computer Engineering**

1. Subject Code: **EC – 554N** Course Title: **Network Security**

2. Contact Hours: **L: 3** **T: 0** **P: 0**

3. Examination Duration (Hrs.): **Theory** 0 | 3 **Practical** 0 | 0

4. Relative Weight: **CWS** 15 **PRS** 00 **MTE** 35 **ETE** 50 **PRE** 00

5. Credits: 0 | 3 6. Semester √ **Autumn** ☐ **Spring** ☐ **Both**

7. Pre-requisite: **EC - 356**

8. Subject Area: **MSC**

9. Objective: To introduce the students to the security aspects of computer networks and electronic transactions

10. Details of the Course:

Sl. No.	Contents	Contact Hours
1.	Security model, security objectives and types of attacks.	3
2.	Symmetric key cryptography, DES, Triple DES, AES, and other symmetric ciphers, block cipher modes of operation.	6
3.	Public-key cryptography principles; Number theory: prime numbers, Chinese remainder theorem, discrete logarithms; RSA and other public key algorithms, key management and PKI; Authentication requirements, message authentication functions and hash algorithms.	9
4.	Digital signature requirements, direct and arbitrated signatures, authentication with symmetric and public key encryption, Kerberos, X.509 authentication service.	8
5.	Security issues in electronic mail, PGP, S/MIME.	4
6.	IP Security issues and architecture, Web security, transport layer security and Secure Socket Layer, secure electronic transaction.	6
7.	Intruders and intrusion detection, password management; Malicious software, viruses, worms and related threats; Firewalls and their design principles, trusted systems.	6
	Total	**42**

11. Suggested Books:

Sl. No.	Name of Books / Authors	Year of Publication
1.	Stallings, W., "Cryptography and Network Security: Principles and Practice", 4th Ed., Prentice-Hall.	2006
2.	Forouzan, B.A., "Cryptography and Network Security", Tata McGraw-Hill.	2007
3.	Schneier, B., "Applied Cryptography", 2nd Ed., Wiley & Sons.	2002
4.	Kaufman, C., Perlman, R. and Speciner, M., "Network Security", Prentice-Hall.	2002
5.	Bishop, M., "Computer Security: Art and Science", Pearson.	2003