PO	1	2	3	4	5	6	7	8	9	10	11	12
Level	H					H						

Syllabus for B. Tech. IV Year I semester
Computer Science and Engineering
INFORMATION SECURITY

Code: 7EC08

L	T	P	C
2	1	0	3

Prerequisite : Computer Networks

Course Objectives: To learn the fundamental concepts of security attacks, security services.To apply conventional cryptographic techniques in order to do encryption.To apply Public key cryptography techniques in order to do encryption.To learn IP security Architecture and its role in security framework.To apply SSL and TLS for Web Security.To design and develop Intrusion Detection Systems and Firewall.

Course Outcomes
At the end of this course, the student will be able to

1. Get familiarized with the fundamental concepts of security attacks, security services.
2. Implement the conventional cryptographic techniques.
3. Simulate the Public key cryptography techniques.
4. Comprehend IP security Architecture and its role in security framework.
5. Implement SSL and TLS for Web Security.
6. Design Intrusion Detection Systems and Firewall.

UNIT – I: Security Attacks (Interruption, Interception, Modification and Fabrication), Security Services (Confidentiality, Authentication, Integrity, Non-repudiation, access Control and Availability) and Mechanisms, A model for Internetwork security, Internet Standards and RFCs.

UNIT – II : Conventional Encryption Principles, Conventional encryption algorithms: DES, TDES, AES, cipher block modes of operation, location of encryption devices, key distribution, Approaches of Message Authentication, Secure Hash Functions: SHA1 and HMAC.

UNIT – III : Public key cryptography principles, public key cryptography algorithms: RSA, DIFFIE HELL MAN, digital signatures, digital Certificates, Certificate Authority and key management
Kerberos, X.509 Directory Authentication Service. Email privacy: Pretty Good Privacy (PGP) and S/MIME.

UNIT - IV
IP Security Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations and Key Management.

UNIT – V
Web Security Requirements, Secure Socket Layer (SSL) and Transport Layer Security (TLS), Secure Electronic Transaction (SET). Intruders, Viruses and related threats.

UNIT – VI: Firewall Design principles, Trusted Systems. Intrusion Detection Systems.

TEXT BOOKS:

1. Network Security Essentials (Applications and Standards) by William Stallings Pearson Education, 4th Edition.
2. Hack Proofing your network by Ryan Russell, Dan Kaminsky, Rain Forest Puppy, Joe Grand, David Ahmad, Hal Flynn Ido Dubrawsky, Steve W.Manzuik and Ryan Permeh, wiley Dreamtech

REFERENCES:

1. Fundamentals of Network Security by Eric Maiwald (Dreamtech press)
2. Network Security - Private Communication in a Public World by Charlie Kaufman, Radia Perlman and Mike Speciner, Pearson/PHI.
3. Cryptography and network Security, Third edition, Stallings, PHI/Pearson
4. Principles of Information Security, Whitman, Thomson.
5. Network Security: The complete reference, Robert Bragg, Mark Rhodes, TMH
6. Introduction to Cryptography, Buchmann, Springer.