PUBLIC KEY INFRASTRUCTURE AND TRUST MANAGEMENT
(ELECTIVE – I)

Course code: 15CS2206	**L**	**P**	**C**
	3	**0**	**3**

Prerequisites: Network security.

Course Outcomes: By the end of the course student can

CO1: Distinguish between public key technology and a public key infrastructure.
CO2: Understand the relationship of identity management to PKI.
CO3: Understand the components of a public key infrastructure.
CO4: Understand the issues related to Trust management mechanisms.
CO5: Understand Secure Crypto protocols like SSL and so on.

UNIT – I (10-Lectures)

Uses of cryptography, the concept devil and Alice. Principle of Cryptography. PKCS standards IEEE P1363, Block cipher modes of operation and data transformation for a symmetrical algorithms, Data transformation for RSA algorithm, Cryptographic Protocols, Protocol properties, Attributes of cryptographic protocols.

UNIT – II (10-Lectures)

Crypto Hardware and software, Smart cards, Universal Crypto interface, Real world attacks, valuation and certification, Public Key Infrastructure, PKI Works.

UNIT – III (10-Lectures)

Directory service, Requesting certificate revocation information, Practical Aspects Of PKI Construction- The course of construction of PKI, Basic questions about PKI construction, The most important PKI suppliers.

UNIT – IV (10-Lectures)

The internet and the OSI model-The OSI model, Crypto standards for OSI Layers 1 and 2-Crypto extensions for ISDN (Layer 1), Cryptography in the GSM standard (Layer 1), Crypto extensions for PPP (Layer 2), Virtual private networks.

UNIT – V (10-Lectures)

IPsec and IKE, IPsec, IKE, SKIP, Critical assessment of IPsec, Virtual private network with IPsec, SSL, TLS AND WTLS (Layer 4)-SSL working method, SSL protocol operation, Successful SSL, Technical comparison between IPsec and SSL, WTLS.

TEXT BOOKS:

Klaus schmeh: ‘‘Cryptography and public key infrastructure on the int ernet’’, 1st Edition, Allied Publishers, 2004.

REFERENCES:

Wenbo Mao: ‘‘Modern Cryptography : theory and practice’’, 1st Edition, Pearson Education, 2005.