PUBLIC KEY INFRASTRUCTURE AND TRUST MANAGEMENT (ELECTIVE – 1)

Course code: 13CS2206	**L**	**P**	**C**
	4	**0**	**3**

Prerequisites: Network security.

Course Educational Objectives:

The goal of this course is to enable the student to understand the foundational elements and complexity of a public key infrastructure.

Course Outcomes:

By the end of the course student can

1. Distinguish between public key technology and a public key infrastructure.
2. Understand the relationship of identity management to PKI
3. Understand the components of a public key infrastructure.
4. Understand the issues related to Trust management mechanisms.
5. Understand Secure Crypto protocols like SSL and so on.

UNIT – I

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

UNIT – II

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

UNIT – III

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

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

IPsec and IKE, IPsec, IKE, SKIP, Critical assessment of IPsec, Virtu al 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:

1. Klaus schmeh: "Cryptography and public key infrastructure on the internet", 1st Edition, Allied Publishers, 2004.

REFERENCES:

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