20ES013 - Embedded System Security

Unit – I
Introduction : Introduction, Services, Attacks, Security model, OSI security architecture and mechanisms, Internet standards and RFC, Buffering.

Unit - II
Encryption algorithms : Principles, Conventional algorithms, Key distribution, AES ,Diffie Hellman, N-parity Deffie Hellman, Elliptic curve and Elliptic curve cryptography,X.509 directory ,Authentication services, Hash functions secure hash

Unit - III
IP security : IP security overview , Architecture,IPV6 authentication header ,Encapsulation Security payload, ESP, Web security requirements.

Unit – IV
Transport layer security : SNMP, SNMPv1, SNMPv3, Intruders, Viruses, Threats , Secure Socket LayerandTransportLayerSecurity–SecureElectronicTransaction.SYSTEMSECURITYIntruders– IntrusionDetection–PasswordManagement–MaliciousSoftware-Firewalls–TrustedSystems.

Unit-V
PublicKeyInfrastructure: DigitalCertificates,PrivateKeyManagement,ThePKIXModel,Public Key CryptographyStandards,XML,PKIandSecurity.InternetSecurityProtocols:BasicConcepts,Secure Socket Layer, SHTTP, Time Stamping Protocol, Secure Electronic Transaction, SSL versus SET, 3-D Secure Protocol, Electronic Money, E-mail Security, Wireless Application Protocol (WAP) Security, Security inGSM

TEXTBOOKS:

1. Cryptography and Network Security – by Atul Kahate –TMH.
2. Data Communications and Networking- byBehourz A Forouzan
3. WilliamStallings,“CryptographyandNetworksecurity”,4thed.,PearsonEducation,2010.
4. William Stallings “Network Security Essentials Applications and Standards”, 2nd ed.,Pearson Education,2009

REFERENCEBOOKS:

1. James .F. Kurouse &W. Rouse, “Computer Networking: A Topdown.Approach Featuring”,3/e, PearsonEducation.
2. Forouzan,“DataCommunicationsandNetworking”,4thEdition,McGrawHill
3. William Stallings, “Data and Computer Communication”, Eighth Edition, Pearson Education, 2000