

with new features and facilities
Course Outcomes : 1. Student gets the wide spectrum of devices and protocols which connect together to create the IT infrastructure 2. Student gets the knowledge of the working and the interoperability between the data communication devices
UNIT I Computer Networking Devices : Router, switch, hub, Internet cables in the sea, DNS service, Certifying Authority(CA), Ethernet, Wireless routers and switches, Network Interface Card, IMEI in mobile phones, Network Protocols: FTP, SMTP, POP3, IMAP, HTTP, HTTPS, ARP, DHCP
(16 Hours)
UNIT II Wifi, Lifi, Wimax, Bluetooth, ZigBee, hotspots, Credit card, debit card, card readers, QR code, bar code, Biometric devices, EM spectrum, Infrared communication, Satellite communications, RADAR, SONAR
(16 Hours)
UNIT III The Onion Router (TOR), darkweb, ATM network, Data flow in Banking Infrastructure, GSM, CDMA, Mobile networks 2G/3G/4G/5G, Point of sale (POS) machine, Data flow in credit card, debit card, RFID, NFC, GPS, Geofencing, data modulation techniques, Wireless Sensor Network (WSN), data communication in drone
(16 Hours)
Textbooks : 1. D. Roddy, “Satellite Communication”, (4/e), McGraw- Hill, 2009. 2. Shuang-Hua Yang, “Wireless Sensor Networks: Principles, Design and Applications”, Springer-Verlag London, 2014. 3. “A Professional’s Guide to Data Communication in a TCP/IP World”, E. Bryan Carne, Artech house, 2004 4. James F Kurose and Keith W Ross, Computer Networking, A Top-Down Approach, Sixth edition, Pearson, 2017 5. Nader F Mir, Computer and Communication Networks, 2nd Edition, Pearson, 2014
CSCS 454 - DESIGN OF CRYPTOGRAPHIC ALGORITHMS

Course Objectives : 1. To make the student aware of the need to design tamper proof protocols using the cryptographic algorithms 2. To make the student aware of the higher level protocols which can withstand the attack from the hackers
Course Outcomes : 1. Student gets the ability to design and test one's own protocol and test their security strengths 2. Student gets the ability to read the laborious protocols written by others and the ability to meticulous work with them
UNIT I Cryptographic Protocols : Introduction to protocols, communications using symmetric cryptography, one-way functions, one-way hash functions, communications using public-key cryptography, digital signatures, digital signatures with encryption, random and pseudo-random-sequence generation Basic protocols : authentication, key exchange, authentication and key exchange, formal analysis of authentication and key-exchange protocols, multiple-key public-key cryptography, secret splitting, secret sharing, cryptographic protection of databases
(12 Hours)
UNIT II Intermediate protocols : Timestamping services, subliminal channel, undeniable digital signatures, designated confirmer signatures, proxy signatures, group signatures, fail-stop digital signatures, computing with encrypted data, bit commitment, fair coin flips, mental poker, one-way accumulators, all-or-nothing disclosure of secrets, key escrow
(12 Hours)
UNIT III Advanced protocols : zero-knowledge proofs, zero-knowledge proofs of identity, blind signatures, identity-based public-key cryptography, oblivious signatures, oblivious transfer, simultaneous contract signing, digital certified mail, simultaneous exchange of secrets, Esoteric protocols : secure elections, secure multiparty computation, anonymous message broadcast, digital cash
(12 Hours)
Textbooks : 1. “Applied Cryptography, protocols, algorithms, and source code in C ”, second edition, Bruce Schneier, Wiley, 1996