

Direct Link Networks : Hardware Building Blocks: Nodes, Links, Encoding (NRZ, NRZI, Manchester, 4B/5B), Framing : Byte-Oriented Protocols (BISYNC, PPP, DDCMP), Bit-Oriented Protocols (HDLC), Clock-Based Framing (SONET), Error Detection: Two-Dimensional Parity, Internet Checksum Algorithm, Cyclic Redundancy Check, Reliable Transmission : Stop-and-Wait, Sliding Window, Concurrent Logical Channels, , Ethernet (802.3): Physical Properties, Access Protocol, Experience with Ethernet, Token Rings (802.5, FDDI): Physical Properties, Token Ring Media Access Control, Token Ring Maintenance, Frame Format, Wireless (802.11): Physical Properties, Collision Avoidance, Distribution System, Frame Format, Network Adaptors. **(16 hours)**

UNIT III

Packet Switching : Switching and Forwarding : Datagrams, Virtual Circuit Switching, Source Routing, Bridges and LAN Switches: Learning Bridges, Spanning Tree Algorithm, Broadcast and Multicast, Limitations of Bridges, Cell Switching (ATM): Cells, Segmentation and Reassembly, Virtual Paths, Physical Layers for ATM, ATM in the LAN, Implementation and Performance. **(16 hours)**

Course Outcome:

At the end of the course student will be able to

- 1) Recognize different networking devices and its functions.
- 2) Designing network requirements for data communication.

TextBooks:

- (1). “Computer Networks, A Systems Approach”, Larry L. Peterson & Bruce S. Davie, Third Edition, Morgan Kaufmann Publishers, 2003
- (2). “Computer Networks”, Andrew S. Tanenbaum David J. Wetherall, Fifth Edition, Pearson Education Limited 2014
- (3). “A Professional’s Guide to Data Communication in a TCP/IP World”, E. Bryan Carne, Artech House Inc, 2004

CSCS 454 - DESIGN OF CRYPTOGRAPHIC ALGORITHMS

Course Objective:

The objective of the courses to

- 1) To understand the fundamentals of Cryptography.
- 2) To understand the security techniques used in cryptography.

UNIT I

Primes, Factoring, and RSA, Assumptions in Cyclic Groups, Cryptographic Applications of Number-Theoretic Assumptions, **Private-Key Management and the Public-Key Revolution**: Limitations of Private-Key Cryptography, A Partial Solution – Key Distribution Centers, The Public-Key Revolution, Diffie-Hellman Key Exchange, Public-Key Encryption, Hybrid Encryption, RSA Encryption. **(12 hours)**

UNIT II

Digital Signature Schemes: RSA Signatures, The “Hash-and-Sign” Paradigm, Lamport’s One-Time Signature Scheme, Public-Key Cryptosystems in the Random Oracle Model. **(12 hours)**

UNIT III

Hardware Design of the Advanced Encryption Standard (AES) : Algorithmic and

Architectural Optimizations for AES Design, Circuit for the AES S-Box, Implementation of the MixColumns Transformation, Reconfigurable Design for the Rijndael Cryptosystem, Single Chip Encryptor/Decryptor.

(12 hours)

Course Outcome:

At the end of the course student will be able to

- 1) Learns the fundamentals and development of cryptographic algorithms.
- 2) Understand hardware design of the advanced Encryption Standards.

TextBooks:

- (1). “Hardware Security Design, Threats, and Safeguards”, DebdeepMukhopadhyayRajatSubhraChakraborty, CRC Press, 2015
- (2). “Hardware IP Security and Trust “ ,Prabhat Mishra, SwarupBhunia, Mark Tehranipoor, Springer, 2017
- (3). “Fault Tolerant Architectures for Cryptography and Hardware Security”, SikharPatranabisDebdeepMukhopadhyay, Springer, 2018
- (4). “Security of Block Ciphers - From Algorithm Design to Hardware Implementation”, Kazuo Sakiyama, Yu Sasaki, Yang Li, Wiley, 2015
- (5). “Physically Unclonable Functions From Basic Design Principles to Advanced Hardware Security Applications”, Basel Halak, Springer, 2018
- (6). “Hardware-Based Computer Security Techniques to Defeat Hackers From Biometrics to Quantum Cryptography”, Roger Dube, Wiley, 2008

CSCS 455 - CYBER THREAT INTELLIGENCE

Course Objective:

The objective of the courses to

- 1) Understand the Fundamentals of Cyber threats
- 2) Understand the threats and prevention methods.

UNIT I

Moving to Proactive Cyber Threat Intelligence: Proactive Intelligence beyond the Deepweb and Darkweb, **Understanding Darkweb Malicious Hacker Forums:** Forum Structure and Community Social Organization. (12 hours)

UNIT II

Automatic Mining of Cyber Intelligence from the Darkweb, Analyzing Products and Vendors in Malicious Hacking Markets: Marketplace Data Characteristics, Users Having Presence in Markets/Forums, Discovery of Zero-Day Exploits, Exploits Targeting Known Vulnerabilities. (12hours)

UNIT III

Using Game Theory for Threat Intelligence: Security Game Framework, Computational Complexity, Algorithms, **Application:** Protecting Industrial Control Systems, **Challenges and Environmental Characteristics.**

(12 hours)

Course Outcome:

At the end of the course student will be able to

- 1) Analysis and evaluate efficient methods, applications and challenges in threat intelligence.
- 2) Ability to evaluate effective detection and prevention methods.