NETWORK AND CYBER SECURITY

B.E., 8TH Semester, Electronics & Communication Engineering/
Telecommunication Engineering
[As per Choice Based credit System (CBCS) Scheme

Course Code	**17EC835**	**CIE Marks**	**40**
Number of Lecture Hours/Week	**03**	**SEE Marks**	**60**
Total Number of Lecture Hours	**40 (8 Hours per Module)**	**Exam Hours**	**03**

CREDITS – 03

Course Objectives: This course will enable students to:

- Know about security concerns in Email and Internet Protocol.
- Understand cyber security concepts.
- List the problems that can arise in cyber security.
- Discuss the various cyber security frame work.

Module-1

Transport Level Security: Web Security Considerations, Secure Sockets Layer, Transport Layer Security, HTTPS, Secure Shell (SSH) (Text 1: Chapter 15)

Module-2

E-mail Security: Pretty Good Privacy, S/MIME, Domain keys identified mail (Text 1: Chapter 17)

Module-3

IP Security: IP Security Overview, IP Security Policy, Encapsulation Security Payload (ESP), Combining security Associations Internet Key Exchange. Cryptographic Suites(Text 1: Chapter 18)

Module-4

Cyber network security concepts: Security Architecture, Antipattern: signature based malware detection versus polymorphic threads, document driven certification and accreditation, policy driven security certifications. Refactored solution: reputational, behavioural and entropy based malware detection.

The problems: cyber antipatterns concept, forces in cyber antipatterns, cyber anti pattern templates, cyber security Antipattern catalog (Text-2: Chapter1 & 2)

Module-5

Cyber network security concepts contd. :

Enterprise security using Zachman framework

Zachman framework for enterprise architecture, primitive models versus composite models, architectural problem solving patterns, enterprise workshop, matrix mining, mini patterns for problem solving meetings.

Case study: cyber security hands on – managing administrations and root accounts, installing hardware, reimaging OS, installing system protection/ antimalware, configuring firewalls (Text-2: Chapter 3 & 4).

Course Outcomes: After studying this course, students will be able to:

- Explain network web security protocols of SSL, TLS, HTTPS, SSH.
- Outline the basic cyber security concepts - Pretty Good Privacy, S/MIME, and Domain keys identified mail.

- Discuss the IP Security, Cyber network security concepts and cyber security problems.
- Explain Enterprise Security using Zachman Framework.
- Apply concept of cyber security framework to computer system administration.

Text Books:

1. William Stallings, “Cryptography and Network Security Principles and Practice”, Pearson Education Inc., 6th Edition, 2014, ISBN: 978-93-325- 1877-3.
2. Thomas J. Mowbray, “Cyber Security – Managing Systems, Conducting Testing, and Investigating Intrusions”, Wiley.

Reference Books:

1. Cryptography and Network Security, Behrouz A. Forouzan, TMH, 2007.
2. Cryptography and Network Security, Atul Kahate, TMH, 2003.