SECURE COMMUNICATIONS

17ECMC1T5C **Credits: 4**

Lecture: 4 periods/week **Internal assessment: 40 marks**

Semester end examination: 60 marks

Prerequisites: Digital Communications, Wireless Communications.

Course Objectives:

Upon completion of this course, students will be able to:

- Conceptualize the necessity of Security.
- Will understand the process involved in data modelling.
- Will be able to analyze and handle security risks.
- Will be able to understand latest technologies on security.

Course Outcomes:

Upon completion of this course, students will be able to:

- Conceptualize the necessity of Security.
- Will understand the process involved in data modelling.
- Will be able to analyze and handle security risks.
- Will be able to understand latest technologies on security.

UNIT-I

Security concepts: Introduction to the Concept of Security, threats, security services, security mechanisms.Basic encryption techniques, Concept of cryptanalysis, Shannon's theory , Perfect secrecy, Block ciphers, Cryptographic algorithms, Features of Data Encryption Standard, Linear and Differential Cryptanalysis, Advanced Encryption Standard, Stream ciphers, Pseudo random sequence generators.

UNIT-II

Database Security: Security policies, Policy enforcement & related issues, Design principles, Multilevel relational data models, Security impact on database function, inference problem Public Key Infrastructure (PKI), Internet Security Protocols, Network Security.

UNIT-III

Software Security: Defining a discipline, A Risk Management Framework, Code review with a tools, Architectural risk analysis, Software penetrating testing, Risk Based security Testing, An Enterprise S/W security program, Security knowledge.

UNIT-IV

Intrusion detection: Defining Intrusion Detection, Security concepts intrusion Detection concept, determining strategies for Intrusion Detection, Responses, Technical issues.

Biometric Security: Biometric Fundamentals, Types of Biometrics, Fingerprints and Hand Geometry, Facial and Voice Recognition, Iris and Retina scanning, Signature Recognition and Keystroke Dynamics, Behavioural and Esoteric Biometric Technologies, Issues Involving Biometrics, Privacy.

Text Books:

1.William Stallings, " Cryptography and Network Security", 4 th edition, Pearson Education, 2006

References:

1. Douglas A. Stinson, "Cryptography, Theory and Practice", 2nd edition, Chapman & Hall, CRC Press Company, Washington.

2. Wade Trappe, Lawrence C. Washington, " Introduction to Cryptography with Coding Theory" Second edition – Pearson Education, 2006

3." Biometric Security and Privacy: Opportunities & Challenges in The Big Data Era ", by Richard Jiang, Somaya Al-Madeed, Ahmed Bouridane, Danny Crookes, AzeddineBeghdadi, Springer 2017.