EE4212: CRYPTOGRAPHY AND INFORMATION THEORY

Effective Term
Semester A 2022/23

Part I Course Overview

Course Title
Cryptography and Information Theory

Subject Code
EE - Electrical Engineering
Course Number
4212

Academic Unit
Electrical Engineering (EE)

College/School
College of Engineering (EG)

Course Duration
One Semester

Credit Units
3

Level
B1, B2, B3, B4 - Bachelor's Degree

Medium of Instruction
English

Medium of Assessment
English

Prerequisites
MA2001 Multi-variable Calculus and Linear Algebra
and
[EE3001 Foundations of Data Engineering
or
EE3313 Applied Queueing Systems
or
MA3160 Probability and Stochastic Processes
or
EE3331 Probability Models In Information Engineering]

Precursors
EE3009 Data Communications and Networking

Equivalent Courses

Nil

Exclusive Courses

Nil

Part II Course Details

Abstract

The course aims to provide students with an understanding of the fundamental concepts of information theory and the principles of cryptography. The objective is intended for students to learn data compression and information coding in digital transmission systems. In addition, the course provides students an understanding of the cryptography and network security technology.

Course Intended Learning Outcomes (CILOs)

	CILOs	Weighting (if app.)	DEC-A1	DEC-A2	DEC-A3
1	Compute and manipulate common information measures and describe their relationship		x	x	
2	Apply source coding techniques to achieve data compression		x	x	
3	Apply error control coding techniques to achieve error detection and correction, and describe their capability		x	x	
4	Describe the key concepts of cryptography		x	x	
5	Apply cryptographic techniques to defend against attacks		x	x	

A1: Attitude
Develop an attitude of discovery/innovation/creativity, as demonstrated by students possessing a strong sense of curiosity, asking questions actively, challenging assumptions or engaging in inquiry together with teachers.

A2: Ability
Develop the ability/skill needed to discover/innovate/create, as demonstrated by students possessing critical thinking skills to assess ideas, acquiring research skills, synthesizing knowledge across disciplines or applying academic knowledge to real-life problems.

A3: Accomplishments
Demonstrate accomplishment of discovery/innovation/creativity through producing /constructing creative works/new artefacts, effective solutions to real-life problems or new processes.

Teaching and Learning Activities (TLAs)

	TLAs	Brief Description	CILO No.	Hours/week (if applicable)
1	Lectures	Key concepts are described and illustrated. Key concepts are worked out based on problems.	1, 2, 3, 4, 5	3 hrs/week
2	Assignments	Problem-based exercises.	1, 2, 3, 4, 5	

3	Quizzes/Test	Assessment of learned concepts and techniques.	1, 2, 3, 4, 5	

Assessment Tasks / Activities (ATs)

	ATs	CILO No.	Weighting (%)	Remarks (e.g. Parameter for GenAI use)
1	Tests (min.: 2)	1, 2, 3, 4, 5	30	
2	#Assignments (min.: 3)	1, 2, 3, 4, 5	20	

Continuous Assessment (%)

50

Examination (%)

50

Examination Duration (Hours)

2

Additional Information for ATs

Remark:
To pass the course, students are required to achieve at least 30% in course work and 30% in the examination.

may include homework, tutorial exercise, project/mini-project, presentation

Assessment Rubrics (AR)

Assessment Task

Examination

Criterion

Achievements in CILOs

Excellent (A+, A, A-)

High

Good (B+, B, B-)

Significant

Fair (C+, C, C-)

Moderate

Marginal (D)

Basic

Failure (F)

Not even reaching marginal levels

Assessment Task

Coursework

Criterion

Achievements in CILOs

Excellent (A+, A, A-)
High

Good (B+, B, B-)
Significant

Fair (C+, C, C-)
Moderate

Marginal (D)
Basic

Failure (F)
Not even reaching marginal levels

Part III Other Information

Keyword Syllabus

Information Measures
Entropy; Joint Entropy; Conditional Entropy; Mutual Information; Chain Rules; Information Inequalities

Data Compression
Fixed-Length Codes; Variable-Length Codes; Prefix Codes; Kraft Inequality; Entropy Bound; Huffman Codes

Finite Field
Definition of Finite Field; Polynomial Representation of Finite Field Elements; Properties of Polynomials and Finite Field Elements

Linear Block Codes
Generator Matrix; Parity-Check Matrix; Syndrome Testing; Minimum Distance; Error Detection and Correction Capability; Cyclic Codes; Well-known Block Codes (e.g. Hamming Codes, Reed-Solomon Codes, Golay Codes, BCH Codes)

Overview of Cryptography
Alice-Bob-Eve framework; Threat Model and Attacker Knowledge; Kerckhoff's Principle; Security by Obscurity

Perfectly Secure Cryptosystems
Information-Theoretic Security vs. Computational Security; One-Time Pad; Threshold Secret Sharing

Public-Key Cryptosystems
ElGamal's Cryptosystems; RSA Cryptosystems; Elliptic Curve Cryptosystems

Introduction to Quantum Computing
Basic Concepts of Quantum Computers and Quantum Cryptography; Shor's Algorithm for Integer Factorization

Reading List

Compulsory Readings

	Title
1	Nil

Additional Readings

	Title
1	T. M. Cover and J. A. Thomas, Elements of Information Theory, 2nd Edition, Wiley-Interscience, 2006.
2	R. W. Yeung, Information Theory and Network Coding, Springer, 2008.
3	W. Stallings, Cryptography and Network Security: Principles and Practice, 7th Edition, Pearson, 2017.
4	S. Rubinstein-Salzedo, Cryptography, Springer, 2018.