MA4539: MATHEMATICS FOR CRYPTOGRAPHY

Effective Term
Semester A 2022/23

Part I Course Overview

Course Title
Mathematics for Cryptography

Subject Code
MA - Mathematics
Course Number
4539

Academic Unit
Mathematics (MA)

College/School
College of Science (SI)

Course Duration
One Semester

Credit Units
3

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

Medium of Instruction
English

Medium of Assessment
English

Prerequisites
MA2504 Discrete Mathematics, or
MA2509 Discrete Mathematics

Precursors
Nil

Equivalent Courses
Nil

Exclusive Courses
Nil

Part II Course Details

Abstract

This course introduces students to the mathematical fundamentals of cryptography. Concepts paramount to the understanding and development of modern cryptography will be discussed and demonstrated. The course helps students understand the ideas and design of a cryptosystem and equips them with the knowledge in solving related problems in cryptography.

Course Intended Learning Outcomes (CILOs)

	CILOs	Weighting (if app.)	DEC-A1	DEC-A2	DEC-A3
1	explain at high levels concepts from number theory, including divisibility and primality.	15	x		
2	state fundamental results in number theory and prove rigorously mathematical statements concerning prime numbers and modular arithmetic.	15	x	x	
3	solve diophantine equations, linear and quadratic congruences.	15		x	
4	describe the notion of quadratic residues and related results (such as Gauss’ s theorem of quadratic reciprocity).	15	x	x	
5	apply knowledge of number theory in describing and analyzing cryptographic tools.	25		x	x
6	the combination of CILOs 1-5	15	x	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	Learning through teaching is primarily based on lectures.	1, 2, 3, 4, 5, 6	39 hours in total

2	Take-home assignments	Learning through take-home assignments helps students understand basic results and methods of elementary number theory, as well as the applications of which in cryptography.	1, 2, 3, 4, 5	after-class

Assessment Tasks / Activities (ATs)

	ATs	CILO No.	Weighting (%)	Remarks (e.g. Parameter for GenAI use)
1	Test	1, 2, 3	15	Questions are designed for the first part of the course to see how well students have learned basic concepts concerning divisibility of integers and prime numbers, as well as methods of solving diophantine equations and congruences.
2	Hand-in assignments	1, 2, 3, 4, 5	15	These are skills based assessment which enables students to apply basic concepts and techniques of number theory in proving mathematical statements, solving congruences and describing applications in cryptography.
3	Formative take-home assignments	1, 2, 3, 4, 5	0	The assignments provide students chances to demonstrate their achievements on number theory and cryptography learned in this course.

Continuous Assessment (%)

30

Examination (%)

70

Examination Duration (Hours)

3

Additional Information for ATs

30% Coursework
70% Examination (Duration: 3 hours, at the end of the semester)
For a student to pass the course, at least 30% of the maximum mark for the examination must be obtained.

Assessment Rubrics (AR)

Assessment Task
1. Test

Criterion
Ability in problem solving

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
2. Hand-in assignments

Criterion
Understanding of concepts and applications

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
3. Formative take-home assignments

Criterion
Study attitude

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
4. Examination

Criterion
Comprehensive ability in independent problem solving

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
Division Algorithm, Prime numbers, Linear and Quadratic Congruences, Quadratic residues, Diophantine Equations, Classical cryptosystems, Cryptanalysis, and Public-key cryptosystems.

Reading List

Compulsory Readings

	Title
1	Nil

Additional Readings

	Title
1	Nil