CS3104: APPLIED CRYPTOGRAPHIC SYSTEMS

Effective Term
Semester A 2025/26

Part I Course Overview

Course Title
Applied Cryptographic Systems

Subject Code
CS - Computer Science
Course Number
3104

Academic Unit
Computer Science (CS)

College/School
College of Computing (CC)

Course Duration
One Semester

Credit Units
3

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

Medium of Instruction
English

Medium of Assessment
English

Prerequisites
MA2185 Discrete Mathematics or equivalent; AND
CS2117 Foundation of Cybersecurity

Precursors
Nil

Equivalent Courses
Nil

Exclusive Courses
Nil

Part II Course Details

Abstract

This course aims to provide an introduction to the practical applications of cryptographic techniques in real-world security systems. The main objective is for students to have a comprehensive understanding of how cryptographic algorithms and protocols are used to secure various systems and applications. The course will cover a wide range of topics, including symmetric encryption, public key infrastructure (PKI), digital signatures, key management, and cryptographic APIs. Throughout the course, students will also explore the challenges and considerations involved in applying cryptographic techniques to real-world systems, such as performance, scalability, and usability.

Course Intended Learning Outcomes (CILOs)

	CILOs	Weighting (if app.)	DEC-A1	DEC-A2	DEC-A3
1	Understand the principles and best practices of symmetric encryption.	20		x	
2	Apply asymmetric cryptographic techniques to design and implement secure systems.	20		x	
3	Evaluate the security of cryptographic systems and identify potential vulnerabilities, taking into account performance, scalability, and usability considerations.	20	x	x	
4	Analyze and implement cryptographic solutions with various cryptographic tools.	20	x	x	
5	Explore and assess the impact of emerging trends in applied cryptography.	20	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.

Learning and Teaching Activities (LTAs)

	LTAs	Brief Description	CILO No.	Hours/week (if applicable)
1	Lecture	Explain basic ideas, concepts, theorems, algorithms and protocols.	1, 2, 3, 4	3 hours/ week
2	Tutorials	Help the students to understand and practise what they have learned in lectures.	1, 2, 3, 4	8 hours/ semester
3	Assignments	Require students to develop the ability to think in depth about concepts and algorithms, and the ability to solve problems independently.	1, 2, 3, 4, 5	

Assessment Tasks / Activities (ATs)

	ATs	CILO No.	Weighting (%)	Remarks ("-" for nil entry)	Allow Use of GenAI?
1	Assignments	1, 2, 3, 4, 5	20	2 assignments	Yes
2	Quiz	1, 2, 3, 4	10	One hour	No

Continuous Assessment (%)
30

Examination (%)
70

Examination Duration (Hours)
2

Minimum Examination Passing Requirement (%)
30

Additional Information for ATs
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
Assignments

Criterion
Ability to explain and use concepts, algorithms and protocols, and the ability to solve problems independently

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
Quiz

Criterion
Ability to explain and use concepts, algorithms and protocols

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
Examination

Criterion
Ability to explain and use concepts, algorithms and protocols

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

Basic number theory, one-way functions, symmetric encryption, one-time Pad, DES, AES, brute force attacks, strength of encryption functions, block and stream cipher, key distribution problem, key management, asymmetric encryption, RSA, prime number generation, public key protocol, hybrid encryption, key exchange protocol, Diffie-Hellman, authentication protocols, hash functions, MD5, SHA, data integrity, message integrity code, non-repudiation, digital signature, RSA signature, ElGamal, DSA, elliptic curve cryptosystem.

Reading List

Compulsory Readings

	Title
1	Applied Cryptography Protocols, Algorithms, and Source Code in C.John Wiley & Sons, ISBN 1119096723, 2nd edition, 2015.

Additional Readings

	Title
1	Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone. Handbook of Applied Cryptography. CRC Press, ISBN 0849385237, Available on-line at http://www.cacr.math.uwaterloo.ca/hac/, 2014.
2	Chapman & Hall. Cryptography, Theory and Practice. CRC, ISBN 1138197017, 4th edition, 2018.