CS5288: CRYPTOGRAPHY: THEORY AND PRACTICE

Effective Term
Semester A 2025/26

Part I Course Overview

Course Title
Cryptography: Theory and Practice

Subject Code
CS - Computer Science
Course Number
5288

Academic Unit
Computer Science (CS)

College/School
College of Computing (CC)

Course Duration
One Semester

Credit Units
3

Level
P5, P6 - Postgraduate Degree

Medium of Instruction
English

Medium of Assessment
English

Prerequisites
(CS5222 Computer Networks and Internets or equivalent) and
(MA2144 Discrete Mathematics or equivalent)

Precursors
Nil

Equivalent Courses
Nil

Exclusive Courses
Nil

Part II Course Details

Abstract

The course provides an in-depth study of cryptographic techniques and their role in practical computer systems and applications. It covers the algorithms for symmetric and asymmetric encryption, hash functions, and pseudo random number generation; and the protocols to achieve practical security objectives such as confidentiality, authentication, data integrity, non-repudiation. Associated protocols such as key distribution and public key infrastructure systems will also be dealt with.

Course Intended Learning Outcomes (CILOs)

	CILOs	Weighting (if app.)	DEC-A1	DEC-A2	DEC-A3
1	Apply modular arithmetic mathematic and basic group theoretic/finite field operations related to cryptographic techniques.			x	
2	Describe basic concepts and algorithms of cryptography, including encryption/decryption, hash functions, pseudo random number generation.			x	
3	Critique and assess the security of cryptographic functions, and evaluate their strength.			x	
4	Create and analyze protocols for various security objectives with cryptographic tools.		x	x	x
5	Explain the impact of potential future development of cryptography such as quantum cryptography.		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.

Learning and Teaching Activities (LTAs)

	LTAs	Brief Description	CILO No.	Hours/week (if applicable)
1	Lecture	Students will engage in lectures about concepts, theory and methodologies.	1, 2, 3, 5	2 hours/ week
2	Tutorials	Students will engage in exercises and discussions	1, 2, 4, 5	1 hour/ week

Assessment Tasks / Activities (ATs)

	ATs	CILO No.	Weighting (%)	Remarks ("-" for nil entry)	Allow Use of GenAI?
1	Assignment #1	1, 2, 4	10	-	Yes
2	Assignment #2	1, 2	10	-	Yes
3	Quiz	1, 2, 5	10	-	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 (for students admitted before Semester A 2022/23 and in Semester A 2024/25 & thereafter)

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 (for students admitted before Semester A 2022/23 and in Semester A 2024/25 & thereafter)

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 (for students admitted before Semester A 2022/23 and in Semester A 2024/25 & thereafter)

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
Assignments (for students admitted from Semester A 2022/23 to Summer Term 2024)

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

Excellent
(A+, A, A-) The answer is correct and written in a clear manner.

Good
(B+, B) The answer is mostly correct, with some minor mistakes.

Marginal
(B-, C+, C) The answer is large correct with some mistakes.

Failure
(F) Below the marginal level

Assessment Task
Quiz (for students admitted from Semester A 2022/23 to Summer Term 2024)

Criterion
Ability to explain and use concepts, algorithms and protocols

Excellent
(A+, A, A-) The answer is correct and written in a clear manner.

Good
(B+, B) The answer is mostly correct, with some minor mistakes.

Marginal
(B-, C+, C) The answer is large correct with some mistakes.

Failure
(F) Below the marginal level

Assessment Task
Examination (for students admitted from Semester A 2022/23 to Summer Term 2024)

Criterion
Ability to explain and use concepts, algorithms and protocols

Excellent
(A+, A, A-) Depending on the rubrics of the final exam paper

Good
(B+, B) Depending on the rubrics of the final exam paper

Marginal
(B-, C+, C) Depending on the rubrics of the final exam paper

Failure
(F) Depending on the rubrics of the final exam paper

Part III Other Information

Keyword Syllabus
Basic number theory, one-way functions, basic randomness, symmetric encryption, one-tine Pad, Feistel structure, DES, IDEA, AES, brute force attacks, strength of encryption functions, block and stream cipher, key distribution problem, secret sharing, 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, trust model, digital certificate, PKI, zero knowledge proofs, blind signature, quantum cryptography.

Reading List

Compulsory Readings

	Title
1	Handbook of Applied Cryptography Online version: http://www.cacr.math.uwaterloo.ca/hac/
2	William Stallings, Cryptography and Network Security: Principles and Practices. Prentice Hall, ISBN-10: 0136097049, 5th edition.

Additional Readings

	Title
1	Chapman & Hall. Cryptography, Theory and Practice. CRC, ISBN 1584882069, 2nd edition.
2	Cryptography: An Introduction
3	Online version: https://www.cs.umd.edu/~waa/414-F11/IntroToCrypto.pdf