CS4288: CRYPTOGRAPHIC ALGORITHMS AND PROTOCOLS

Effective Term
Semester A 2022/23

Part I Course Overview

Course Title
Cryptographic Algorithms and Protocols

Subject Code
CS - Computer Science
Course Number
4288

Academic Unit
Computer Science (CS)

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
MA2185 Discrete Mathematics or equivalent

Precursors
Nil

Equivalent Courses
Nil

Exclusive Courses
Nil

Part II Course Details

Abstract

The course aims to provide an introduction to cryptographic techniques. The main objective is for students to learn and understand basic algorithms for symmetric and asymmetric cryptography and their mathematical principles, as well as their applications to fundamental security protocols. A particular emphasize is put on improving their abilities to follow up advancement of cryptographic techniques and security protocols in the future.

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	Understand basic concepts and algorithms of cryptography, including encryption/decryption, hash functions, pseudo random number generation.			x	
3	Make critique and assessment on the security of cryptographic functions, and evaluate their strength.		x	x	
4	Create and analyse protocols for various security objectives with cryptographic tools.		x	x	
5	Develop an ability to explore and analyse the impact of potential future development of cryptography.		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	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 (e.g. Parameter for GenAI use)
1	Assignments	1, 2, 3, 4, 5	20	2 assignments
2	Quiz	1, 2, 3, 4	10	One hour

Continuous Assessment (%)

30

Examination (%)

70

Examination Duration (Hours)

2

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, 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, zero knowledge proofs.

Reading List

Compulsory Readings

	Title
1	William Stallings, Cryptography and Network Security: Principles and Practices. Prentice Hall, ISBN-10: 0136097049, 5th edition.

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/
2	Chapman & Hall. Cryptography, Theory and Practice. CRC, ISBN 1584882069, 2nd edition.