City University of Hong Kong
Course Syllabus

offered by Department of Computer Science
with effect from Semester A 2022/23

Part I Course Overview

Course Title:	Cryptography: Theory and Practice
Course Code:	CS5288
Course Duration:	One semester
Credit Units:	3 credits
Level:	P5
Medium of Instruction:	English
Medium of Assessment:	English
Prerequisites: *(Course Code and Title)*	(CS5222 Computer Networks and Internets or equivalent) and (MA2144 Discrete Mathematics or equivalent)
Precursors: *(Course Code and Title)*	Nil
Equivalent Courses: *(Course Code and Title)*	Nil
Exclusive Courses: *(Course Code and Title)*	Nil

Part II Course Details

1. 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.

2. Course Intended Learning Outcomes (CILOs)

(CILOs state what the student is expected to be able to do at the end of the course according to a given standard of performance.)

No.	CILOs	Weighting (if applicable)	Discovery-enriched curriculum related learning outcomes (please tick where appropriate)		
			A1	*A2*	*A3*
1.	Apply modular arithmetic mathematic and basic group theoretic/finite field operations related to cryptographic techniques.			✓	
2.	Describe basic concepts and algorithms of cryptography, including encryption/decryption, hash functions, pseudo random number generation.			✓	
3.	Make critique and assessment on the security of cryptographic functions, and evaluate their strength.			✓	
4.	Create and analyze protocols for various security objectives with cryptographic tools.		✓	✓	✓
5.	Explain the impact of potential future development of cryptography such as quantum cryptography.		✓	✓	✓
		100%			

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 self-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.

3. Teaching and Learning Activities (TLAs)

(TLAs designed to facilitate students' achievement of the CILOs.)

TLA	Brief Description	CILO No.					Hours/week (if applicable)
		1	2	3	4	5	
Lectures	Concepts, theory and methodologies.	✓	✓	✓		✓	2 hours/ week
Tutorials	Exercises and discussions	✓	✓		✓	✓	1 hour/ week

4. Assessment Tasks/Activities (ATs)

(ATs are designed to assess how well the students achieve the CILOs.)

Assessment Tasks/Activities	CILO No.					Weighting	Remarks
	1	2	3	4	5		
Continuous Assessment: 30%							
Assignment #1	✓	✓		✓		10%	
Assignment #2	✓	✓				10%	
Quiz	✓	✓			✓	10%	
Examination^: 70% (duration: 2 hours)							
						100%	

^ For a student to pass the course, at least 30% of the maximum mark for the examination must be obtained.

5. Assessment Rubrics

(Grading of student achievements is based on student performance in assessment tasks/activities with the following rubrics.)

Applicable to students admitted in Semester A 2022/23 and thereafter

Assessment Task	Criterion	Excellent (A+, A, A-)	Good (B+, B)	Marginal (B-, C+, C)	Failure (F)
1. Assignments	Ability to explain and use concepts, algorithms and protocols, and the ability to solve problems independently	The answer is correct and written in a clear manner.	The answer is mostly correct, with some minor mistakes.	The answer is large correct with some mistakes.	Below the marginal level
2. Quiz	Ability to explain and use concepts, algorithms and protocols	The answer is correct and written in a clear manner.	The answer is mostly correct, with some minor mistakes.	The answer is large correct with some mistakes.	Below the marginal level
3. Examination	Ability to explain and use concepts, algorithms and protocols	Depending on the rubrics of the final exam paper	Depending on the rubrics of the final exam paper	Depending on the rubrics of the final exam paper	Depending on the rubrics of the final exam paper

Applicable to students admitted before Semester A 2022/23

Assessment Task	Criterion	Excellent (A+, A, A-)	Good (B+, B, B-)	Fair (C+, C, C-)	Marginal (D)	Failure (F)
1. Assignments	Ability to explain and use concepts, algorithms and protocols, and the ability to solve problems independently	High	Significant	Moderate	Basic	Not even reaching marginal levels
2. Quiz	Ability to explain and use concepts, algorithms and protocols	High	Significant	Moderate	Basic	Not even reaching marginal levels
3. Examination	Ability to explain and use concepts, algorithms and protocols	High	Significant	Moderate	Basic	Not even reaching marginal levels

Part III Other Information (more details can be provided separately in the teaching plan)

1. Keyword Syllabus

(An indication of the key topics of the course.)

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.

2. Reading List

2.1 Compulsory Readings

(Compulsory readings can include books, book chapters, or journal/magazine articles. There are also collections of e-books, e-journals available from the CityU Library.)

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.

2.2 Additional Readings

(Additional references for students to learn to expand their knowledge about the subject.)

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