THE CHINESE UNIVERSITY OF HONG KONG
Print Course Catalog Details

Academic Org: Div of Computer Science & Engg – Subject: Computer Science

Course: CSCI5440 **Course ID:** 009056 **Eff Date:** 2022-07-01 **Crse Status: Active** **Apprv. Status:** Approved **[**Course Rev**]**

Theory of Cryptography **密碼學理論**

The modern theory of cryptography studies the formal modelling and construction of computing systems that address security concerns. This course aims to introduce the rigorous methodology that underlies the design of such systems. Topics include: * Computational foundations: Average-case hardness in NP, one-way functions * Pseudo-random number generators and pseudo-random functions * Zero-knowledge proofs and arguments * Generic protocols for secure multi-party computation * Trap-door permutations and public-key encryption * Black-box separations among cryptographic primitives

現代密碼學理論研究關於安全性的建模與構造安全計算系統方面的問題。本科旨在介紹設計這類系統的嚴謹的方法學。內容包括： *計算基礎：NP問題的平均複雜性，單向函數 *偽隨機數生成器和偽隨機函數 *零知識證明系統與論言 *安全多方計算的通用協議 *陷阱門置換和公鑰系統 *密碼原語間的黑盒式分離

Grade Descriptor:

A

EXCELLENT – exceptionally good performance and far exceeding expectation in all or most of the course learning outcomes; demonstration of superior understanding of the subject matter, the ability to analyze problems and apply extensive knowledge, and skillful use of concepts and materials to derive proper solutions.

有關等級說明的資料，請參閱英文版本。

B

GOOD – good performance in all course learning outcomes and exceeding expectation in some of them; demonstration of good understanding of the subject matter and the ability to use proper concepts and materials to solve most of the problems encountered.

有關等級說明的資料，請參閱英文版本。

C

FAIR – adequate performance and meeting expectation in all course learning outcomes; demonstration of adequate understanding of the subject matter and the ability to solve simple problems.

有關等級說明的資料，請參閱英文版本。

D

MARGINAL – performance barely meets the expectation in the essential course learning outcomes; demonstration of partial understanding of the subject matter and the ability to solve simple problems.

有關等級說明的資料，請參閱英文版本。

F

FAILURE – performance does not meet the expectation in the essential course learning outcomes; demonstration of serious deficiencies and the need to retake the course.

有關等級說明的資料，請參閱英文版本。

Equivalent Offering:
Units: 3 (Min) / 3 (Max) / 3 (Acad Progress)
Grading Basis: Graded
Repeat for Credit: N
Multiple Enroll: N
Course Attributes: MSc Computer Science
MPhil-PhD Computer Sci & Erg

Topics:

COURSE OUTCOMES

Learning Outcomes:

Modern cryptography is the rigorous foundation of the security of all computer systems. After completing the course students should:
- Be able to understand and produce cryptographic proofs of security, and to discover gaps in incomplete proofs.
- Understand the strengths and weaknesses of the computational assumptions that underlie different cryptographic primitives, and the relations among these assumptions.
- Know how to apply basic building blocks (e.g., pseudo-random generators, zero-knowledge arguments) in constructing more complex

cryptographic functionalities.

Course Syllabus:

The modern theory of cryptography studies the formal modelling and construction of computing systems that address security concerns. This course aims to introduce the rigorous methodology that underlies the design of such systems. Topics include: * Computational foundations: Average-case hardness in NP, one-way functions * Pseudo-random number generators and pseudo-random functions * Zero-knowledge proofs and arguments * Generic protocols for secure multi-party computation * Trap-door permutations and public-key encryption * Black-box separations among cryptographic primitives.

Assessment Type:

Homework or assignment	: 30%
Project	: 40%
Short answer test or exam	: 30%

Feedback for Evaluation:

1. Quiz and examinations
2. Course evaluation and questionnaire
3. Question-and-answer sessions during class
4. Student consultation during office hours or online

Required Readings:

To be provided by course teacher.

Recommended Readings:

Jonathan Katz and Yehuda Lindell. Introduction to Modern Cryptography. Chapman & Hall / CRC, 2007.
Oded Goldreich. Foundations of Cryptography, volume 1: Basic Tools. Cambridge University Press, 2001.
Oded Goldreich. Foundations of Cryptography, volume 2: Basic Applications. Cambridge University Press, 2004.
Ronald Cramer, Ivan Damgard, and Jesper Buus Nielsen. Secure multiparty computation and secret sharing. Cambridge University Press, 2015.
Tutorials on the Foundations of Cryptography, Yehuda Lindell (editor).
Rafael Pass and abhi shelat. A course in cryptography.
Dan Boneh and Victor Shoup. A graduate course in applied cryptography.

OFFERINGS

1. CSCI5440 Acad Organization=CSEGV; Acad Career=RPG

COMPONENTS

LEC : Size=30; Final Exam=Y; Contact=3

ENROLMENT REQUIREMENTS

1. CSCI5440

Enrollment Requirement Group:

For students in MSc Computer Science; or
For students in MPhil-PhD Computer Science & Engineering; or
For undergraduate students in Computer Science (CSCIU & CSCIN) or Computer Engineering (CENGU & CENGN)

CAF

< E N D O F R E P O R T >