Undergraduate Program

Course Title Cryptography and Computer Security

Mahidol University International College

Course Code EGCI 476

Division Science

TQF 3 Course Specifications

Section 1 General Information

1. Course code and course title

Thai EGCI 476 วิทยาการรหัสลับและความมั่นคงคอมพิวเตอร์

English EGCI 476 Cryptography and Computer Security

2. Number of credits 4 Credits

3. Program and type of subject

3.1 Program Bachelor of Engineering (Computer Engineering)

3.2 Type of Subject Major elective course

4. Course Coordinator and Course Lecturer

4.1 Course Coordinator Dr. Mingmanas Sivaraksa

4.2 Course Lecturer Dr. Vasin Suttichaya

5. Trimester/ Year of Study

5.1 Trimester Second trimester / for 4th year Computer Engineering

5.2 Course Capacity Approximately 25 students

6. Pre-requisite N/A

7. Co-requisites N/A

8. Venue of Study Mahidol University, Salaya campus

Section 2 Goals and Objectives

1. Course Goals

This course focuses towards the introduction of cryptography and network security using various cryptographic algorithms. Topics include Foundations of cryptography, Encryption/decryption algorithms, Zero-knowledge proofs, and Cryptographic protocols. After finish this course, student should be able to analyze, design, and evaluate various types of cryptographic applications.

2. Objectives of Course Development/Revision

2.1 Course Objectives

1. To develop the principle knowledge about cryptographic primitives.
2. To develop the fluency in using mathematical tools for analyzing, designing, and evaluating cryptographic primitives.
3. To develop skills needed in order to analyze and design cryptographic mechanism to prevent threats in computer network.

2.2 Course-level Learning Outcomes: CLOs

By the end of the course, students will be able to (CLOs)

1. CLO1 Explain the principle of cryptography.
2. CLO2 Show steps and procedure to analyze, design, and evaluate cryptographic primitives
3. CLO3 Apply the principle of cryptography to analyze and design cryptographic mechanism to prevent threats in computer network.

Section 3 Course Management

1. Course Description

(Thai) แนะนำทฤษฎีพื้นฐานและกลวิธีในการเข้ารหัสลับ ฟังก์ชันทางเดียว การเข้ารหัสแบบสมมาตรและอสมมาตร กลวิธีการวิเคราะห์การเข้ารหัสและถอดรหัส การยืนยันธุรกรรมโดยไม่เปิดเผยข้อมูล โพรโตคอลการเข้ารหัส

(English) Introduction to basic theory and techniques in cryptography, Symmetric and Asymmetric encryption, cryptanalysis techniques, Zero-knowledge proofs, and Cryptographic protocols.

2. Credit hours per trimester

Lecture (Hour(s))	Laboratory/field trip/internship (Hour(s))	Self-study (Hour(s))
48 hours (4 hours x 12 weeks)	-	96 hours (8 hours x 12 weeks)

3. Number of hours that the lecturer provides individual counseling and guidance.

1 hours/week

Section 4 Development of Students' Learning Outcome

1. Short summary on the knowledge or skills that the course intends to develop in students (CLOs)

By the end of the course, students will be able to

1. CLO1 Explain the principle of cryptography.
2. CLO2 Show steps and procedure to analyze, design, and evaluate cryptographic primitives
3. CLO3 Apply the principle of cryptography to analyze and design cryptographic mechanism to prevent threats in computer network.

2. Teaching methods for developing the knowledge or skills specified in item 1 and evaluation methods of the course learning outcomes

Course Code	Teaching methods	Evaluation Methods
CLO1	Interactive Lecture, Individual Assignment	Written Examination , Individual Evaluation
CLO2	Interactive Lecture, Individual Assignment	Written Examination , Individual Evaluation
CLO3	Interactive Lecture, Individual Assignment	Written Examination , Individual Evaluation

Section 5 Teaching and Evaluation Plans

1. Teaching plan

Week	Topic	Number of Hours		Teaching Activities/ Media	Lecturer
		Lecture Hours	Lab/Field Trip/Internship Hours		
1-2	Mathematics for cryptography	8	0	Interactive Lecture, Individual Assignment	Dr. Vasin Suttichaya
3	Principle of cryptography and network security	4	0		
4-5	One-way functions	8	0		
6	Pseudorandom generators	4	0		
7	Examination	2	0		Midterm Assessment
7-8	Encryption algorithms	6	0	Interactive Lecture, Individual Assignment	Dr. Vasin Suttichaya
9-10	Zero-knowledge proof	8	0		
11-12	Cryptographic protocols	8	0		
13	Examination				Final Assessment
	Total	48	0		

2. Plan for Assessing Course Learning Outcomes

2.1 Assessing and Evaluating Learning Achievement

a. Formative Assessment

The assessment tools such as homework, quizzes and exam are used to evaluate student's understanding by their ability to apply mathematical tools in order to design, analyze, and evaluate cryptographic components. The student should be able to explain the principle of cryptography and network security. The assessments are made through their homework, quizzes, and exams. The ability to analyze and evaluate the security of cryptographic components have to be shown by applying knowledge in probability, statistics, and discrete mathematics. The assessments are made through their homework, quizzes, and exams. The ability to analyze and design cryptographic mechanism have to be shown by applying knowledge in various cryptographic primitive to prevent threats in computer network. The assessments are made through their homework, quizzes, and exams.

b. Summative Assessment

(1) Tools and Percentage Weight in Assessment and Evaluation

Learning Outcomes	Assessment Methods	Assessment Ratio (Percentage)	
CLO1 Explain the principle of cryptography.	Homework	5	30
	Quiz	5	
	Midterm Exam	10	
	Final Exam	10	
CLO2 Show steps and procedure to analyze, design, and evaluate cryptographic primitives	Homework	5	40
	Quiz	5	
	Midterm Exam	15	
	Final Exam	15	
CLO3 Apply the principle of cryptography to analyze and design cryptographic mechanism to prevent	Homework	5	30
	Quiz	5	
	Midterm Exam	10	
	Final Exam	10	

threats in computer network.			
Total			100

(2) Grading System

Grade	Achievement	Final Score (% range)	GPA
A	Excellent	90-100	4.0
B+	Very Good	85-89	3.5
B	Good	80-84	3.0
C+	Fairly Good	75-79	2.5
C	Fair	70-74	2.0
D+	Poor	65-69	1.5
D	Very Poor	60-64	1.0
F	Fail	Less than 60	0.0

(3) Re-examination (If course lecturer allows to have re-examination)

N/A - (Not applicable with MUIC)

3. Student Appeals

The student wishing to appeal according to grading result must submit a written and signed appeal form personally to the academic affair unit. It is prohibited to assign another person to appeal on one’s behalf. The written appeal form is then sent to the program director and chair of department. The final decision is transferred for approval by the faculty committee. The result of appeal then is informed to the student.

Section 6 Teaching Materials and Resources

1. Textbooks and/or other documents/materials

    1) W. Stallings, “Cryptography and Network Security: Principles and Practice”, Pearson, 7th edition, 2016.

    2) B. A. Forouzan, “Cryptography and Network Securit”, McGraw Hill, 3rd edition, 2015.

2. Recommended textbooks and/or other documents/materials

    1) O. Goldreich, “Foundations of Cryptography – A Primer”, Foundations and Trends in Theoretical Computer Science 1(1) (2005)

3. Other Resources (If any)

    None

Section 7 Evaluation and Improvement of Course Management

1. Strategies for evaluating course effectiveness by students

    1.1 Evaluation of peers by students

    1.2 Student evaluation

    1.2.1 Course content

    1.2.2 Course management

    1.2.3 Suggestions

    1.2.4 Overall opinion

2. Strategies for evaluating teaching methods

    2.1 Student evaluation

    2.2 Presentation

3. Improvement of teaching methods

    Use evaluation from 1 and 2 for course improvement

4. Verification process for evaluating students’ standard achievement outcomes in the course

    Analysis of students’ learning outcomes using scores from each CLOs for evaluation.

5. Review and plan for improving the effectiveness of the course

    Review the course before trimester starts, before each teaching period and review course contents every 3 years.

Appendix

Alignment between Courses and Program

Table 1 The relationship between course and Program Learning Outcomes (PLOs)

Cryptography and Computer Security	Program Learning Outcomes (PLOs)					
	PLO1	PLO2	PLO3	PLO4	PLO5	PLO6
EGCI 476	M					R

Table 2 The relationship between CLOs and PLOs

EGCI 201	PLOs					
	PLO1	PLO2	PLO3	PLO4	PLO5	PLO6
CLO1 Explain the principle of cryptography.	x					x
CLO2 Show steps and procedure to analyze, design, and evaluate cryptographic primitives	x					x
CLO3 Apply the principle of cryptography to analyze and design cryptographic mechanism to prevent threats in computer network.	x					x

Table 3 The description of PLOs and Sub Los of the course

PLOs	SubPLOs
PLO1: Analyze ethical impacts of computer usage to personals, organizations social, and the rights and value of others	1.3 Show responsibilities in their work with on time submission without plagiarism or fabrication of work
PLO6: Create a related computer engineering development based on information technologies in mathematics or applied statistics.	6.1 Use Choose information technology tools properly for computer engineering development 6.2 Create a related computer engineering development based on selected tools