Tamkang University Academic Year 108, 1st Semester Course Syllabus

Course Title	INTRODUCTION TO CRYPTOGRAPHY	Instructor	HWANG SHIN-JIA
Course Class	TEIBM1A MASTER'S PROGRAM, DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION ENGINEERING (ENGLISH-TAUGHT PROGRAM), 1A	Details	◆ Blended Course ◆ Selective ◆ One Semester ◆ 3 Credits

Departmental Aim of Education

Ⅰ. Cultivate the ability to conduct independent research and problem solving.

Ⅱ. Strengthen creativity and research capacity.

Ⅲ. Build profound professional knowledge in computer science and information engineering.

Ⅳ. Engage in self-directed lifelong learning.

Subject Departmental core competences

B. Independent innovative thinking ability.(ratio:50.00)

D. Research & development (R&D) ability in information engineering.(ratio:50.00)

Subject Schoolwide essential virtues

2. Information literacy. (ratio:60.00)

5. Independent thinking. (ratio:40.00)

Course Introduction	This course introduces cryptographic concepts, algorithms and protocols. The related security definition and proof are also introduced.

The correspondences between the course's instructional objectives and the cognitive, affective, and psychomotor objectives.

Differentiate the various objective methods among the cognitive, affective and psychomotor domains of the course's instructional objectives.

I. Cognitive : Emphasis upon the study of various kinds of knowledge in the cognition of the course's veracity, conception, procedures, outcomes, etc.

II.Affective : Emphasis upon the study of various kinds of knowledge in the course's appeal, morals, attitude, conviction, values, etc.

III.Psychomotor: Emphasis upon the study of the course's physical activity and technical manipulation.

No.	Teaching Objectives	objective methods
1	Introduction concepts of cryptogrpahy.	Cognitive
2	Introduce cryptographic algorithms and protocols.	Cognitive
3	Introduce the recent results about cryptography.	Psychomotor

The correspondences of teaching objectives : core competences, essential virtues, teaching methods, and assessment

No.	Core Competences	Essential Virtues	Teaching Methods	Assessment
1	BD	25	Lecture	Testing
2	BD	25	Lecture	Testing
3	BD	25	Lecture	Testing

Course Schedule

Note for Blended Course : When utilizing weekly digital instruction, please fill in "Online Asynchronous Instruction".

Week	Date	Course Contents	Note
1	108/09/09 ~ 108/09/15	Course Introduction and Ch 01 Computer and Network Security Concepts	
2	108/09/16 ~ 108/09/22	Ch 3 Classic Encryption Techniques (3.1-3.3)+4.1 Traditional Block Cipher and Ch 7 Block Cipher Operations	線上非同步教學
3	108/09/23 ~ 108/09/29	Ch 2 Number Theory	線上非同步教學
4	108/09/30 ~ 108/10/06	Ch 2 Number Theory	
5	108/10/07 ~ 108/10/13	Test1	
6	108/10/14 ~ 108/10/20	Ch 5 Finite Fields	
7	108/10/21 ~ 108/10/27	Ch 5 Finite Fields	

8	108/10/28 ~ 108/11/03	Ch 9 Public Key Cryptography and RSA	
9	108/11/04 ~ 108/11/10	Middle Exam.	
10	108/11/11 ~ 108/11/17	Ch 9 Public Key Cryptography and RSA	
11	108/11/18 ~ 108/11/24	Ch 10 Other Public Key Cryptography	
12	108/11/25 ~ 108/12/01	Ch 13 Digital Signatures	線上非同步教學
13	108/12/02 ~ 108/12/08	Ch 13 Digital Signatures	線上非同步教學
14	108/12/09 ~ 108/12/15	Test 2	
15	108/12/16 ~ 108/12/22	Ch 11 Cryptography Hash Functions	學生上台報告
16	108/12/23 ~ 108/12/29	Ch 14 Key Management and Distribution	學生上台報告。
17	108/12/30 ~ 109/01/05	Ch 15 User Authentication	學生上台報告。
18	109/01/06 ~ 109/01/12	期末報告	

Requirement	1. All students have to attend tests and exam. The unattended students with irresistible reasons are required to show the legal proof of your reasons in one week after the attendance check. With legal proof, the unattended record can be canceled and the make-up test will be held. 2. Your scores are made public on iClass website. 3. The result of the final exam. is made public during 3 to 5 days after the final exam. in our iClass website. 4. If you are absent about your (group) oral presentation, the presentation score will be 0.
Teaching Facility	Computer, Projector
Textbooks and Teaching Materials	Cryptography and Network Security: Principles and Practice (7th Edition), William Stallings, Pearson, 2016.
References	"Handbook of Applied Cryptography," Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, CRC Press, 2001
Number of Assignment(s)	(Filled in by assignment instructor only)
Grading Policy	◆ Attendance： 10.0 % ◆ Mark of Usual：40.0 % ◆ Midterm Exam： 25.0 % ◆ Final Exam： % ◆ Other〈Final Oral Report〉：25.0 %

Note	1. This syllabus may be uploaded at the website of the Course Syllabus Management System at https://info.ais.tku.edu.tw/csp or through the link of the Course Syllabus Upload posted on the home page of the TKU Office of Academic Affairs http://www.acad.tku.edu.tw/CS/main.php 2. According to the Implementation regulations of distance education for junior college and above are prescribed pursuant to Article 2, "The distance learning course referred to in these Measures refers to more than one-half of the teaching hours in each subject." 3. According to the regulations of Tamkang University Enforcement Rules for digital teaching, Paragraph 2 and Article 3, the distance learning course of our school must be "The course of digital teaching with distance learning platform or synchronous video system in our school. Teaching Hours include course lectures, teacher-student interaction discussions, quizzes and other learning activities." 4. If there are any temporary course changes (including time changes and classroom changes of distance learning courses, blended courses), please make out an application according to regulations to the Office of Academic Affairs. **※ Unauthorized photocopying is illegal. Using original textbooks is advised. It is a crime to improperly photocopy others' publications.**