Tamkang University Academic Year 107, 1st Semester Course Syllabus

Course Title	CRYPTOGRAPHIC ALGORITHMS	Instructor	HWANG SHIN-JIA
Course Class	TEIBM1A MASTER'S PROGRAM, DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION ENGINEERING (ENGLISH-TAUGHT PROGRAM), 1A	Details	◆ 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.

Departmental core competences

A. Independent problem solving ability.

B. Independent innovative thinking ability.

C. Research paper writing and presentation ability.

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

E. Project execution and control ability.

F. Lifelong self-directed learning ability.

Course Introduction	This course introduce cryptographic algorithms and protocols. The related security defintion and proof are also introduced.

The Relevance among Teaching Objectives, Objective Levels and Departmental core competences

I.Objective Levels (select applicable ones) :

(i) Cognitive Domain : C1-Remembering, C2-Understanding, C3-Applying, C4-Analyzing, C5-Evaluating, C6-Creating

(ii) Psychomotor Domain : P1-Imitation, P2-Mechanism, P3-Independent Operation, P4-Linked Operation, P5-Automation, P6-Origination

(iii) Affective Domain : A1-Receiving, A2-Responding, A3-Valuing, A4-Organizing, A5-Charaterizing, A6-Implementing

II.The Relevance among Teaching Objectives, Objective Levels and Departmental core competences :

(i) Determine the objective level(s) in any one of the three learning domains (cognitive, psychomotor, and affective) corresponding to the teaching objective. Each objective should correspond to the objective level(s) of ONLY ONE of the three domains.

(ii) If more than one objective levels are applicable for each learning domain, select the highest one only. (For example, if the objective levels for Cognitive Domain include C3,C5,and C6, select C6 only and fill it in the boxes below. The same rule applies to Psychomotor Domain and Affective Domain.)

(iii) Determine the Departmental core competences that correspond to each teaching objective. Each objective may correspond to one or more Departmental core competences at a time. (For example, if one objective corresponds to three Departmental core competences: A,AD, and BEF, list all of the three in the box.)

No.	Teaching Objectives	Relevance	
		Objective Levels	Departmental core competences
1	Introduction concepts of cryptogrpahy.	C4	AB
2	Introduce cryptographic algorithms and protocols.	C4	AB
3	Introduce the recent results about cryptography.	P5	AB

Teaching Objectives, Teaching Methods and Assessment

No.	Teaching Objectives	Teaching Methods	Assessment
1	Introduction concepts of cryptogrpahy.	Lecture	Written test, Participation
2	Introduce cryptographic algorithms and protocols.	Lecture	Written test, Participation
3	Introduce the recent results about cryptography.	Lecture	Written test

This course has been designed to cultivate the following essential qualities in TKU students	
Essential Qualities of TKU Students	Description
◇ A global perspective	Helping students develop a broader perspective from which to understand international affairs and global development.
◆ Information literacy	Becoming adept at using information technology and learning the proper way to process information.
◇ A vision for the future	Understanding self-growth, social change, and technological development so as to gain the skills necessary to bring about one's future vision.
◇ Moral integrity	Learning how to interact with others, practicing empathy and caring for others, and constructing moral principles with which to solve ethical problems.
◆ Independent thinking	Encouraging students to keenly observe and seek out the source of their problems, and to think logically and critically.
◇ A cheerful attitude and healthy lifestyle	Raising an awareness of the fine balance between one's body and soul and the environment; helping students live a meaningful life.
◇ A spirit of teamwork and dedication	Improving one's ability to communicate and cooperate so as to integrate resources, collaborate with others, and solve problems.
◇ A sense of aesthetic appreciation	Equipping students with the ability to sense and appreciate aesthetic beauty, to express themselves clearly, and to enjoy the creative process.

Course Schedule

Week	Date	Subject/Topics	Note
1	107/09/10 ~ 107/09/16	Course Introduction and Ch 01 Computer and Network Security Concepts	
2	107/09/17 ~ 107/09/23	Ch 2 Number Theory	
3	107/09/24 ~ 107/09/30	Ch 2 Number Theory	
4	107/10/01 ~ 107/10/07	Ch 5 Finite Fields	
5	107/10/08 ~ 107/10/14	Ch 5 Finite Fields	
6	107/10/15 ~ 107/10/21	TEST1	
7	107/10/22 ~ 107/10/28	4.1 Traditional Block Cipher and Ch 7 Block Cipher Operations	
8	107/10/29 ~ 107/11/04	Ch 9 Public Key Cryptography and RSA	
9	107/11/05 ~ 107/11/11	Middle Exam.	
10	107/11/12 ~ 107/11/18	Ch 10 Other Public Key Cryptography	
11	107/11/19 ~ 107/11/25	Ch 11 Cryptography Hash Functions	
12	107/11/26 ~ 107/12/02	Ch 13 Digital Signatures	

13	107/12/03～ 107/12/09	Ch 13 Digital Signatures	
14	107/12/10～ 107/12/16	Test2	
15	107/12/17～ 107/12/23	Ch 14 Key Management and Distribution	
16	107/12/24～ 107/12/30	Ch 15 User Authenation	
17	107/12/31～ 108/01/06	Final Exam.	
18	108/01/07～ 108/01/13	期末報告	

Requirement	
Teaching Facility	Computer, Projector
Textbook(s)	Cryptography and Network Security: Principles and Practice (7th Edition), William Stallings, Pearson, 2016.
Reference(s)	"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： 25.0 % ◆ Other〈 〉： %
Note	This syllabus may be uploaded at the website of Course Syllabus Management System at http://info.ais.tku.edu.tw/csp or through the link of Course Syllabus Upload posted on the home page of TKU Office of Academic Affairs at http://www.acad.tku.edu.tw/CS/main.php . **※ Unauthorized photocopying is illegal. Using original textbooks is advised. It is a crime to improperly photocopy others' publications.**