

## Tamkang University Academic Year 103, 2nd Semester Course Syllabus

Course Title	CRYPTOGRAPHIC ALGORITHMS	Instructor	HWANG SHIN-JIA
Course Class	TEIBM1A ENGLISH MASTER'S PROGRAM, DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION ENGINEERING, 1A	Details	<ul style="list-style-type: none"> <li>◆ Selective</li> <li>◆ One Semester</li> <li>◆ 3 Credits</li> </ul>
D e p a r t m e n t a l   A i m   o f   E d u c a t i o n			
<p>I. Cultivate the ability to conduct independent research and problem solving.</p> <p>II. Strengthen creativity and research capacity.</p> <p>III. Build profound professional knowledge in computer science and information engineering.</p> <p>IV. Engage in self-directed lifelong learning.</p>			
D e p a r t m e n t a l   c o r e   c o m p e t e n c e s			
<p>A. Independent problem solving ability.</p> <p>B. Independent innovative thinking ability.</p> <p>C. Research paper writing and presentation ability.</p> <p>D. Research &amp; development (R&amp;D) ability in information engineering.</p> <p>E. Project execution and control ability.</p> <p>F. Lifelong self-directed learning ability.</p>			
Course Introduction	<p>This course briefly introduces some algorithms in Cryptography. During the introduction of those algorithms, the related mathmatic background and computation theory are also introduced.</p>		

**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	Mathematic Learning	C3	AD
2	Learning cryptogapic algorithms and cryptographic thinging.	C4	AB
3	Understanding Computation Theory.	C3	A

**Teaching Objectives, Teaching Methods and Assessment**

No.	Teaching Objectives	Teaching Methods	Assessment
1	Mathematic Learning	Lecture, Problem solving	Participation
2	Learning cryptogapic algorithms and cryptographic thinging.	Lecture, Discussion, Problem solving	Written test, Participation
3	Understanding Computation Theory.	Lecture, Discussion	Participation

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	104/02/24 ~ 104/03/01	Course Introduction, Overview of Cryptography and Its Applications	
2	104/03/02 ~ 104/03/08	Overview of Cryptography and Its Applications	
3	104/03/09 ~ 104/03/15	Basic Number Theory	
4	104/03/16 ~ 104/03/22	Basic Number Theory	
5	104/03/23 ~ 104/03/29	RSA Algorithm	
6	104/03/30 ~ 104/04/05	RSA Algorithm	
7	104/04/06 ~ 104/04/12	RSA Algorithm	
8	104/04/13 ~ 104/04/19	Discrete Logarithms	
9	104/04/20 ~ 104/04/26	Discrete Logarithms	
10	104/04/27 ~ 104/05/03	Mid Exam.	
11	104/05/04 ~ 104/05/10	Hash Functions	
12	104/05/11 ~ 104/05/17	Hash Functions	

13	104/05/18 ~ 104/05/24	Digital Signatures	
14	104/05/25 ~ 104/05/31	Digital Signatures	
15	104/06/01 ~ 104/06/07	Security Protocols	
16	104/06/08 ~ 104/06/14	Security Protocols	
17	104/06/15 ~ 104/06/21	Secret Sharing	
18	104/06/22 ~ 104/06/28	Final Exam.	
Requirement			
Teaching Facility	Computer, Projector		
Textbook(s)	Introduction to Cryptography with Coding Theory, 2nd Ed., Trappe and Washington, 2006.		
Reference(s)	Introduction to Cryptography with Maple, Pardo, 2014.		
Number of Assignment(s)	(Filled in by assignment instructor only)		
Grading Policy	◆ Attendance : 10.0 %   ◆ Mark of Usual : 25.0 %   ◆ Midterm Exam : 20.0 % ◆ Final Exam : 25.0 % ◆ Other <Discussions> : 20.0 %		
Note	This syllabus may be uploaded at the website of Course Syllabus Management System at <a href="http://info.ais.tku.edu.tw/csp">http://info.ais.tku.edu.tw/csp</a> or through the link of Course Syllabus Upload posted on the home page of TKU Office of Academic Affairs at <a href="http://www.acad.tku.edu.tw/CS/main.php">http://www.acad.tku.edu.tw/CS/main.php</a> . <b>※ Unauthorized photocopying is illegal. Using original textbooks is advised. It is a crime to improperly photocopy others' publications.</b>		