Tamkang University Academic Year 111, 2nd Semester Course Syllabus

Course Title	CRYPTOLOGY	Instructor	YAO CHENG
Course Class	TSMAB4A DEPARTMENT OF MATHEMATICS (SECTION OF MATHEMATICS), 4A	Details	◆ General Course ◆ Selective ◆ One Semester
Relevance to SDGs	SDG4 Quality education		

Departmental Aim of Education

Ⅰ. To teach knowledge in mathematics.

Ⅱ. To train teaching professionals in mathematics.

Ⅲ. To develop independent and creative thinking.

Ⅳ. To establish ability to present oneself.

Ⅴ. To promote cooperative working spirit.

Ⅵ. To prepare self learning ability in multiple areas.

Subject Departmental core competences

A. To learn the fundamentals of mathematics.(ratio:10.00)

B. To develop independent and logical thinking ability.(ratio:30.00)

C. To learn basics of probability and statistic.(ratio:20.00)

D. To use the aid of computer in solving mathematical and statistical problems.(ratio:20.00)

E. To obtain the ability to collect and analyze data.(ratio:10.00)

F. To establish ability to pursue knowledge in advanced mathematics.(ratio:10.00)

Subject Schoolwide essential virtues

1. A global perspective. (ratio:10.00)

2. Information literacy. (ratio:20.00)

3. A vision for the future. (ratio:10.00)

4. Moral integrity. (ratio:10.00)

5. Independent thinking. (ratio:20.00)

6. A cheerful attitude and healthy lifestyle. (ratio:5.00)

7. A spirit of teamwork and dedication. (ratio:15.00)

8. A sense of aesthetic appreciation. (ratio:10.00)

Course Introduction	This course will cover the following topics: (1)Elementary concepts in number theory such as Euclidean algorithm and congruence. (2)Introduction to cryptography and RAS system. (3)Error-correcting code and quantum algorithm.

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	The aim of this course is to give an elementary introduction to the cryptography	Cognitive

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

No.	Core Competences	Essential Virtues	Teaching Methods	Assessment
1	ABCDEF	12345678	Lecture, Discussion	Testing, Study Assignments, Report(including oral and written)

Course Schedule

Week	Date	Course Contents	Note
1	112/02/13 ~ 112/02/19	Introduction to cryptography	
2	112/02/20 ~ 112/02/26	Elementary number theory	
3	112/02/27 ~ 112/03/05	O and Omega notation, cost of multiplication, addition and division with remainder	

4	112/03/06 ~ 112/03/12	Cryptosystems	
5	112/03/13 ~ 112/03/19	Block Ciphers	
6	112/03/20 ~ 112/03/26	Identification problem	
7	112/03/27 ~ 112/04/02	Perfect secrecy	
8	112/04/03 ~ 112/04/09	DES and AES	
9	112/04/10 ~ 112/04/16	Public key encryption	
10	112/04/17 ~ 112/04/23	Midterm Exam Week	
11	112/04/24 ~ 112/04/30	RSA	
12	112/05/01 ~ 112/05/07	Decryption	
13	112/05/08 ~ 112/05/14	Shor's algorithm	
14	112/05/15 ~ 112/05/21	Diffie-Hellman key exchange	
15	112/05/22 ~ 112/05/28	Graduate Exam Week	
16	112/05/29 ~ 112/06/04	---	
17	112/06/05 ~ 112/06/11	---	
18	112/06/12 ~ 112/06/18	---	

Requirement	
Teaching Facility	(None)
Textbooks and Teaching Materials	Introduction to cryptography by Johannes A. Bachmann, Second edition
References	
Number of Assignment(s)	(Filled in by assignment instructor only)
Grading Policy	◆ Attendance： 20.0 % ◆ Mark of Usual：20.0 % ◆ Midterm Exam： 30.0 % ◆ Final Exam： 30.0 % ◆ 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.**