



教學計劃表 Syllabus

課程名稱(中文) Course Name in Chinese	代數專題(一)		學年/學期 Academic Year/Semester	114/2
課程名稱(英文) Course Name in English	Topics in Algebra (I)			
科目代碼 Course Code	AM_53500	系級 Department & Year	碩士	開課單位 Course-Offering Department
修別 Type	選修 Elective	學分數/時間 Credit(s)/Hour(s)	3.0/3.0	
授課教師 Instructor	/王立中			
先修課程 Prerequisite				
課程描述 Course Description				
The course will introduce background knowledge in multivariate cryptography, encompassing fundamental topics such as linear algebra, finite fields, multivariate polynomials, and related algebraic foundations. Instruction will include hands-on training in implementation and computational experimentation using the open-source mathematical software SageMath.				
課程目標 Course Objectives				
研習基本代數結構，以訓練學生處理複雜問題的簡化能力。 To study basic algebraic structures to train the students to have the ability to simplify and reduce complicated problems.				
系專業能力 Basic Learning Outcomes				課程目標與系專業能力相關性 Correlation between Course Objectives and Dept.'s Education Objectives
A	具備專業數學知識及邏輯推理能力。Have well-founded expertise in mathematics and be capable of logical reasoning.			●
B	具備學習其它學科的能力，以期能邁向跨領域研究。Be able to study other fields of science so as to conduct interdisciplinary research in the future			○
C	具備獨立思考與解決問題的能力。Be capable of independent thinking and have the problem-solving skills.			●
圖示說明 Illustration : ● 高度相關 Highly correlated ○ 中度相關 Moderately correlated				
授課進度表 Teaching Schedule & Content				
週次 Week	內容 Subject/Topics			備註 Remarks
1	2/27補假、2/28和平紀念日			
2	SageMath 安裝			
3	SageMath 介紹			
4	multivariate cryptography 介紹			
5	multivariate cryptography			
6	春假			
7	UOV variants			

8	attacks of uov variants	
9	期中考試週 Midterm Exam implementation of complexity estimate of attacks	
10	勞動節	
11	attacks of uov variants	
12	implementation of complexity estimate of attacks	
13	attacks of uov variants	
14	implementation of complexity estimate of attacks	
15	attacks of uov variants	
16	implementation of complexity estimate of attacks	
17	端午節	
18	期末考試週 Final Exam	

教學策略 Teaching Strategies

- 課堂講授 Lecture
 分組討論 Group Discussion
 參觀實習 Field Trip
 其他 Miscellaneous:

教學創新自評 Teaching Self-Evaluation

創新教學 (Innovative Teaching)

- 問題導向學習 (PBL)
 團體合作學習 (TBL)
 解決導向學習 (SBL)
 翻轉教室 Flipped Classroom
 磨課師 Moocs

社會責任 (Social Responsibility)

- 在地實踐 Community Practice
 產學合作 Industry-Academia Cooperation

跨域合作 (Transdisciplinary Projects)

- 跨界教學 Transdisciplinary Teaching
 跨院系教學 Inter-collegiate Teaching

- 業師合授 Courses Co-taught with Industry Practitioners

其它 other:

學期成績計算及多元評量方式 Grading & Assessments

配分項目 Items	配分比例 Percentage	多元評量方式 Assessments							
		測驗 會考	實作 觀察	口頭 發表	專題 研究	創作 展演	卷宗 評量	證照 檢定	其他
平時成績(含出缺席) General Performance (Attendance Record)	50%								
期中考成績 Midterm Exam									
期末考成績 Final Exam									
作業成績 Homework and/or Assignments	50%								
其他 Miscellaneous (_____)									

評量方式補充說明

Grading & Assessments Supplemental instructions

教科書與參考書目 (書名、作者、書局、代理商、說明)

Textbook & Other References (Title, Author, Publisher, Agents, Remarks, etc.)

課程教材網址(含線上教學資訊, 教師個人網址請列位於本校內之網址)

Teaching Aids & Teacher's Website(Including online teaching information.
Personal website can be listed here.)

其他補充說明 (Supplemental instructions)