淡江大學１０８學年度第２學期課程教學計畫表

課程名稱	密碼數學 MATHEMATICS FOR CRYPTOGRAPHY	授課教師	黃心嘉 HWANG SHIN-JIA
開課系級	資工一碩士班Ａ TEIXM1A	開課資料	實體課程 選修 單學期 3學分

系（ 所） 教 育 目 標

一、培養獨立研究解決問題。

二、提昇研發能量創意設計。

三、厚植資訊工程專業知能。

四、養成自發自主終生學習。

本課程對應院、系(所)核心能力之項目與比重

A. 獨立解決問題能力。(比重：50.00)

D. 資訊工程研發能力。(比重：50.00)

本課程對應校級基本素養之項目與比重

2. 資訊運用。(比重：50.00)

5. 獨立思考。(比重：50.00)

課程簡介	本課程的目的在提供密碼學與安全基礎的數學背景, 介紹主題涵蓋數論、近代代數、機率與資訊理論、以及在密碼學與安全的應用。
	The purpose of this course is to give the fundamental mathematical background for cryptography and security. The topics of this course include number theory, modern algebra, probability and information theory, security definition, and the applications on cryptography and security.

本課程教學目標與認知、情意、技能目標之對應

將課程教學目標分別對應「認知（Cognitive）」、「情意（Affective）」與「技能(Psychomotor)」的各目標類型。

一、認知(Cognitive)：著重在該科目的事實、概念、程序、後設認知等各類知識之學習。
二、情意(Affective)：著重在該科目的興趣、倫理、態度、信念、價值觀等之學習。
三、技能(Psychomotor)：著重在該科目的肢體動作或技術操作之學習。

序號	教學目標(中文)	教學目標(英文)
1	學生學習數論、近代代數、機率等相關基本數學背景，並透過口頭報告與討論進一步學習。	Students learn the fundamantal mathematical background, including number theory, modern algebra, and probability. Through the oral reports and discussions to enhance depth of students' studies.
2	學生學習密碼學與資訊安全的基本理論應用，並透過口頭報告與討論進一步學習。	Students leans appliaciotns of the fundamental background on cryptography and infromation security. Through the oral reports and discussions to enhance depth of students' studies.
3	概觀性介紹資訊安全與密碼學的安全性定義。	Briefly introduction about the security defintion in security and cryptography.

教學目標之目標類型、核心能力、基本素養教學方法與評量方式

序號	目標類型	院、系(所)核心能力	校級基本素養	教學方法	評量方式
1	技能	AD	25	講述、討論	測驗
2	技能	AD	25	講述、討論	測驗
3	認知	AD	25	講述、討論	測驗

授 課 進 度 表

週次	日期起訖	內 容 (Subject/Topics)	備註
1	109/03/02～109/03/08	課程介紹與參考文獻格式	
2	109/03/09～109/03/15	Ch 1 Introduction to Cryptography and Data Security (Pelzl)	
3	109/03/16～109/03/22	論文報告+ Ch 1 Modular Arithmetic, Groups, Finite Fields, and Probability (Smart)	
4	109/03/23～109/03/29	論文報告+ Ch 1 Modular Arithmetic, Groups, Finite Fields, and Probability (Smart)	
5	109/03/30～109/04/05	論文報告+ Ch 1 Modular Arithmetic, Groups, Finite Fields, and Probability (Smart)	
6	109/04/06～109/04/12	論文報告+ Chapter 9. Information-Theoretic Security (Smart)	
7	109/04/13～109/04/19	論文報告+ Chapter 9. Information-Theoretic Security (Smart)	

8	109/04/20～ 109/04/26	論文報告+ Chapter 9. Information-Theoretic Security (Smart)	
9	109/04/27～ 109/05/03	期中考 (Chapter 9. Information-Theoretic Security (Smart))	
10	109/05/04～ 109/05/10	機器或深度學習短期課程	
11	109/05/11～ 109/05/17	Chapter 11. Defining Security (Smart)	線上非同步課程
12	109/05/18～ 109/05/24	Chapter 11. Defining Security (Smart)	線上非同步課程
13	109/05/25～ 109/05/31	Chapter 11. Defining Security (Smart)	線上非同步課程
14	109/06/01～ 109/06/07	區塊鍊短期課程	
15	109/06/08～ 109/06/14	區塊鍊短期課程	
16	109/06/15～ 109/06/21	區塊鍊短期課程	
17	109/06/22～ 109/06/28	Chapter 16. Public Key Encryption and Signature (Smart)	
18	109/06/29～ 109/07/05	教師彈性補充教學： (Chapter 16. Public Key Encryption and Signature (smart))	線上非同步課程

修課應注意事項	1. 報告者不可以缺席請假, 若有不可避免因素, 請事先告知老師, 並與同學換報告日期。 2. 報告者自行研讀短期課程內容或是課本內容報告。非本實驗室修課同學請選與課本內容報告。 3. 投影片PPT或PDF檔需要報告日前三天給老師上傳。 4. 請把握時間在150分鐘內報告完畢。 5.尊重智慧財產權。
教學設備	電腦、投影機
教科書與教材	Understanding Cryptography: A Textbooks for Students and Practitioncers, Chrsitof Paar and Jan Pelzl, Springer, 2010. Cryptography Made Simple, Smart, Nigel P., Springer, 2016
參考文獻	Cryptography and Network Security: Principles and Practice, 5th Ed., William Stallings, Pearson, 2010. "Introduction to Cryptography: Principle and Applications," 2nd Ed., Hans Delfs and Helmut Knebl, New York: Springer-Verlag, 2007. "Protocols for Authentication and Key Establishment," Colin Boyd and Anish Mathuria, New York: Springer, 2003.
批改作業篇數	1 篇（本欄位僅適用於所授課程需批改作業之課程教師填寫）
學期成績計算方式	◆出席率： 20.0 % ◆平時評量： % ◆期中評量： % ◆期末評量： % ◆其他〈口頭報告〉：80.0 %

備　考	「教學計畫表管理系統」網址：https://info.ais.tku.edu.tw/csp 或由教務處首頁→教務資訊「教學計畫表管理系統」進入。 **※不法影印是違法的行為。請使用正版教科書，勿不法影印他人著作，以免觸法。**