淡江大學１１３學年度第２學期課程教學計畫表

課程名稱	密碼學 CRYPTOLOGY	授課教師	王千真 CHIAN-JEN WANG
開課系級	數學系四Ａ TSNXB4A	開課資料	實體課程 選修 單學期 3學分
課程與SDGs關聯性	SDG4 優質教育		

系（ 所 ） 教 育 目 標

一、專業知識傳授。

二、基礎教育人才養成。

三、獨力創新思維。

四、自我能力表現。

五、團隊合作精神。

六、多元自我學習。

本課程對應院、系(所)核心能力之項目與比重

A. 認知與理解數學的基礎知識。(比重：10.00)

B. 具備獨立與邏輯思考能力。(比重：30.00)

C. 理解機率，統計方面的基礎知識。(比重：20.00)

D. 具有利用電腦當輔助工具，解決數學及統計上的專業問題。(比重：20.00)

E. 具備資料蒐集與分析的知識。(比重：10.00)

F. 理解進階數學科學的能力。(比重：10.00)

本課程對應校級基本素養之項目與比重

1. 全球視野。(比重：10.00)
2. 資訊運用。(比重：20.00)
3. 洞悉未來。(比重：10.00)
4. 品德倫理。(比重：10.00)
5. 獨立思考。(比重：20.00)
6. 樂活健康。(比重：5.00)
7. 團隊合作。(比重：15.00)
8. 美學涵養。(比重：10.00)

課程簡介	本課程介紹現代密碼學的基本概念、技術以及數學基礎。課程將討論的主題包括離散對數問題、RSA 密碼系統、數位簽章、橢圓曲線密碼學等。
	This course introduces the fundamental concepts, techniques, and mathematical foundations of modern cryptography. Topics to be discussed include the discrete logarithm problem, the RSA cryptography, digital signatures, the elliptic curve cryptography, etc.

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	了解密碼學的數學基礎	Understand the mathematical foundations of cryptography.
2	了解密碼學的應用	Understand the applications of 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	認知	ABC	1234	講述、討論	測驗、作業
2	認知	DEF	5678	講述、討論	測驗、作業

授 課 進 度 表

週次	日期起訖	內 容 (Subject/Topics)	備註
1	114/02/17～114/02/23	Introduction to Cryptography	
2	114/02/24～114/03/02	Symmetric and Asymmetric Ciphers	
3	114/03/03～114/03/09	The Discrete Logarithm Problem	
4	114/03/10～114/03/16	Diffie-Hellman Key Exchange	
5	114/03/17～114/03/23	Integer Factorization and RSA	
6	114/03/24～114/03/30	Digital Signatures	

7	114/03/31～ 114/04/06	教學行政觀摩週	
8	114/04/07～ 114/04/13	The Vigenera Cipher	
9	114/04/14～ 114/04/20	期中考/期中評量週(老師得自行調整週次)	
10	114/04/21～ 114/04/27	The Birthday Paradox	
11	114/04/28～ 114/05/04	Pollard's Rho Method	
12	114/05/05～ 114/05/11	Elliptic Curves over Finite Fields	
13	114/05/12～ 114/05/18	Elliptic Curve Cryptography	
14	114/05/19～ 114/05/25	Bilinear Pairings on Elliptic Curves	
15	114/05/26～ 114/06/01	畢業考/畢業評量週(老師得自行調整週次)	
16	114/06/02～ 114/06/08		
17	114/06/09～ 114/06/15		
18	114/06/16～ 114/06/22		

課程培養關鍵能力	
跨領域課程	
特色教學課程	
課程教授內容	邏輯思考
修課應注意事項	
教科書與教材	採用他人教材:教科書 教材說明: An Introduction to Mathematical Cryptography, by Hoffstein, Pipher, and Silverman
參考文獻	

學期成績計算方式	◆出席率：　　％　◆平時評量：20.0　％　◆期中評量：40.0　％ ◆期末評量：40.0　％ ◆其他〈　〉：　　％
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。**