

淡江大學 110 學年度第 2 學期課程教學計畫表

課程名稱	密碼學	授課 教師	潘志實 ZHISHI PAN
	CRYPTOLOGY		
開課系級	數學系數學四 A	開課 資料	實體課程 選修 單學期 3學分
	TSMAB4A		
課程與SDGs 關聯性	SDG4 優質教育		
系（所）教育目標			
<p>一、專業知識傳授。</p> <p>二、基礎教育人才養成。</p> <p>三、獨力創新思維。</p> <p>四、自我能力表現。</p> <p>五、團隊合作精神。</p> <p>六、多元自我學習。</p>			
本課程對應院、系(所)核心能力之項目與比重			
<p>A. 認知與理解數學的基礎知識。(比重：60.00)</p> <p>B. 具備獨立與邏輯思考能力。(比重：40.00)</p>			
本課程對應校級基本素養之項目與比重			
<p>2. 資訊運用。(比重：50.00)</p> <p>5. 獨立思考。(比重：50.00)</p>			
課程簡介	<p>本課程主要介紹密碼學的演化過程。並學習加密解密的重要性，以及加密者和解密者相互較勁的情形。並讓學生學習密碼學在日常生活中的應用。</p>		
	<p>This course is an introduction to the topics on evolution of cryptology. And study the importance of encipher and decipher in communication, and the compeles between the encipherer and the decipher. And let student study the application of the cryptology in the daily life.</p>		

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	讓學生學習密碼學的演化。	Let students study the evolution of cryptology.
2	讓學生學習將訊息加密及解密的方法。	Let students study how to encipher and decipher a message.

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	AB	25	講述、討論	測驗、討論(含課堂、線上)
2	認知	AB	25	講述、討論	測驗、作業、討論(含課堂、線上)

授課進度表

週次	日期起訖	內容 (Subject/Topics)	備註
1	111/02/21~ 111/02/25	蘇格蘭瑪莉女王的密碼	
2	111/02/28~ 111/03/04	蘇格蘭瑪莉女王的密碼	
3	111/03/07~ 111/03/11	無法破解的密碼	
4	111/03/14~ 111/03/18	無法破解的密碼	
5	111/03/21~ 111/03/25	秘密書寫的機械化	
6	111/03/28~ 111/04/01	秘密書寫的機械化	
7	111/04/04~ 111/04/08	奇謎機	
8	111/04/11~ 111/04/15	破解"奇謎"	
9	111/04/18~ 111/04/22	破解"奇謎"	
10	111/04/25~ 111/04/29	期中考試週	
11	111/05/02~ 111/05/06	愛麗絲和巴伯公開鑰匙	
12	111/05/09~ 111/05/13	愛麗絲和巴伯公開鑰匙	

13	111/05/16~ 111/05/20	極佳隱私	
14	111/05/23~ 111/05/27	極佳隱私	
15	111/05/30~ 111/06/03	畢業考試週	
16	111/06/06~ 111/06/10	---	
17	111/06/13~ 111/06/17	---	
18	111/06/20~ 111/06/24	---	
修課應 注意事項	1. 請同學特別留意出席率。另外所有請假都必須事先告知(可用msteam傳訊息) 2. 請同學務必了解學期成績的計分方式。		
教學設備	電腦、投影機		
教科書與 教材	The code book 碼書-編碼與解碼的戰爭, 作者:Simon Singh, 譯:劉燕芬 出版:台灣商務印書館		
參考文獻			
批改作業 篇數	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： 30.0 % ◆平時評量：30.0 % ◆期中評量：20.0 % ◆期末評量：20.0 % ◆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。		