

淡江大學 113 學年度第 2 學期課程教學計畫表

課程名稱	資訊安全	授課 教師	陳夏祥 HSIA-HSIANG CHEN
	INFORMATION SECURITY		
開課系級	資工三 B	開課 資料	遠距課程 必修 單學期 2學分
	TEIXB3B		
課程與SDGs 關聯性	SDG4 優質教育 SDG8 尊嚴就業與經濟發展 SDG9 產業創新與基礎設施 SDG11 永續城市與社區		
系（ 所 ） 教 育 目 標			
一、通達專業知能。 二、熟練實用技能。 三、展現創意成果。			
本課程對應院、系(所)核心能力之項目與比重			
A. 程式設計應用能力。(比重：10.00) B. 數學推理演繹能力。(比重：30.00) C. 資訊系統實作能力。(比重：30.00) D. 網路技術應用能力。(比重：10.00) E. 資訊技能就業能力。(比重：20.00)			
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：20.00) 5. 獨立思考。(比重：10.00) 6. 樂活健康。(比重：10.00) 7. 團隊合作。(比重：10.00) 8. 美學涵養。(比重：10.00)			

課程簡介	本課程主旨在說明資訊安全原理與實務。其內容包含發展歷程、對稱式與非對稱式密碼、加密資料完整性演算法、雙向認證、加密資料完整性演算法、雙向認證、特定網路與網際網路安全。最終學生將瞭解電腦與網路安全的觀念與應用。				
	The course introduces the principles and practices for information security. The contents include the background, symmetric and asymmetric ciphers, cryptographic data integrity algorithms, mutual trust, and network and internet security. Eventually, everyone can also understand computer and network security concepts and applications.				
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	學生將學習認證、授權和存取控制的觀念。		Students learn concepts of authentication, authorization, and access control.		
2	學生能夠瞭解弱點攻擊的行為模式。		Students may understand the vulnerability of attack.		
3	學生能夠結合理論和實務知識應用於安全資料傳輸。		Students may apply theoretical and practical knowledge in secure data transmission.		
4	學生將瞭解分散式拒絕存取服務的大型攻擊模式、惡意程式和錯誤確認。		Students will know the large-scale attacks of DDoS, malware software, and faults found.		
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	ABCDE	12345678	講述、討論	測驗、作業、討論(含課堂、線上)、實作
2	認知	ABCDE	12345678	講述、討論	測驗、作業、討論(含課堂、線上)、實作
3	認知	ABCDE	12345678	講述、討論	測驗、作業、討論(含課堂、線上)、實作
4	認知	ABCDE	12345678	講述、討論	測驗、作業、討論(含課堂、線上)、實作
授 課 進 度 表					
週次	日期起訖	內 容 (Subject/Topics)			備 註 (請註明為同步、非同步課程)
1	114/02/17~114/02/23	Introduction to Network Security			

2	114/02/24~ 114/03/02	Number Theory	非同步課程
3	114/03/03~ 114/03/09	Number Theory	非同步課程
4	114/03/10~ 114/03/16	Classical and Advanced Encryption Approach	非同步課程
5	114/03/17~ 114/03/23	Classical and Advanced Encryption Approach	非同步課程
6	114/03/24~ 114/03/30	Block Ciphers and Data Encryption	非同步課程
7	114/03/31~ 114/04/06	Block Ciphers and Data Encryption	非同步課程
8	114/04/07~ 114/04/13	Finite Fields	非同步課程
9	114/04/14~ 114/04/20	期中考	
10	114/04/21~ 114/04/27	Finite Fields	非同步課程
11	114/04/28~ 114/05/04	Public-Key Cryptogaphy and RSA	非同步課程
12	114/05/05~ 114/05/11	Public-Key Cryptogaphy and RSA	非同步課程
13	114/05/12~ 114/05/18	Cryptography Hash Function	非同步課程
14	114/05/19~ 114/05/25	Message Authentication Codes	非同步課程
15	114/05/26~ 114/06/01	Digital Signatures	非同步課程
16	114/06/02~ 114/06/08	Digital Signatures	非同步課程
17	114/06/09~ 114/06/15	期末考	
18	114/06/16~ 114/06/22	Complementary Materials	非同步課程
課程培養 關鍵能力		自主學習、國際移動、資訊科技、社會參與、問題解決、跨領域	
跨領域課程		STEAM課程(S科學、T科技、E工程、M數學，融入A人文藝術領域) 素養導向課程(探索素養、永續素養或全球議題STEEP(Society ,Technology, Economy, Environment, and Politics))	
特色教學 課程			
課程 教授內容		程式設計或程式語言(學生有實際從事相關作業或活動) 智慧財產(課程內容教授智慧財產) 邏輯思考 A I 應用 永續議題	

修課應 注意事項	
教科書與 教材	自編教材：簡報、講義 採用他人教材：教科書、簡報、講義 教材說明： 1. W. Stallings, Cryptography and Network Security, PEARSON, Eighth Edition. 2. M. Ciampa, Security Guide to Network Security Fundamentals, COURSE TECHNOLOGY, Fourth Edition.
參考文獻	
學期成績 計算方式	◆出席率： % ◆平時評量：30.0 % ◆期中評量：35.0 % ◆期末評量：35.0 % ◆其他〈 〉： %
備 考	1. 「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。 2. 依「專科以上學校遠距教學實施辦法」第2條規定：「本辦法所稱遠距教學課程，指每一科目授課時數二分之一以上以遠距教學方式進行」。 3. 依「淡江大學數位教學施行規則」第3條第2項，本校遠距教學課程須為「於本校遠距教學平台或同步視訊系統進行數位教學之課程。授課時數包含課程講授、師生互動討論、測驗及其他學習活動之時數」。 4. 如有課程臨時異動(含遠距教學、以實整虛課程之上課時間及教室異動)，請依規定向教務處提出申請。 ※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。