

淡江大學 112 學年度第 2 學期課程教學計畫表

課程名稱	網路安全	授課 教師	陳夏祥 HSIA-HSIANG CHEN
	NETWORK SECURITY		
開課系級	智應一碩士班 A	開課 資料	遠距課程 選修 單學期 2學分
	TEIEM1A		
課程與SDGs 關聯性	SDG3 良好健康和福祉 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		
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、厚植資訊網路專業知能。 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：20.00) B. 獨立研究創新能力。(比重：20.00) C. 論文撰寫發表能力。(比重：20.00) D. 資訊網路研發能力。(比重：20.00) E. 專案計畫管理能力。(比重：10.00) F. 自主終生學習能力。(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：20.00) 4. 品德倫理。(比重：10.00) 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	本課程主旨在說明網路安全與密碼學原理與實務。其內容包括發展歷程、對稱式與非對稱式密碼、加密資料完整性演算法、雙向認證、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 cryptography and network 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 fault 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	ABCDEF	12345678	講述、討論、實作、模擬	測驗、作業、討論(含課堂、線上)、實作、報告(含口頭、書面)
2	認知	ABCDEF	12345678	講述、討論、實作、模擬	測驗、作業、討論(含課堂、線上)、實作、報告(含口頭、書面)
3	認知	ABCDEF	12345678	講述、討論、實作、模擬	測驗、作業、討論(含課堂、線上)、實作、報告(含口頭、書面)

4	認知	ABCDEF	12345678	講述、討論、實作、模擬	測驗、作業、討論(含課堂、線上)、實作、報告(含口頭、書面)
---	----	--------	----------	-------------	--------------------------------

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	113/02/19~ 113/02/25	Introduction to Network Security	
2	113/02/26~ 113/03/03	Number Theory	非同步課程
3	113/03/04~ 113/03/10	Number Theory	非同步課程
4	113/03/11~ 113/03/17	Classical and Advanced Encryption Approach	
5	113/03/18~ 113/03/24	Classical and Advanced Encryption Approach	非同步課程
6	113/03/25~ 113/03/31	Block Ciphers and Data Encryption	
7	113/04/01~ 113/04/07	Block Ciphers and Data Encryption	非同步課程
8	113/04/08~ 113/04/14	Finite Fields	非同步課程
9	113/04/15~ 113/04/21	Midterm Exam	
10	113/04/22~ 113/04/28	Finite Fields	非同步課程
11	113/04/29~ 113/05/05	Public-Key Cryptography and RSA	
12	113/05/06~ 113/05/12	Public-Key Cryptography and RSA	非同步課程
13	113/05/13~ 113/05/19	Cryptographic Hash Function	
14	113/05/20~ 113/05/26	Message Authentication Codes	非同步課程
15	113/05/27~ 113/06/02	Digital Signatures	
16	113/06/03~ 113/06/09	Digital Signatures	非同步課程
17	113/06/10~ 113/06/16	Final Exam	
18	113/06/17~ 113/06/23	Complementary Materials	

課程培養
關鍵能力

自主學習、資訊科技、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	專案實作課程 專題/問題導向(PBL)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) 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、影片 採用他人教材:教科書、簡報、講義、影片
參考文獻	1. William Stallings, Cryptography and Network Security, PEARSON, Eighth Edition. 2. Mark Ciampa, Security+ Guide to Network Security Fundamentals, COURSE TECHNOLOGY, Fourth Edition.
學期成績計算方式	◆出席率： 10.0 % ◆平時評量：30.0 % ◆期中評量：20.0 % ◆期末評量：20.0 % ◆其他〈report/presentation〉：20.0 %
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。