

淡江大學 112 學年度第 1 學期課程教學計畫表

課程名稱	網路安全	授課 教師	黃仁俊 HWANG REN-JUNN
	NETWORK SECURITY		
開課系級	資工一碩士班 A	開課 資料	實體課程 選修 單學期 3學分
	TEIXM1A		
課程與SDGs 關聯性	SDG9 產業創新與基礎設施 SDG11 永續城市與社區 SDG12 負責任的消費與生產		
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：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. 資訊工程研發能力。(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：5.00) 2. 資訊運用。(比重：30.00) 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：30.00) 6. 樂活健康。(比重：5.00) 7. 團隊合作。(比重：5.00) 8. 美學涵養。(比重：5.00)			

課程簡介	本課程的目的是介紹網路安全的原理、技術與實務，共分兩個部分執行：第一個部分介紹密碼學及網路安全的基礎技術，後半學期將深入討論網路安全現有技術的發展趨勢及相關技術現況及其優缺點。
	The purpose of this course is to introduce the principles, techniques and practices of network security. The course is divided into two parts: the first part introduces the basic techniques of cryptography and network security. In the second part, the course will discuss the technology trends, advantages and drawbacks of existing network security technologies.

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	學生能夠了解網路及其相關的安全議題	Students may appreciate the issues of network security
2	學生能夠瞭解網路及其相關所面臨的攻擊與威脅	Students may understand the attacks and threats of network security
3	學生了解網路安全技術	Students are able to understand the network security techniques.
4	學生能夠合成並應用網路安全相關技術	Students may be able to synthesize and apply the knowledge and technologies of network security.
5	使學生經常注意新網路安全機制	Students may regularly take notice of new mechanisms of network security.
6	增進學生網路安全專業英文閱讀能力	Enhancing students' ability to read technical English especially in the realm of network security.

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	ABDF	12356	講述、討論	討論(含課堂、線上)、報告(含口頭、書面)
2	情意	ABCDE	2578	講述、討論	討論(含課堂、線上)、報告(含口頭、書面)
3	情意	ABCD	257	講述、討論	討論(含課堂、線上)、報告(含口頭、書面)

4	情意	ABCD	25	講述、討論	討論(含課堂、線上)、報告(含口頭、書面)
5	認知	ABCDF	12345	講述、討論	討論(含課堂、線上)、報告(含口頭、書面)
6	情意	BCDEF	123568	討論	報告(含口頭、書面)

授 課 進 度 表

週次	日期起訖	內 容 (Subject/Topics)	備註
1	112/09/11~ 112/09/17	What is network security?	
2	112/09/18~ 112/09/24	Security Attacks, Services and Mechanisms	
3	112/09/25~ 112/10/01	Symmetric Cryptography	
4	112/10/02~ 112/10/08	Block Cipher Operations	
5	112/10/09~ 112/10/15	RSA	
6	112/10/16~ 112/10/22	ECC	
7	112/10/23~ 112/10/29	Cryptography Hash Function	
8	112/10/30~ 112/11/05	Message Authentication Codes	部分時間學生上台報告
9	112/11/06~ 112/11/12	Message Authentication Codes	部分時間學生上台報告
10	112/11/13~ 112/11/19	Digital Signatures	部分時間學生上台報告
11	112/11/20~ 112/11/26	Lightweight Cryptography	部分時間學生上台報告
12	112/11/27~ 112/12/03	Lightweight Cryptography	部分時間學生上台報告
13	112/12/04~ 112/12/10	Cryptography Key Management and Distribution	部分時間學生上台報告
14	112/12/11~ 112/12/17	Cryptography Key Management and Distribution	部分時間學生上台報告
15	112/12/18~ 112/12/24	User Authentication	部分時間學生上台報告
16	112/12/25~ 112/12/31	User Authentication	部分時間學生上台報告
17	113/01/01~ 113/01/07	期末考試週	
18	113/01/08~ 113/01/14	教師彈性教學週(依學生自主視個人需求做進階學習或補救學習諮詢)建議閱聽：國際資安認證	無教室實體課程
課程培養 關鍵能力		自主學習、資訊科技	

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	<ol style="list-style-type: none"> 1.本課程期待同學以積極態度參與學習。 2.希望同學於課堂盡量針對上課主題發表意見與觀點一起討論。 3.教學內容是以英文撰寫。 4.學生上台報告須以英文撰寫投影片。 5.學生上台報告內容須包含評論分析所報告的論文(事先錄製影片)。 6.學生自行選擇的論文需為2021年以後的期刊或優質會議論文(經老師同意者例外)。
教科書與教材	<p>採用他人教材:教科書、簡報</p> <p>教材說明: William Stallings, Cryptography and Network Security, 8th edition, Pearson, 2020</p>
參考文獻	
學期成績計算方式	<p>◆出席率： 20.0 % ◆平時評量： % ◆期中評量： %</p> <p>◆期末評量： %</p> <p>◆其他〈書面報告50%；上台報告30%〉：80.0 %</p>
備考	<p>「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。</p> <p>※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。</p>