

淡江大學 110 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	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、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) D. 資訊工程研發能力。(比重：40.00) F. 自主終生學習能力。(比重：20.00)			
本課程對應校級基本素養之項目與比重			
2. 資訊運用。(比重：60.00) 4. 品德倫理。(比重：20.00) 5. 獨立思考。(比重：20.00)			
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，前半學期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 network security principles, techniques and practices. First half of the semester introduces cryptography and network security practices, the latter half of the semester 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	ADF	245	講述、討論	討論(含課堂、線上)、報告(含口頭、書面)
2	情意	ABD	245	講述、討論	討論(含課堂、線上)、報告(含口頭、書面)
3	情意	ABD	245	講述、討論	討論(含課堂、線上)、報告(含口頭、書面)
4	情意	ABD	25	講述、討論	討論(含課堂、線上)、報告(含口頭、書面)
5	認知	BDF	245	講述、討論	討論(含課堂、線上)、報告(含口頭、書面)
6	情意	F	245	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	110/09/22~ 110/09/28	What is network security?	

2	110/09/29~ 110/10/05	Security Attacks, Services and Mechanisms	
3	110/10/06~ 110/10/12	Symmetric Cryptography	部分時間學生上台報告
4	110/10/13~ 110/10/19	Block Cipher Operation	部分時間學生上台報告
5	110/10/20~ 110/10/26	Asymmetric Cryptography	部分時間學生上台報告
6	110/10/27~ 110/11/02	RSA	部分時間學生上台報告
7	110/11/03~ 110/11/09	Key Exchange	部分時間學生上台報告
8	110/11/10~ 110/11/16	Elliptic Curve Cryptography	部分時間學生上台報告
9	110/11/17~ 110/11/23	期中考週	
10	110/11/24~ 110/11/30	Hash Function	部分時間學生上台報告
11	110/12/01~ 110/12/07	Message Authentication Code	部分時間學生上台報告
12	110/12/08~ 110/12/14	Message Authentication Code	部分時間學生上台報告
13	110/12/15~ 110/12/21	Digital Signature	部分時間學生上台報告
14	110/12/22~ 110/12/28	Digital Signature	部分時間學生上台報告
15	110/12/29~ 111/01/04	Key Management	部分時間學生上台報告
16	111/01/05~ 111/01/11	Key Management	部分時間學生上台報告
17	111/01/12~ 111/01/18	期末考週	
18	111/01/19~ 111/01/25	參考閱讀TibaMe：區塊鏈的前世今生與未來	自主學習，12/31前繳交一份報告
修課應 注意事項	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。 6.學生自行選擇的論文需為2019年以後的期刊或優質會議論文(經老師同意者例外)。 7.自主學習為參考閱讀TibaMe：區塊鏈的前世今生與未來；12/31前至iClass上傳交一篇與區塊鏈有關的報告		
教學設備	電腦、投影機		
教科書與 教材	William Stallings, Cryptography and Network Security, seventh edition, Pearson, 2017		
參考文獻	2019年以後期刊或優質學術研討會論文		

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： 10.0 % ◆平時評量： % ◆期中評量： % ◆期末評量： % ◆其他〈書面報告50%上台40%〉：90.0 %
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。