

淡江大學 101 學年度第 1 學期課程教學計畫表

課程名稱	電腦密碼學	授課 教師	黃心嘉 HWANG SHIN-JIA
	CRYPTOGRAPHY		
開課系級	資網一碩士班 A	開課 資料	選修 單學期 3學分
	TEIAM1A		

系（所）教育目標

- 一、培養克服困難及解決問題之能力-教育研究生面對困難接受挑戰及分析問題、評析各種解決問題的工具及方法，以啟發獨立研究及解決問題的能力。
- 二、啟發獨立思考及研發創新之潛能-透過論文的資料收集、研讀、理解、歸納、分析、表達以及研究議題的思考、創新、驗證、實作等過程，培養研究生獨立思考及研發創新之潛能。
- 三、建立網路通訊專業及科技實作之技能-經由資訊網路與通訊專業課程、論文研讀、書報討論、演講及研討會參與等多樣化管道，建立研究生網路通訊專業的背景，並透過國科會、教育部及各單位委託之計畫實作以及論文實作，以培養科技實作的技能。
- 四、擴展國際趨勢及產業脈動之視野-營造國際化的學習與研發環境，積極參與或舉辦國際研討會及校際演講，以擴展研究生的國際視野。因應產業快速轉移與全球化之演變，促進產學合作，並與校友互動，以洞悉產業的脈動及趨勢。
- 五、塑造樸實剛毅及德智兼修之人格-本著淡江大學大學的校訓與治校理念，塑造科技與人文兼具的求知環境，塑造樸實剛毅及德智兼修之人格特質與涵養。
- 六、養成積極進取及終身學習之態度-因應知識的快速成長，教育學生終身學習及不斷自我成長，以養成其追求真理、積極進取及終身學習的態度。

系（所）核心能力

- A. 具有獨立思考、判斷與分析問題的能力，並能啟發創新思維運用於研究議題。
- B. 具有面對困難接受挑戰之態度，及獨立探索、推導與設計解決問題的方法與工具之能力。
- C. 具有運用專業領域之網路與通訊知識與技能，並用以規劃資訊系統的分析、設計、製作與整合的能力。
- D. 具有良好專業技術論文撰寫及口語表達之能力。
- E. 具有專案計畫之規劃、撰寫、領導及管理之能力。
- F. 具有運用外語能力於學習與交流的能力、認知全球議題，並藉以透析產業趨勢動向與全球化之變遷。
- G. 具有理解專業倫理及社會責任的能力，並以負責任的態度用於人際溝通、團隊合作及協調整合。
- H. 具有樸實剛毅、德智兼修之人格特質及服務人群之精神。
- I. 瞭解終身學習的重要，並持續培養自我學習的能力。

課程簡介	本課程的目的在提供密碼學與安全基礎的理論背景，介紹最近的研究成果。
	The purpose of this course is to give the fundamental theoretical background for cryptography and security. The current research results are also introduced.

本課程教學目標與目標層級、系(所)核心能力相關性

一、目標層級(選填)：

- (一)「認知」(Cognitive 簡稱C)領域：C1 記憶、C2 瞭解、C3 應用、C4 分析、C5 評鑑、C6 創造
- (二)「技能」(Psychomotor 簡稱P)領域：P1 模仿、P2 機械反應、P3 獨立操作、P4 聯結操作、P5 自動化、P6 創作
- (三)「情意」(Affective 簡稱A)領域：A1 接受、A2 反應、A3 重視、A4 組織、A5 內化、A6 實踐

二、教學目標與「目標層級」、「系(所)核心能力」之相關性：

- (一)請先將課程教學目標分別對應前述之「認知」、「技能」與「情意」的各目標層級，惟單項教學目標僅能對應C、P、A其中一項。
- (二)若對應「目標層級」有1~6之多項時，僅填列最高層級即可(例如：認知「目標層級」對應為C3、C5、C6項時，只需填列C6即可，技能與情意目標層級亦同)。
- (三)再依據所訂各項教學目標分別對應其「系(所)核心能力」。單項教學目標若對應「系(所)核心能力」有多項時，則可填列多項「系(所)核心能力」。(例如：「系(所)核心能力」可對應A、AD、BEF時，則均填列。)

序號	教學目標(中文)	教學目標(英文)	相關性	
			目標層級	系(所)核心能力
1	學生學習最近研究成果，並透過口頭報告與討論進一步學習。	Students learn the current research results. Through the oral reports and discussions to enhance depth of students' studies.	P5	ABDF
2	學生學習密碼學與資訊安全的基本理論應用，並透過口頭報告與討論進一步學習。	Students learn applications of the fundamental background on cryptography and information security. Through the oral reports and discussions to enhance depth of students' studies.	P5	ABF
3	增進學生資訊科學專業英文閱讀能力。	Enhancing students' ability to read technical English especially in Computer Sciences.	P5	F

教學目標之教學方法與評量方法

序號	教學目標	教學方法	評量方法
1	學生學習最近研究成果，並透過口頭報告與討論進一步學習。	上台報告	上課表現、上台報告
2	學生學習密碼學與資訊安全的基本理論應用，並透過口頭報告與討論進一步學習。	上台報告	上課表現、上台報告
3	增進學生資訊科學專業英文閱讀能力。	原文資料	上台報告

本課程之設計與教學已融入本校校級基本素養

淡江大學校級基本素養	內涵說明
◇ 全球視野	
◆ 洞悉未來	
◆ 資訊運用	
◇ 品德倫理	
◆ 獨立思考	
◇ 樂活健康	
◇ 團隊合作	
◇ 美學涵養	

授課進度表

週次	日期起訖	內容 (Subject/Topics)	備註
1	101/09/10~ 101/09/16	課程與密碼理論介紹	
2	101/09/17~ 101/09/23	課程與密碼理論介紹	
3	101/09/24~ 101/09/30	課程與密碼理論介紹	
4	101/10/01~ 101/10/07	課程與密碼理論介紹	
5	101/10/08~ 101/10/14	最近研究成果報告	
6	101/10/15~ 101/10/21	最近研究成果報告	
7	101/10/22~ 101/10/28	最近研究成果報告	

8	101/10/29~ 101/11/04	最近研究成果報告	
9	101/11/05~ 101/11/11	期中考	
10	101/11/12~ 101/11/18	最近研究成果報告	
11	101/11/19~ 101/11/25	最近研究成果報告	
12	101/11/26~ 101/12/02	最近研究成果報告	
13	101/12/03~ 101/12/09	最近研究成果報告	
14	101/12/10~ 101/12/16	最近研究成果報告	
15	101/12/17~ 101/12/23	最近研究成果報告	
16	101/12/24~ 101/12/30	最近研究成果報告	
17	101/12/31~ 102/01/06	最近研究成果報告	
18	102/01/07~ 102/01/13	安全性理論介紹	
修課應 注意事項			
教學設備		電腦、投影機	
教材課本		(1)Understanding Cryptography: A Textbooks for Students and Practitioncers, Chrsitof Paar and Jan Pelzl, Springer, 2010. (2) Papers	
參考書籍		Cryptography and Network Security: Principles and Practice, 5th Ed., William Stallings, Pearson, 2010. “Introduction to Cryptography: Principle and Applications,” 2nd Ed., Hans Delfs and Helmut Knebl, New York: Springer-Verlag, 2007. “Protocols for Authentication and Key Establishment,” Colin Boyd and Anish Mathuria, New York: Springer, 2003.	
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： 20.0 % ◆平時評量： % ◆期中評量： % ◆期末評量： % ◆其他〈口頭報告〉：80.0 %	
備 考		「教學計畫表管理系統」網址： http://info.ais.tku.edu.tw/csp 或由教務處 首頁〈網址： http://www.acad.tku.edu.tw/index.asp/ 〉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。	