

淡江大學 105 學年度第 1 學期課程教學計畫表

課程名稱	網路密碼學	授課 教師	黃仁俊 HWANG REN-JUNN
	INTERNET CRYPTOGRAPHY		
開課系級	資網一碩士班 A	開課 資料	選修 單學期 2學分
	TEICM1A		
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。			
系（ 所 ） 核 心 能 力			
A. 獨立解決問題能力。 B. 獨立研究創新能力。 C. 論文撰寫發表能力。 D. 資訊網路研發能力。 E. 專案計畫管理能力。 F. 自主終生學習能力。			
課程簡介	本課程除了密碼基本觀念介紹外，也涵蓋密碼協定。密碼協定的主要議題有零知識協定、身分識別法、驗證式金鑰建立協定與其他適用於多人的協定。安全性的定義與證明也是主要議題。		
	This course gives not only the overview of cryptography concepts but also the cryptographic protocols. The major topics of cryptographic protocols are zero-knowledge protocols, identification schemes, authenticated key established protocols and some protocols for multi-parties. Security definitions and proofs are also the major topics.		

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	1學生學習密碼方法與協定的安全性定義與要求，並透過口頭報告與討論進一步學習。	1Students learn the security definition and requirements for cryptographic schemes and protocols. Through the oral reports and discussions to enhance depth of students' studies.	C2	AB
2	2學生學習密碼協定與相關的安全性分析，並透過口頭報告與討論進一步學習。	2. Students learn the cryptographic protocols and cryptanalysis. Through the oral reports and discussions to enhance depth of students' studies.	P3	AD
3	3增進學生資訊科學專業英文閱讀能力。	3 Enhancing students' ability to read technical English especially in Computer Sciences.	C2	AF

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	1學生學習密碼方法與協定的安全性定義與要求，並透過口頭報告與討論進一步學習。	講述、討論	報告、上課表現
2	2學生學習密碼協定與相關的安全性分析，並透過口頭報告與討論進一步學習。	講述、討論	報告、上課表現
3	3增進學生資訊科學專業英文閱讀能力。	講述、討論	報告、上課表現

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	培養認識國際社會變遷的能力，以更寬廣的視野了解全球化的發展。	
◆	資訊運用	熟悉資訊科技的發展與使用，並能收集、分析和妥適運用資訊。	
◇	洞悉未來	瞭解自我發展、社會脈動和科技發展，以期具備建構未來願景的能力。	
◇	品德倫理	了解為人處事之道，實踐同理心和關懷萬物，反省道德原則的建構並解決道德爭議的難題。	
◆	獨立思考	鼓勵主動觀察和發掘問題，並培養邏輯推理與批判的思考能力。	
◇	樂活健康	注重身心靈和環境的和諧，建立正向健康的生活型態。	
◇	團隊合作	體察人我差異和增進溝通方法，培養資源整合與互相合作共同學習解決問題的能力。	
◇	美學涵養	培養對美的事物之易感性，提升美學鑑賞、表達及創作能力。	
授 課 進 度 表			
週次	日期起訖	內 容 (Subject/Topics)	備 註
1	105/09/12~ 105/09/18	Introduction(Textbook 2)	
2	105/09/19~ 105/09/25	Public Key Cryptography(Textbook 2)	
3	105/09/26~ 105/10/02	Cryptographic Protocols (Textbook 2)	
4	105/10/03~ 105/10/09	A Tutorial Introduction to Authentication and Key Establishment	
5	105/10/10~ 105/10/16	A Tutorial Introduction to Authentication and Key Establishment	部分時間學生上台報告
6	105/10/17~ 105/10/23	Goals for Authentication and Key Establishment	部分時間學生上台報告
7	105/10/24~ 105/10/30	Goals for Authentication and Key Establishment	部分時間學生上台報告
8	105/10/31~ 105/11/06	Protocols Using Shared Key Cryptography	部分時間學生上台報告
9	105/11/07~ 105/11/13	Protocols Using Shared Key Cryptography	部分時間學生上台報告
10	105/11/14~ 105/11/20	期中考試週	部分時間學生上台報告
11	105/11/21~ 105/11/27	Secret Sharing Schemes	部分時間學生上台報告
12	105/11/28~ 105/12/04	Authentication and Key Transport Using Public Key Cryptography	部分時間學生上台報告

13	105/12/05~ 105/12/11	Authentication and Key Transport Using Public Key Cryptography	部分時間學生上台報告
14	105/12/12~ 105/12/18	Key Agreement Protocols	部分時間學生上台報告
15	105/12/19~ 105/12/25	Key Agreement Protocols	部分時間學生上台報告
16	105/12/26~ 106/01/01	Zero-Knowledge Proof (1) (Textbook 1)	部分時間學生上台報告
17	106/01/02~ 106/01/08	Zero-Knowledge Proof (2) (Textbook 1)	部分時間學生上台報告
18	106/01/09~ 106/01/15	期末考試週	部分時間學生上台報告
修課應 注意事項		修課同學需事先研讀指定教材，課堂以討論報告為主	
教學設備		電腦、投影機	
教材課本		1.DStinson Cryptography: Theory and Practice, CRC, 2006. 2. H Delfs and H Knebl, Introduction to Cryptography: Principle and Applications, Springer 2007.	
參考書籍		3. C Boyd and A Mathuria, "Protocols for Authentication and Key Establishment," Springer, 2003. 4.N Smart Cryptography: An introduction McGraw-Hill, 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： 10.0 % ◆平時評量： % ◆期中評量： % ◆期末評量： % ◆其他〈課堂報告與表現〉：90.0 %	
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/CS/main.php 〉業務連結「教師教學 計畫表上傳下載」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。	