

淡江大學 103 學年度第 2 學期課程教學計畫表

課程名稱	數位簽章法	授課 教師	黃心嘉 HWANG SHIN-JIA
	DIGITAL SIGNATURE SCHEMES		
開課系級	資工一碩士班 A	開課 資料	選修 單學期 3學分
	TEIXM1A		
系 (所) 教育目標			
<p>一、培養獨立研究解決問題。</p> <p>二、提昇研發能量創意設計。</p> <p>三、厚植資訊工程專業知能。</p> <p>四、養成自發自主終生學習。</p>			
系 (所) 核心能力			
<p>A. 獨立解決問題能力。</p> <p>B. 獨立研究創新能力。</p> <p>C. 論文撰寫發表能力。</p> <p>D. 資訊工程研發能力。</p> <p>E. 專案計畫管理能力。</p> <p>F. 自主終生學習能力。</p>			
課程簡介	本課程首先介紹密碼的背景知識、安全性定義與證明方式，隨後介紹各式各樣密碼方法與數位簽章演算法。		
	This course first introduce mathematic backgroup for cryptography, security defintion and proof. Then many digital signature schemes and relative topics 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	介紹密碼學的基本觀念。	Introduction concepts of cryptogrphahy.	C4	A
2	介紹密碼學中演算法與協定的安全定義	Introduce the security definitions of cryptographic algorithms and protocols.	C4	A
3	介紹近來數位簽章與其相關研究結果。	Introduce the recent results about digital signature schemes.	P5	AB
4	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	介紹密碼學的基本觀念。	講述、學生上台報告	紙筆測驗、報告、上課表現
2	介紹密碼學中演算法與協定的安全定義	講述、學生上台報告	紙筆測驗、報告、上課表現
3	介紹近來數位簽章與其相關研究結果。	講述、學生上台口頭報告。	紙筆測驗、報告
4	增進學生資訊科學專業英文閱讀能力。	講述、原文教材	紙筆測驗、報告、原文出題

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	104/02/24~ 104/03/01	課程與密碼學介紹	
2	104/03/02~ 104/03/08	密碼的理論背景	
3	104/03/09~ 104/03/15	Definition of Security	Smart Ch15
4	104/03/16~ 104/03/22	Complexity Theoretic Approaches	Smart Ch16
5	104/03/23~ 104/03/29	Provable Security: With Random Oracles	Smart Ch 17
6	104/03/30~ 104/04/05	TEST1	
7	104/04/06~ 104/04/12	Provable Security: Without Random Oracles	Smart Ch 18
8	104/04/13~ 104/04/19	Information Theoretic Security	Smart Ch 4
9	104/04/20~ 104/04/26	期中考	
10	104/04/27~ 104/05/03	Zero-Knowledge Proof	
11	104/05/04~ 104/05/10	Zero-Knowledge Proof	
12	104/05/11~ 104/05/17	Identification Schemes and Entity Authentication	

13	104/05/18~ 104/05/24	Secret Sharing Scheme	
14	104/05/25~ 104/05/31	Test2	
15	104/06/01~ 104/06/07	Pseudo-random Number Generation	
16	104/06/08~ 104/06/14	Probabilistic public-key encryption	
17	104/06/15~ 104/06/21	Signature Schemes	
18	104/06/22~ 104/06/28	期末報告	
修課應 注意事項	負責報告的同學，須在上課前三天將投影片以電子郵件的方式寄給老師與助教。		
教學設備	電腦、投影機		
教材課本	"Cryptography: An introduction", 3,0.1 2 Ed., Nigel Smart, New York: McGraw-Hill,2011 Cryptography: Theory and Practice, 3rd Ed., Douglas R. Stinson, CRC, 2006		
參考書籍	"Handbook of Applied Cryptography," Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, CRC Press, 2001		
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：40.0 % ◆期中評量：40.0 % ◆期末評量： % ◆其他〈期末報告〉：10.0 %		
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。		