淡江大學１０７學年度第２學期課程教學計畫表

課程名稱	安全理論 SECURITY THEORY	授課教師	黃心嘉 HWANG SHIN-JIA
開課系級	資工一碩士班Ａ TEIXM1A	開課資料	選修 單學期 3學分

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。

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. 資訊工程研發能力。

E. 專案計畫管理能力。

F. 自主終生學習能力。

課程簡介	本課程的目的在提供進階密碼學與安全性證明的理論背景，並介紹最近的研究成果。
	The purpose of this course is to give the theoretical background for advanced cryptography and security proof. 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	D
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 of advanced cryptography and information security. Through the oral reports and discussions to enhance the depth of students' studies.	P4	D
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	D

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。	講述、討論、上台報告	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。	討論、上台報告	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。	討論、原文資料	實作、上課表現、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	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	108/02/18～108/02/24	課程介紹	
2	108/02/25～108/03/03	Ch 1 Introduction to Cryptography and Data Security (Pelzl)& Ch 1 Modular Arithmetic, Groups, Finite Fields, and Probability (Smart)	
3	108/03/04～108/03/10	Ch 1 Modular Arithmetic, Groups, Finite Fields, and Probability (Smart)	
4	108/03/11～108/03/17	Ch 6 Introduction to Public-Key Cryptography (Pelzl), Ch 7 The RSA Cryptosystem (Pelzl)與最近研究成果報告	
5	108/03/18～108/03/24	Ch 8 Public-Key Cryptosystems Based on the Discrete Logarithm Problem (Pelzl)與最近研究成果報告	
6	108/03/25～108/03/31	Chapter 9. Information-Theoretic Security (Smart)與最近研究成果報告	
7	108/04/01～108/04/07	教學觀摩週	
8	108/04/08～108/04/14	Chapter 11. Defining Security (Smart)與最近研究成果報告	
9	108/04/15～108/04/21	Chapter 11. Defining Security (Smart)(期中考週)	
10	108/04/22～108/04/28	Chapter 17. Cryptography Based on Really Hard Problems (Smart)與最近研究成果報告	

11	108/04/29～ 108/05/05	Ch 10 Digital Signatures (Pelzl)與最近研究成果報告	
12	108/05/06～ 108/05/12	Ch 10 Digital Signatures (Pelzl)與最近研究成果報告	
13	108/05/13～ 108/05/19	深度學習介紹與最近研究成果報告	
14	108/05/20～ 108/05/26	深度學習介紹與最近研究成果報告	
15	108/05/27～ 108/06/02	深度學習介紹與最近研究成果報告	
16	108/06/03～ 108/06/09	深度學習介紹與最近研究成果報告	
17	108/06/10～ 108/06/16	深度學習介紹與最近研究成果報告	
18	108/06/17～ 108/06/23	最近研究成果報告	

修課應注意事項	1.出席與討論為評分考量之一。 2. 報告內容為評分考量之一。 3. 若自己負責報告時卻缺席，若無不可避免的理由，該次報告是零分。 4. 課程會使用圖書館的資料庫電子書，請自行下載! 5. 請尊重智慧財產權。本課程的PPT將只瀏覽不可下載。 6.本課程會使用學校教學平台iClass或Moodle，請自行留意教學平台上的公告與通知。
教學設備	電腦、投影機
教材課本	"Cryptography Made Simple," Nigel P. Smart, Springer, 2016. "Understanding Cryptography, " Christof PaarJan Pelzl, Springer, 2010
參考書籍	Cryptography and Network Security: Principles and Practice, 7th Ed., William Stallings, Pearson, 2017 “Introduction to Cryptography: Principle and Applications,” 3rd Ed., Hans Delfs and Helmut Knebl, New York: Springer-Verlag, 2010. “Protocols for Authentication and Key Establishment,” Colin Boyd and Anish Mathuria, New York: Springer, 2003. "Understanding Cryptography A Textbook for Students and Practitioners", Christof Paar, Jan Pelzl (2010)
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： 40.0 %　◆平時評量： %　◆期中評量： % ◆期末評量： % ◆其他〈口頭報告〉：60.0 %
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。**