# 淡江大學９９學年度第２學期課程教學計畫表

| | | | |
|---|---|---|---|
| 課程名稱 | 網路密碼學<br>INTERNET CRYPTOGRAPHY | 授課教師 | 黃心嘉<br>Hwang Shin-jia |
| 開課系級 | 資網一碩士班Ａ<br>TEIAM1A | 開課資料 | 選修 單學期 3學分 |

## 學 系(門) 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。

## 學 生 基 本 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、學生基本能力相關性

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」、「學生基本能力」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該系「學生基本能力」。單項教學目標若對應「學生基本能力」有多項時，則可填列多項「學生基本能力」(例如：「學生基本能力」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 | 學生基本能力 |
| 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。 | Students learn the security definition and requirements for cryptographic schemes and protocols. Through the oral reports and discussions to enhance depth of students' studies. | C4 | ABF |
| 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。 | Students learn the cryptographic protocols and cryptanalysis. Through the oral reports and discussions to enhance depth of students' studies. | P3 | ABDF |
| 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. | P4 | F |

| 教學目標之教學策略與評量方法 | | | |
|---|---|---|---|
| 序號 | 教學目標 | 教學策略 | 評量方法 |
| 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。 | 課堂講授、分組討論、學生口頭報告 | 出席率、報告、小考、期中考 |
| 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。 | 課堂講授、分組討論、學生口頭報告 | 出席率、報告、小考、期中考 |
| 3 | 增進學生資訊科學專業英文閱讀能力。 | 課堂講授、分組討論、學生口頭報告 | 出席率、報告、小考、期中考 |

| 授 課 進 度 表 | | | |
|---|---|---|---|
| 週次 | 日期起訖 | 內 容 (Subject/Topics) | 備註 |
| 1 | 100/02/14～100/02/20 | Introduction | |
| 2 | 100/02/21～100/02/27 | Public Key Cryptography | |
| 3 | 100/02/28～100/03/06 | Cryptographic Protocols | |
| 4 | 100/03/07～100/03/13 | A Tutorial Introduction to Authentication and Key Establishment | |
| 5 | 100/03/14～100/03/20 | TEST1 | |
| 6 | 100/03/21～100/03/27 | Goals for Authentication and Key Establishment | |
| 7 | 100/03/28～100/04/03 | Protocols Using Shared Key Cryptography | |
| 8 | 100/04/04～100/04/10 | Secret Sharing Schemes | |
| 9 | 100/04/11～100/04/17 | 期中考 | |
| 10 | 100/04/18～100/04/24 | Authentication and Key Transport Using Public Key Cryptography | |
| 11 | 100/04/25～100/05/01 | Key Agreement Protocols | |
| 12 | 100/05/02～100/05/08 | Zero-Knowledge Proof | |
| 13 | 100/05/09～100/05/15 | TEST2 | |
| 14 | 100/05/16～100/05/22 | 論文研討 | |
| 15 | 100/05/23～100/05/29 | 論文研討 | |
| 16 | 100/05/30～100/06/05 | 論文研討 | |
| 17 | 100/06/06～100/06/12 | 論文研討 | |
| 18 | 100/06/13～100/06/19 | 期末報告 | |

| | |
|---|---|
| 修課應注意事項 | |
| 教學設備 | 電腦、其它(教學支援平台) |
| 教材課本 | “Introduction to Cryptography: Principle and Applications,” 2nd Ed., Hans Delfs and Helmut Knebl, New York: Springer-Verlag, 2007. |
| 參考書籍 | “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 | ◆平時考成績：20.0 % ◆期中考成績：15.0 % ◆期末考成績：15.0 %<br>◆作業成績： %<br>◆其他〈口頭報告〉：50.0 % |
| 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。<br>**※非法影印是違法的行為。請使用正版教科書，勿非法影印他人著作，以免觸法。** |