# 淡江大學９９學年度第２學期課程教學計畫表

| | | | |
|---|---|---|---|
| 課程名稱 | 資訊安全實務<br>PRACTICE OF INFORMATION SECURITY | 授課教師 | 洪文斌<br>Horng Wen-bing |
| 開課系級 | 資訊四Ｐ<br>TEIXB4P | 開課資料 | 選修 單學期 3學分 |

## 學 系(門) 教 育 目 標

一、傳授專業知識-教導學生資訊技術的基本原理與應用實務的專業知能。

二、訓練實用技能-教導學生如何執行與驗證各項實驗，其中包括問題之分析與解決方法、資料的蒐集、維護、管理，以及理論的測試。

三、啟發創新思維-教授學生分析、設計、實作與數學等方面的資訊基礎能力，和有解決科學、工程、企業等上各種問題所需要的獨立思考與創新能力。

四、表現人格特質-使學生能以他/她們的忠誠、剛毅、樸實、專注、厚道等個人特質與專業技能獲得主管與同儕認同。

五、培養團隊精神-訓練學生具有組織能力與溝通技術，讓他/她們能具有融入企業團隊的適應力，並具有發揮與指揮團隊力量來解決相關之專案問題。

六、營造國際視野-順應全球化的趨勢，營造國際化的學習環境與機會，教育學生不斷的自我成長，吸收國內外新的知識，在未來的領域中成為一位具有國際視野與領導能力的專業人才。

## 學 生 基 本 能 力

A. 具有程式設計、系統軟體與軟體應用的知識，並應用於系統分析、設計與應用的能力。

B. 具有計算機硬體設計、資訊網路與通訊的專業知識，並能應用解決工程問題的能力。

C. 具有資訊工程所需的數學、科學與工程知識的能力。

D. 具有邏輯思考、問題分析、實驗執行、數據解釋與推導演繹的能力，並用於規劃與發展資訊系統。

E. 具備良好的口語與書面之溝通技巧，並具有計畫書撰寫、專案執行與時程管理的能力。

F. 培養團隊合作的精神與能力，並具有專業及倫理的責任。

G. 應用外語能力於學習與交流，並具有國際觀。

H. 具備人文素養，能夠瞭解社會生態及資訊產業發展的派動。

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 | 此課程將介紹資訊安全實務中的公鑰基礎建設(PKI), 以上機實作為主, 輔以課程簡介, 讓學生有PKI實務經驗。 |

| | |
|---|---|
| | This course will introduce the Public Key Infrastructure (PKI), a practical course of information security. Students are asked to have the hand-on experience on PKI, aided with some instructions. |

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 | 瞭解現代密碼學：對稱式與非對稱式加解密技術 | Understanding modern cryptography: symmetric and asymmetric encryption/decryption techniques | C3 | ABCD |
| 2 | 了解密碼學雜湊函數：SHA, MD5 | Understanding cryptographic hash functions: SHA, MD5 | C3 | ABCD |
| 3 | 熟悉PKI所需軟體操作 | Familiar with the PKI software | C3 | ABCD |
| 4 | 數位簽章的建立與使用 | Building and using digital signatures | C3 | ABCD |
| 5 | 電子憑證的建立與使用 | Building and using electronic certificates | C3 | ABCD |
| 6 | 憑證資料解析 | Analysis of certificate data | C3 | ABCD |

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 | 瞭解現代密碼學：對稱式與非對稱式加解密技術 | 課堂講授、上機實作 | 出席率、報告、討論、上機驗收 |
| 2 | 了解密碼學雜湊函數：SHA, MD5 | 課堂講授、上機實作 | 出席率、報告、討論、上機驗收 |
| 3 | 熟悉PKI所需軟體操作 | 課堂講授、上機實作 | 出席率、報告、討論、上機驗收 |

| | | | |
|---|---|---|---|
| 4 | 數位簽章的建立與使用 | 課堂講授、上機實作 | 報告、討論、上機驗收 |
| 5 | 電子憑證的建立與使用 | 課堂講授、上機實作 | 出席率、報告、討論、上機驗收 |
| 6 | 憑證資料解析 | 課堂講授、上機實作 | 出席率、報告、討論、上機驗收 |

授 課 進 度 表

| 週次 | 日期起訖 | 內 容 (Subject/Topics) | 備註 |
|---|---|---|---|
| 1 | 100/02/14～100/02/20 | PKI 簡介 | |
| 2 | 100/02/21～100/02/27 | Lab 1: 硬體及軟體環境設置 | |
| 3 | 100/02/28～100/03/06 | Lab 2: 建立資料物件和憑證物件 | |
| 4 | 100/03/07～100/03/13 | Lab 3: 建立金鑰物件 | |
| 5 | 100/03/14～100/03/20 | Lab 4: 金鑰產生 | |
| 6 | 100/03/21～100/03/27 | Lab 5: 資料加解密 | |
| 7 | 100/03/28～100/04/03 | Lab 6: 簽章和驗章 | |
| 8 | 100/04/04～100/04/10 | Lab 7: 單向雜湊函數 (1) | |
| 9 | 100/04/11～100/04/17 | Lab 7: 單向雜湊函數 (2) | |
| 10 | 100/04/18～100/04/24 | 期中考試週 | |
| 11 | 100/04/25～100/05/01 | Lab 8: 金鑰物件管理 | |
| 12 | 100/05/02～100/05/08 | Lab 9: 憑證物件管理 (1) | |
| 13 | 100/05/09～100/05/15 | Lab 9: 憑證物件管理 (2) | |
| 14 | 100/05/16～100/05/22 | Lab 10:憑證資料解析 (1) | |
| 15 | 100/05/23～100/05/29 | Lab 10:憑證資料解析 (2) | |
| 16 | 100/05/30～100/06/05 | Lab 11: 電子信封資料解析 (1) | |
| 17 | 100/06/06～100/06/12 | Lab 11: 電子信封資料解析 (2) | |
| 18 | 100/06/13～100/06/19 | 期末考試週 | |

| | |
|---|---|
| 修課應注意事項 | |
| | |

| | |
|---|---|
| 教學設備 | 電腦、投影機 |
| 教材課本 | PKI Lab Manu |
| 參考書籍 | |
| 批改作業篇數 | 10 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：30.0 %　◆期末考成績：30.0 %<br>◆作業成績： 20.0 %<br>◆其他〈 〉： % |
| 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。** |