# 淡江大學１０２學年度第２學期課程教學計畫表

| | | | |
|---|---|---|---|
| 課程名稱 | 密碼安全性分析<br>CRYPTOGRAPHIC SECURITY ANALYSIS | 授課教師 | 黃心嘉<br>HWANG SHIN-JIA |
| 開課系級 | 資工一碩士班Ａ<br>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 | 本課程介紹密碼學的基本觀念與安全性的定義，並且介紹密碼系統與數位簽章法的安全性證明，並進一步探討近年來的研究成果。 |
| | This course introduce the basic concepts and security defintions in cryptography. The security proofs for cryptosystems and digital signautre schemes are introduced. Finally, some current research results are given. |

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 | 介紹密碼學的基本概念 | Introduction concepts of cryptogrpahy. | C4 | AB |
| 2 | 介紹密碼學中的安全定義。 | Introduce the security definitions in cryptography. | C4 | AB |
| 3 | 介紹近來密碼學相關研究結果。 | Introduce the recent results about cryptography. | P5 | AB |
| 4 | 介紹密碼的安全證明 | Introduce the security proofs for cryptographic schemes. | P4 | AB |

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 | 介紹密碼學的基本概念 | 講述、討論 | 紙筆測驗、報告、上課表現 |
| 2 | 介紹密碼學中的安全定義。 | 講述、討論 | 紙筆測驗、報告、上課表現 |
| 3 | 介紹近來密碼學相關研究結果。 | 討論 | 報告、上課表現 |
| 4 | 介紹密碼的安全證明 | 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 | 103/02/17～103/02/23 | 課程與密碼學介紹 | |
| 2 | 103/02/24～103/03/02 | 密碼的理論背景 | |
| 3 | 103/03/03～103/03/09 | Definition of Security | Smart Ch15 |
| 4 | 103/03/10～103/03/16 | Complexity Theoretic Approaches | Smart Ch16 |
| 5 | 103/03/17～103/03/23 | Provable Security: With Random Oracles | Smart Ch17 |
| 6 | 103/03/24～103/03/30 | TEST 1 | |
| 7 | 103/03/31～103/04/06 | Provable Security: Without Random Oracles | Smart Ch 18 |
| 8 | 103/04/07～103/04/13 | Information Theoretic Security | Smaret Ch 4 |
| 9 | 103/04/14～103/04/20 | Zero-Knowledge Proof | |
| 10 | 103/04/21～103/04/27 | 期中考 | |
| 11 | 103/04/28～103/05/04 | Zero-Knowledge Proof | |
| 12 | 103/05/05～103/05/11 | Identification Schemes and Entity Authentication | |

| | | | |
|---|---|---|---|
| 13 | 103/05/12～<br>103/05/18 | Pseudo-random Number Generation (Ch 8) +<br>Probabilistic public-key encryption (8.7) | |
| 14 | 103/05/19～<br>103/05/25 | TEST2 | |
| 15 | 103/05/26～<br>103/06/01 | Public-key Cryptography and Discrete Logarithms | |
| 16 | 103/06/02～<br>103/06/08 | The RSA Cryptosystem and Factoring Integers | |
| 17 | 103/06/09～<br>103/06/15 | Signature Schemes | |
| 18 | 103/06/16～<br>103/06/22 | 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 | “Cryptography: An introduction”, Nigel Smart, New York: McGraw-Hill, 2003.<br>Cryptography: Theory and Practice, 3rd Ed., Douglas R. Stinson, CRC, 2006 |
| 參考書籍 | |
| 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： 20.0 % ◆平時評量：15.0 % ◆期中評量：15.0 %<br>◆期末評量： %<br>◆其他〈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/CS/main.php〉業務連結「教師教學計畫表上傳下載」進入。<br>**※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。** |