# 淡江大學１００學年度第１學期課程教學計畫表

| | | | |
|---|---|---|---|
| 課程名稱 | 密碼數學<br>MATHEMATICS FOR 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 |

## 系 所 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。

## 系 所 核 心 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 | 本課程的目的在提供密碼學與安全基礎的數學背景, 介紹主題涵蓋數論、近代代數、機率與資訊理論、以及在密碼學與安全的應用。 |
| | The purpose of this course is to give the fundamental mathematical background for cryptography and security. The topics of this course include number theory, modern algebra, probability and information theory, security definition, and the applications on cryptography and security. |

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該系「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 | 學生學習數論、近代代數、機率等相關基本數學背景, 並透過口頭報告與討論進一步學習。 | Students learn the fundamantal mathematical background, including number theory, modern algebra, and probability. Through the oral reports and discussions to enhance depth of students' studies. | P5 | ABDF |
| 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 leans appliaciotns of the fundamental background on cryptography and infromation security. Through the oral reports and discussions to enhance depth of students' studies. | P5 | 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. | P5 | DF |
| | | | | |

| | | | | |
|---|---|---|---|---|
| 4 | 概觀性介紹資訊安全與密碼學的安全性定義。 | Briefly introduction about the security defintion in security and cryptography. | C4 | AD |

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 | 學生學習數論、近代代數、機率等相關基本數學背景，並透過口頭報告與討論進一步學習。 | 分組討論、口頭報告 | 報告、討論、小考、期中考、期末考 |
| 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。 | 分組討論、口頭報告 | 出席率、小考、期中考、期末考 |
| 3 | 增進學生資訊科學專業英文閱讀能力。 | 分組討論、英文教材 | 出席率、討論、小考、期中考、期末考 |
| 4 | 概觀性介紹資訊安全與密碼學的安全性定義。 | 分組討論、口頭報告 | 出席率、討論、小考、期中考、期末考 |

本課程之設計與教學已融入下列本校基本素養與核心能力

| 淡江大學基本素養與核心能力 | 內涵說明 |
|---|---|
| ◆ 表達能力與人際溝通 | 有效運用中、外文進行表達，能發揮合作精神，與他人共同和諧生活、工作及相處。 |
| ◆ 科技應用與資訊處理 | 正確、安全、有效運用資訊科技，並能蒐集、分析、統整與運用資訊。 |
| ◇ 洞察未來與永續發展 | 能前瞻社會、科技、經濟、環境、政治等發展的未來，發展與實踐永續經營環境的規劃或行動。 |
| ◇ 學習文化與理解國際 | 具備因應多元化生活的文化素養，面對國際問題和機會，能有效適應和回應的全球意識與素養。 |
| ◆ 自我了解與主動學習 | 充分了解自我，管理自我的學習，積極發展自我多元的興趣和能力，培養終身學習的價值觀。 |
| ◆ 主動探索與問題解決 | 主動觀察和發掘、分析問題、蒐集資料，能運用所學不畏挫折，以有效解決問題。 |
| ◇ 團隊合作與公民實踐 | 具備同情心、正義感，積極關懷社會，參與民主運作，能規劃與組織活動，履行公民責任。 |
| ◇ 專業發展與職涯規劃 | 掌握職場變遷所需之專業基礎知能，管理個人職涯的職業倫理、心智、體能和性向。 |

授 課 進 度 表

| 週次 | 日期起訖 | 內 容 (Subject/Topics) | 備註 |
|---|---|---|---|
| 1 | 100/09/05～100/09/11 | 課程與數學理論介紹 | |
| 2 | 100/09/12～100/09/18 | 課程與數學理論介紹 | |
| 3 | 100/09/19～100/09/25 | 課程與數學理論介紹 | |
| 4 | 100/09/26～100/10/02 | 課程與數學理論介紹 | |

| | | | |
|---|---|---|---|
| 5 | 100/10/03～<br>100/10/09 | 小考 | |
| 6 | 100/10/10～<br>100/10/16 | Introduction to Public-Key Cryptography | |
| 7 | 100/10/17～<br>100/10/23 | The RSA Cryptosystem | |
| 8 | 100/10/24～<br>100/10/30 | Public-Key Cryptosystems Based on the Discrete | |
| 9 | 100/10/31～<br>100/11/06 | 期中考 | |
| 10 | 100/11/07～<br>100/11/13 | Elliptic Curve Cryptosystems | |
| 11 | 100/11/14～<br>100/11/20 | Digital Signatures | |
| 12 | 100/11/21～<br>100/11/27 | Hash Functions | |
| 13 | 100/11/28～<br>100/12/04 | 小考 | |
| 14 | 100/12/05～<br>100/12/11 | Message Authenticaiton Codes (MACs) | |
| 15 | 100/12/12～<br>100/12/18 | Key Establishment | |
| 16 | 100/12/19～<br>100/12/25 | More About Block Ciphers | |
| 17 | 100/12/26～<br>101/01/01 | 期末考 | |
| 18 | 101/01/02～<br>101/01/08 | 安全性理論介紹 | |

| | |
|---|---|
| 修課應<br>注意事項 | |
| 教學設備 | 電腦、投影機 |
| 教材課本 | Understanding Cryptography: A Textbooks for Students and Practitioncers, Chrsitof Paar and Jan Pelzl, Springer, 2010. |
| 參考書籍 | Cryptography and Network Security: Principles and Practice, 5th Ed., William Stallings, Pearson, 2010.<br>"Introduction to Cryptography: Principle and Applications," 2nd Ed., Hans Delfs and Helmut Knebl, New York: Springer-Verlag, 2007.<br>"Protocols for Authentication and Key Establishment," Colin Boyd and Anish Mathuria, New York: Springer, 2003. |
| 批改作業<br>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<br>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。** |