# 淡江大學１０８學年度第１學期課程教學計畫表

| | | | |
|---|---|---|---|
| 課程名稱 | 資訊安全導論<br>INTRODUCTION TO INFORMATION SECURITY | 授課教師 | 黃心嘉<br>HWANG SHIN-JIA |
| 開課系級 | 資工三Ｐ<br>TEIXB3P | 開課資料 | 以實整虛課程<br>選修 單學期 3學分 |

系（ 所） 教 育 目 標

一、通達專業知能。

二、熟練實用技能。

三、展現創意成果。

本課程對應院、系(所)核心能力之項目與比重

E. 資訊技能就業能力。(比重：100.00)

本課程對應校級基本素養之項目與比重

2. 資訊運用。(比重：100.00)

| | |
|---|---|
| 課程簡介 | 本課程為資訊安全與密碼學的入門課程, 學生可以學到資訊安全與密碼學的基本知識, 與相關的背景理論, 足以研習網路安全或系統安全等課程 |
| | This course introduce the basic concpets and theory for information security and cryptography. After this course, stundents will be ability to join the course about Intenet security or system security. |

本課程教學目標與認知、情意、技能目標之對應

將課程教學目標分別對應「認知（Cognitive）」、「情意（Affective）」與「技能(Psychomotor)」的各目標類型。

一、認知(Cognitive)：著重在該科目的事實、概念、程序、後設認知等各類知識之學習。
二、情意(Affective)：著重在該科目的興趣、倫理、態度、信念、價值觀等之學習。
三、技能(Psychomotor)：著重在該科目的肢體動作或技術操作之學習。

| 序號 | 教學目標(中文) | 教學目標(英文) |
|---|---|---|
| 1 | 學生學習資訊安全觀念與架構。 | Students learns the information security concept and architecture. |
| | | |

| | | |
|---|---|---|
| 2 | 學生學習數論與有限體的基本觀念。 | Studnets learn basic concepts in number theory and finite fields. |
| 3 | 學生學習對稱式密碼系統與操作模式，也要求自行了解。 | Students learn sysmetric cryptosystems and operation modes. Students are required to first collect specificaiton about AES and then coding AES cryptosystem. |
| 4 | 學生學習公開金鑰密碼學，包含公開金鑰密碼系統、數位簽章法、雜湊函數與訊息檢查碼。 | Sduents learns Public-key crypography inlcuding public-key cryptosystems,digitial signature schemes,hash functions, and message authentication codes. |

教學目標之目標類型、核心能力、基本素養教學方法與評量方式

| 序號 | 目標類型 | 院、系(所)核心能力 | 校級基本素養 | 教學方法 | 評量方式 |
|---|---|---|---|---|---|
| 1 | 認知 | E | 2 | 講述、討論 | 測驗 |
| 2 | 認知 | E | 2 | 講述、討論 | 測驗 |
| 3 | 技能 | E | 2 | 講述、討論 | 測驗、作業 |
| 4 | 技能 | E | 2 | 講述、討論 | 測驗 |

授 課 進 度 表

| 週次 | 日期起訖 | 內 容 (Subject/Topics) | 備 註<br>(採數位教學之週次，請填「線上非同步教學」) |
|---|---|---|---|
| 1 | 108/09/09～108/09/15 | 課程介紹、單元一Computer and Network Security Concepts | |
| 2 | 108/09/16～108/09/22 | 單元三Classical Encryption Techniques 單元四Block Ciphers and the Data Encryption Standard | 線上非同步教學 |
| 3 | 108/09/23～108/09/29 | 單元二 Introduction to Number Theory | 線上非同步教學 |
| 4 | 108/09/30～108/10/06 | 單元二 Introduction to Number Theory | |
| 5 | 108/10/07～108/10/13 | 單元五 Finite Fields | |
| 6 | 108/10/14～108/10/20 | 單元五 Finite Fields | |
| 7 | 108/10/21～108/10/27 | 單元六Advance Encryption Standard | 小考 |
| 8 | 108/10/28～108/11/03 | 單元六 Advance Encryption Standard | |
| 9 | 108/11/04～108/11/10 | 單元六 Advance Encryption Standard | 繳交AES規格書報告 |
| 10 | 108/11/11～108/11/17 | 期中考試週 | |
| 11 | 108/11/18～108/11/24 | 單元七 Block Cipher Operation | |
| 12 | 108/11/25～108/12/01 | 單元七 Block Cipher Operation | |
| 13 | 108/12/02～108/12/08 | 單元九Public-Key Cryptography and RSA | |

| | | | |
|---|---|---|---|
| 14 | 108/12/09～<br>108/12/15 | 單元十Other Public-Key Cryptosystems | 線上非同步教學 |
| 15 | 108/12/16～<br>108/12/22 | 單元十Other Public-Key Cryptosystems | 線上非同步教學 |
| 16 | 108/12/23～<br>108/12/29 | 單元十一Cryptographic Hash Functions | 小考。AES分組程式作業驗收 |
| 17 | 108/12/30～<br>109/01/05 | 單元十二Message Authentication Codes | AES分組程式作業驗收 |
| 18 | 109/01/06～<br>109/01/12 | 期末考試週(本學期期末考試日期為:109/1/3-109/1/9) | |

| | |
|---|---|
| 修課應注意事項 | ※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。<br>1.補考/補點須提出校方證明，經老師許可後，方可補考/補點，並在一週內完成補考/補點，逾期不候，且補考成績超過60分部分打八折。<br>2.本課程大量使用iClass公告注意事項或舉行臨時小考，請同學務必注意iClass的電子郵件通知與公告。<br>3.各項成績會在iClass上公告，請在當公告當周更正成績，逾期不候。<br>4.期末與學期成績會在期末考後5天內公佈，有問題者須於公佈當天找老師，逾期不候。<br>5.若是整組作業，需要整組出席評分時，若有小組非不可避免因素而缺席，缺席者該次作業零分。 |
| 教學設備 | 電腦、投影機 |
| 教科書與教材 | Cryptography and Network Security: Principles and Practice, 7th Ed., William Stallings, Pearson, (Global Edition) |
| 參考文獻 | The Design of RijndaeL: AES - The Advanced Encryption Standard, Joan Daemen and Vincent Rijmen, Springer; 2002 Ed. |
| 批改作業篇數 | 2 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： 10.0 %　◆平時評量：20.0 %　◆期中評量：20.0 %<br>◆期末評量： %<br>◆其他〈書面(25%)與程式作業(25%)〉：50.0 % |
| 備　考 | 1.「教學計畫表管理系統」網址：https://info.ais.tku.edu.tw/csp 或由教務處首頁→教務資訊「教學計畫表管理系統」進入。<br>2.依「專科以上學校遠距教學實施辦法」第2條規定：「本辦法所稱遠距教學課程，指每一科目授課時數二分之一以上以遠距教學方式進行」。<br>3.依「淡江大學數位教學施行規則」第3條第2項，本校遠距教學課程須為「於本校遠距教學平台或同步視訊系統進行數位教學之課程。授課時數包含課程講授、師生互動討論、測驗及其他學習活動之時數」。<br>4.如有課程臨時異動(含遠距教學、以實整虛課程之上課時間及教室異動)，請依規定向教務處提出申請。<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。** |