淡江大學１０３學年度第１學期課程教學計畫表

課程名稱	資訊安全導論 INTRODUCTION TO INFORMATION SECURITY	授課教師	黃心嘉 HWANG SHIN-JIA
開課系級	資工三Ｐ TEIXB3P	開課資料	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。

系（ 所 ） 核 心 能 力

A. 程式設計應用能力。

B. 數學推理演繹能力。

C. 資訊系統實作能力。

D. 網路技術應用能力。

E. 資訊技能就業能力。

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	學生學習資訊安全觀念與架構。	Students learns the information security concept and architecture.	A3	E
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.	P4	E
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.	P5	E
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.	P3	E

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	學生學習資訊安全觀念與架構。	講述	上課表現
2	學生學習數論與有限體的基本觀念。	講述、問題解決	紙筆測驗
3	學生學習對稱式密碼系統與操作模式, 也要求自行了解。	講述、分組程式作業	紙筆測驗、實作、報告
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。	講述	紙筆測驗

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	103/09/15～103/09/21	課程介紹、單元一Computer security overview	
2	103/09/22～103/09/28	單元二Classical Encryption Techniques	
3	103/09/29～103/10/05	單元三Block Ciphers and the Data Encryption Standard	
4	103/10/06～103/10/12	單元四Basic Concepts in Number Theory and Finite Fields	
5	103/10/13～103/10/19	單元四Basic Concepts in Number Theory and Finite Fields	
6	103/10/20～103/10/26	單元四Basic Concepts in Number Theory and Finite Fields	
7	103/10/27～103/11/02	單元五Advance Encryption Standard	小考
8	103/11/03～103/11/09	單元五Advance Encryption Standard	
9	103/11/10～103/11/16	單元六Block Cipher Operations	繳交AES規格書報告
10	103/11/17～103/11/23	期中考試週	
11	103/11/24～103/11/30	單元七Pseudorandom Number Generation	
12	103/12/01～103/12/07	單元八Introduction to Number Theory	

13	103/12/08～ 103/12/14	單元九Public-Key Cryptography and RSA	
14	103/12/15～ 103/12/21	單元十Other Public-Key Cryptosystems	
15	103/12/22～ 103/12/28	單元十一Cryptographic Hash Functions	小考
16	103/12/29～ 104/01/04	單元十二Message Authentication Codes	AES分組程式作業驗收
17	104/01/05～ 104/01/11	單元十三Digital Signautres	AES分組程式作業驗收
18	104/01/12～ 104/01/18	期末考試週	

修課應注意事項	1.補考/補點須一週內提出校方證明，經老師許可方可補考/補點，且補考成績超過60分的部分打八折，逾期不候。 2.成績在期中/末考前各公佈一次，請在當周更正成績，逾期不候。 3.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。 4.請尊重智慧財產權。
教學設備	電腦、投影機
教材課本	Cryptography and Network Security: Principles and Practice, 5th Ed., William Stallings, Pearson, 2010
參考書籍	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： 5.0 % ◆平時評量：25.0 % ◆期中評量：20.0 % ◆期末評量： % ◆其他〈書面(20%)與程式作業(30%)〉：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。 **※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。**