淡江大學９９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	資訊三Ｐ TEIXB3P	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	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、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	學生學習資訊安全觀念與架構。	Students learns the information security concept and architecture.	A3	HI
2	學生學習數論與有線體的基本觀念。	Studnets learn basic concepts in number theory and finite fields.	P4	CD
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	ACDEFGI
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	CD
5	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.	P4	GI

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	學生學習資訊安全觀念與架構。	課堂講授、程式作業	出席率、報告、小考、期中考、程式作業

2	學生學習數論與有線體的基本觀念。	課堂講授	出席率、期中考
3	學生學習對稱式密碼系統與操作模式，也要求自行了解	課堂講授、分組程式作業	出席率、報告、期中考、分組程式作業
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。	課堂講授	出席率、小考、期中考
5	增進學生資訊科學專業英文閱讀能力。	課堂講授	原文教材與考卷

授 課 進 度 表

週次	日期	內 容 (Subject/Topics)	備註
1	09/13	課程介紹、單元一Computer security overview	
2	09/20	單元二Classical Encryption Techniques	
3	09/27	單元二Classical Encryption Techniques	
4	10/04	單元三Block Ciphers and the Data Encryption Standard	
5	10/11	單元四Basic Concepts in Number Theory and Finite Fields	
6	10/18	單元四Basic Concepts in Number Theory and Finite Fields	
7	10/25	單元四Basic Concepts in Number Theory and Finite Fields	
8	11/01	單元五Advance Encryption Standard	
9	11/08	單元六Block Cipher Operations	繳交AES規格書報告。
10	11/15	期中考試週	
11	11/22	單元七Pseudorandom Number Generation	
12	11/29	單元八Introduction to Number Theory	
13	12/06	單元九Public-Key Cryptography and RSA	
14	12/13	單元十Other Public-Key Cryptosystems	
15	12/20	單元十一Cryptographic Hash Functions	小考
16	12/27	單元十二Message Authentication Codes	
17	01/03	單元十三Digital Signautres	AES分組程式作業驗收開始
18	01/10	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。
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
參考書籍	
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	◆平時考成績：10.0 %　◆期中考成績：20.0 %　◆期末考成績： % ◆作業成績： 70.0 % ◆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。 **※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。**