淡江大學１０２學年度第２學期課程教學計畫表

課程名稱	網路安全技術與應用 TECHNOLOGIES ON NETWORK SECURITY AND APPLICATION	授課教師	李鴻璋 LEE HUNG-CHANG
開課系級	資管一碩專班Ａ TLMXJ1A	開課資料	選修 單學期 3學分

系（ 所） 教 育 目 標

致力於資訊科技與經營管理知識之科際整合研究發展，為國家與社會培育兼具資訊技術能力與現代管理知識的中高階人才。

系（ 所） 核 心 能 力

A. 現代管理知識應用。
B. 邏輯思考。
C. 關鍵分析。
D. 結合資訊技術與管理。
E. 研究與創新。
F. 資料分析與應用。
G. 資通安全管理。
H. 言辭與文字表達。

課程簡介	本課程介紹使用在資通安全重要安全技術, 如傳統秘密金鑰系統、現代公開金鑰系統、雜湊與亂數演算法、認證協定與系統與公鑰基礎架構等
	This course introduces the essential technologies on Information security. Theses includes the traditional symmetric system, modern public key system, hashing function, and authentication protocols etc.

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	資訊與網路安全概念	Information and network security concept	C2	ADE
2	傳統秘密金鑰系統	traditional symmetric systems	P3	BCDEG
3	公開金鑰系統	public key systems	P3	BCDG
4	雜湊與亂數演算法	Hashing functions	P3	DEG
5	認證協定與系統與公鑰基礎架構	authentication protocols and PKI	C2	ABDE
6	資訊科技產品與英文之表達	State-of-the-art 3C product and English Expression	P3	ABCDEH
7	防火牆架構與封包過濾	Firewall architecture and Packet Filter	P3	BCDG

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	資訊與網路安全概念	講述、討論	紙筆測驗、上課表現
2	傳統秘密金鑰系統	講述、討論	紙筆測驗、上課表現
3	公開金鑰系統	講述、討論	紙筆測驗、上課表現
4	雜湊與亂數演算法	講述、討論	紙筆測驗、上課表現
5	認證協定與系統與公鑰基礎架構	講述、討論	紙筆測驗、上課表現
6	資訊科技產品與英文之表達	討論、賞析	報告、上課表現
7	防火牆架構與封包過濾	講述、討論	紙筆測驗、實作

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	課程簡介與網路安全技術概論與專題報告	
2	103/02/24～103/03/02	資訊與網路安全簡介與專題報告	
3	103/03/03～103/03/09	OSI安全架構簡介與專題報告	
4	103/03/10～103/03/16	傳統秘密金鑰系統與專題報告	
5	103/03/17～103/03/23	傳統秘密金鑰系統-DES、RC5、AES與專題報告	
6	103/03/24～103/03/30	進階秘密金鑰系統-Triple DES與專題報告	
7	103/03/31～103/04/06	整數數論基礎與專題報告	
8	103/04/07～103/04/13	現代公開金鑰系統-RSA與專題報告	
9	103/04/14～103/04/20	現代公開金鑰系統-ElGamal與專題報告	
10	103/04/21～103/04/27	期中課程了解測驗	
11	103/04/28～103/05/04	雜湊與亂數演算法-MD5, SHA-1與專題報告	
12	103/05/05～103/05/11	訊息確認與專題報告	

13	103/05/12～ 103/05/18	數位簽章、數位憑證與專題報告	
14	103/05/19～ 103/05/25	認證協定與系統與公鑰基礎架構與專題報告	
15	103/05/26～ 103/06/01	網際網路安全(Wireless and 2G、3G security)與專題報告	
16	103/06/02～ 103/06/08	防火牆觀念、架構與專題報告	
17	103/06/09～ 103/06/15	網際網路安全(SSL, IPSec, VPN) 與專題報告	
18	103/06/16～ 103/06/22	期末測驗	

修課應注意事項	
教學設備	電腦、投影機
教材課本	老師自編講義
參考書籍	資訊與網路安全技術 粘添壽、吳順欲著 旗標出版Cryptography and Network Security – Principles and Practices by William Stallings, Pearson publisher.近代密碼學及其應用 賴溪松等編著 松崗書局資訊與網路安全概論黃明祥、林詠章著麥格羅、希爾(McGraw Hill)出版
批改作業篇數	3 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：30.0 % ◆期中評量：30.0 % ◆期末評量： % ◆其他〈報告〉：20.0 %
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。**