淡江大學１０１學年度第１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	資管一碩士班Ａ TLMXM1A	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	本課程介紹使用在網路安全重要安全技術, 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 Network 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	ABCDG
2	傳統秘密金鑰系統	traditional symmetric systems	C2	AB
3	公開金鑰系統	public key systems	C2	BCEFG
4	雜湊與亂數演算法	Hashing functions	C2	AEFG
5	認證協定與系統與公鑰基礎架構	authentication protocols and PKI	C2	EFG
6	科技英文之表達	English Expression in infromation Security Field	P3	EH

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	科技英文之表達	討論、賞析	報告、上課表現

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	
◆ 洞悉未來	
◆ 資訊運用	
◇ 品德倫理	
◆ 獨立思考	
◇ 樂活健康	
◇ 團隊合作	
◇ 美學涵養	

授 課 進 度 表

週次	日期起訖	內 容 (Subject/Topics)	備註
1	101/09/10～101/09/16	課程簡介與網路安全技術概論與英文	
2	101/09/17～101/09/23	資訊與網路安全簡介與英文	
3	101/09/24～101/09/30	OSI安全架構簡介與英文	
4	101/10/01～101/10/07	傳統秘密金鑰系統與英文	
5	101/10/08～101/10/14	傳統秘密金鑰系統-DES、RC5、AES與英文	
6	101/10/15～101/10/21	進階秘密金鑰系統-Triple DES與英文	
7	101/10/22～101/10/28	整數數論基礎與英文	
8	101/10/29～101/11/04	現代公開金鑰系統-RSA與英文	
9	101/11/05～101/11/11	現代公開金鑰系統-ElGamal與英文	
10	101/11/12～101/11/18	期中課程了解測驗	
11	101/11/19～101/11/25	雜湊與亂數演算法-MD5, SHA-1與英文	
12	101/11/26～101/12/02	訊息確認與英文	

13	101/12/03～ 101/12/09	數位簽章、數位憑證與英文	
14	101/12/10～ 101/12/16	認證協定與系統與公鑰基礎架構與英文	
15	101/12/17～ 101/12/23	網際網路安全(Wireless and 2G、3G security)與英文	
16	101/12/24～ 101/12/30	防火牆觀念、架構與英文	
17	101/12/31～ 102/01/06	網際網路安全(SSL, IPSec, VPN) 與英文	
18	102/01/07～ 102/01/13	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	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/index.asp/〉教務資訊「教學計畫表管理系統」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。**