淡江大學１００學年度第１學期課程教學計畫表

課程名稱	資通安全技術專題 TOPICS ON INFORMATION SECURITY TECHNOLOGY	授課教師	李鴻璋 Lee Hung-chang
開課系級	資管一碩士班Ａ TMIXM1A	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該系「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	ABC
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	AB
4	雜湊與亂數演算法	Hashing functions	C2	AB
5	認證協定與系統與公鑰基礎架構	authentication protocols and PKI	C2	AB
6	科技英文之表達	English Expression in infromation Security Field	P3	AGH

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	資訊與網路安全概念	課堂講授	出席率、討論
2	傳統秘密金鑰系統	課堂講授	出席率、討論
3	公開金鑰系統	課堂講授	出席率、討論
4	雜湊與亂數演算法	課堂講授	出席率、討論
5	認證協定與系統與公鑰基礎架構	課堂講授	出席率、討論
6	科技英文之表達	分組討論	出席率、報告

本課程之設計與教學已融入下列本校基本素養與核心能力	
淡江大學基本素養與核心能力	內涵說明
◆ 表達能力與人際溝通	有效運用中、外文進行表達，能發揮合作精神，與他人共同和諧生活、工作及相處。
◆ 科技應用與資訊處理	正確、安全、有效運用資訊科技，並能蒐集、分析、統整與運用資訊。
◇ 洞察未來與永續發展	能前瞻社會、科技、經濟、環境、政治等發展的未來，發展與實踐永續經營環境的規劃或行動。
◇ 學習文化與理解國際	具備因應多元化生活的文化素養，面對國際問題和機會，能有效適應和回應的全球意識與素養。
◇ 自我了解與主動學習	充分了解自我，管理自我的學習，積極發展自我多元的興趣和能力，培養終身學習的價值觀。
◇ 主動探索與問題解決	主動觀察和發掘、分析問題、蒐集資料，能運用所學不畏挫折，以有效解決問題。
◇ 團隊合作與公民實踐	具備同情心、正義感，積極關懷社會，參與民主運作，能規劃與組織活動，履行公民責任。
◇ 專業發展與職涯規劃	掌握職場變遷所需之專業基礎知能，管理個人職涯的職業倫理、心智、體能和性向。

授 課 進 度 表

週次	日期起訖	內 容 (Subject/Topics)	備註
1	100/09/05～100/09/11	課程簡介與網路安全技術概論與英文	
2	100/09/12～100/09/18	資訊與網路安全簡介與英文	
3	100/09/19～100/09/25	OSI安全架構簡介與英文	
4	100/09/26～100/10/02	傳統秘密金鑰系統與英文	
5	100/10/03～100/10/09	傳統秘密金鑰系統-DES、RC5、AES與英文	
6	100/10/10～100/10/16	進階秘密金鑰系統-Triple DES與英文	
7	100/10/17～100/10/23	整數數論基礎與英文	
8	100/10/24～100/10/30	現代公開金鑰系統-RSA與英文	
9	100/10/31～100/11/06	現代公開金鑰系統-ElGamal與英文	
10	100/11/07～100/11/13	期中課程了解測驗	
11	100/11/14～100/11/20	雜湊與亂數演算法-MD5, SHA-1與英文	
12	100/11/21～100/11/27	訊息確認與英文	

13	100/11/28～ 100/12/04	數位簽章、數位憑證與英文	
14	100/12/05～ 100/12/11	認證協定與系統與公鑰基礎架構與英文	
15	100/12/12～ 100/12/18	網際網路安全(Wireless and 2G、3G security)與英文	
16	100/12/19～ 100/12/25	防火牆觀念、架構與英文	
17	100/12/26～ 101/01/01	網際網路安全(SSL, IPSec, VPN) 與英文	
18	101/01/02～ 101/01/08	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	◆平時考成績：20.0 ％ ◆期中考成績：30.0 ％ ◆期末考成績：30.0 ％ ◆作業成績： ％ ◆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。 **※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。**