淡江大學９９學年度第１學期課程教學計畫表

課程名稱	網路安全技術 TECHNOLOGIES ON NETWORK SECURITY	授課教師	李鴻璋 Lee Hung-chang
開課系級	管科一博士班Ａ TMFXD1A	開課資料	選修 單學期 3學分

學 系(門) 教 育 目 標

培育具備優良專業數理分析與邏輯判斷能力之學術人才、高階管理人才及分析幹部，以因應國內及國際企業或是教研機構的需要。

學 生 基 本 能 力

A. 具有博士研究理論及方法學習之能力。
B. 訓練獨立邏輯分析與組織寫作之能力。
C. 培育具有跨領域科際整合之能力。
D. 參與國際學術活動之能力。
E. 參與規畫及執行研究案之能力。
F. 具有外語運用能力。
G. 參與規畫及執行研究案之能力。
H. 具有外語運用能力。

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、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	資訊與網路安全概念	Information and network security concept	C2	AB
2	傳統秘密金鑰系統	traditional symmetric systems	C2	A
3	公開金鑰系統	public key systems	C2	A
4	雜湊與亂數演算法	Hashing functions	C2	A
5	認證協定與系統與公鑰基礎架構	authentication protocols and PKI	C2	A
6	科技英文之表達	English Expression in infromation Security Field	P3	AFH

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

授 課 進 度 表

週次	日期	內 容 (Subject/Topics)	備註
1	09/13	課程簡介與網路安全技術概論與英文	

2	09/20	資訊與網路安全簡介與英文	
3	09/27	OSI安全架構簡介與英文	
4	10/04	傳統秘密金鑰系統與英文	
5	10/11	傳統秘密金鑰系統-DES、RC5、AES與英文	
6	10/18	進階秘密金鑰系統-Triple DES與英文	
7	10/25	整數數論基礎與英文	
8	11/01	現代公開金鑰系統-RSA與英文	
9	11/08	現代公開金鑰系統-ElGamal與英文	
10	11/15	期中考試週	
11	11/22	雜湊與亂數演算法-MD5, SHA-1與英文	
12	11/29	訊息確認與英文	
13	12/06	數位簽章、數位憑證與英文	
14	12/13	認證協定與系統與公鑰基礎架構與英文	
15	12/20	網際網路安全(Wireless and 2G、3G security)與英文	
16	12/27	防火牆觀念、架構與英文	
17	01/03	網際網路安全(SSL, IPSec, VPN) 與英文	
18	01/10	期末考週	

修課應注意事項	
教學設備	電腦、投影機
教材課本	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.
參考書籍	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	4 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：40.0 % ◆期末考成績： % ◆作業成績： 20.0 % ◆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。**