

淡江大學 106 學年度第 2 學期課程教學計畫表

課程名稱	資訊安全概論	授課 教師	李鴻璋 LEE HUNG-CHANG
	INTRODUCTION TO INFORMATION SECURIT		
開課系級	資管三 C	開課 資料	必修 單學期 2學分
	TLMXB3C		
系 (所) 教育目標			
<p>一、精進資訊管理知能。</p> <p>二、提升資訊科技專業。</p> <p>三、獨立思考邏輯分析。</p> <p>四、強化團隊合作能力。</p> <p>五、重視企業資訊倫理。</p> <p>六、培育全球化世界觀。</p>			
系 (所) 核心能力			
<p>A. 問題分析與關鍵思考。</p> <p>B. 企業基礎與實務知識。</p> <p>C. 資訊系統運用。</p> <p>D. 程式設計。</p> <p>E. 網路系統規劃。</p> <p>F. 資料庫設計與管理。</p> <p>G. 資訊系統分析、設計與整合。</p> <p>H. 專案管理。</p>			
課程簡介	<p>本課程介紹資通安全重要觀念與常用之安全技術。 資通安全重要觀念如資訊中心安全管理與實體安全，使用者身分鑑別，作業系統安全等 常用之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</p>		
	<p>This course introduces the essential concept of information security and technologies on Information/Network security. Information security concept includes information center management and physical security, user authentication, Operationg Security, etc. Technologies on Information/Network security includes the traditional symmetric system, modern public key system, hashing function, and authentication protocols etc.</p>		

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	資訊安全威脅與架構	Information Security Threat and Frame work	C2	CG
2	使用者身分鑑別	User Authentication	C3	CG
3	作業中系統安全	System Security in Operating processing	C4	CG
4	秘密金鑰系統	Secret Key Cryptosystem	C3	CG
5	認證協定與系統與公鑰基礎架構	authentication protocols and PKI	P3	CG
6	電子商務與資料庫安全	Electronic Commerce security and Database security	C3	CG

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	資訊安全威脅與架構	講述、討論、賞析	紙筆測驗、報告、上課表現
2	使用者身分鑑別	講述、討論、賞析	紙筆測驗、上課表現
3	作業中系統安全	講述、討論	紙筆測驗、上課表現
4	秘密金鑰系統	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	電子商務與資料庫安全	講述、討論	紙筆測驗、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	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	107/02/26~ 107/03/04	課程簡介與資通安全概論	
2	107/03/05~ 107/03/11	資訊安全技術-傳統秘密金鑰系統-DES	
3	107/03/12~ 107/03/18	資訊安全技術-3DES, RC5	
4	107/03/19~ 107/03/25	資訊安全技術-AES	
5	107/03/26~ 107/04/01	資訊安全技術-AES operation mode	
6	107/04/02~ 107/04/08	離散數論基礎	
7	107/04/09~ 107/04/15	現代公開金鑰系統-RSA	
8	107/04/16~ 107/04/22	現代公開金鑰系統-ElGamal, DSS	
9	107/04/23~ 107/04/29	金鑰管理及認證中心	
10	107/04/30~ 107/05/06	期中考試週	
11	107/05/07~ 107/05/13	資訊安全管理專題與報告1	
12	107/05/14~ 107/05/20	資訊安全管理專題與報告2	

13	107/05/21~ 107/05/27	資訊安全管理專題與報告3	
14	107/05/28~ 107/06/03	資訊安全管理專題與報告4	
15	107/06/04~ 107/06/10	資訊安全管理專題與報告5	
16	107/06/11~ 107/06/17	資訊安全管理專題與報告6	
17	107/06/18~ 107/06/24	資訊安全管理專題與報告7	
18	107/06/25~ 107/07/01	期末考試週	
修課應 注意事項	堅持才會成功。基本要點是不遲到及不缺席。		
教學設備	電腦、投影機、其它(專題報告與分享)		
教材課本	1. 講義 (必備) 2. 資訊與網路安全概論 黃明祥、林詠章著 高立圖書 3. 資訊安全概論與實務(第三版) 潘天佑 碁峰書局 4. 資訊安全管理認證實戰寶典(第二版) 林文恭等 碁峰書局 5. 資訊安全 Merkow&Breithaut 柳望君譯 滄海書局		
參考書籍	1. 資訊與網路安全技術 粘添壽、吳順欲著 旗標出版 2. 近代密碼學及其應用 賴溪松等編著 松崗書局		
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： 10.0 % ◆平時評量： % ◆期中評量：30.0 % ◆期末評量：20.0 % ◆其他〈專題報告(20%)與實習課(20%)〉：40.0 %		
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。		