101-1 大葉大學 完整版課綱

基本資訊			
課程名稱	電子商務安全	科目序號 / 代號	2110 / IGR6053
開課系所	資訊管理學系碩士班	學制 / 班級	研究所碩士班1年1班
任課教師	曹偉駿	專兼任別	專任
必選修 / 學分數	選修 / 3	畢業班 / 非畢業班	非畢業班
上課時段 / 地點	(二)234 / J117	授課語言別	中文

課程簡介

A. 資訊管理學系之教育目標：
1. 管理知識與資訊專業能力
2. 理論基礎與實務實作能力
3. 研究分析與跨域整合能力
4. 企業e化之應用能力

B. 管理學院與資訊管理學系之核心能力：
1. 專業能力: 資管系強調以下之專業能力
(1)管理專業
(2)研究專業：(a) 大學部：整合應用專業; (b) 研究所：學術研究專業
(3)資訊技術專業
2. 解決問題能力(執行力、決策力、洞析力)：資管系強調「分析能力(探索的能力)」
3. 溝通能力(傾聽能力、表達能力)：資管系強調「協調能力：技術與管理間的協調能力」
4. 倫理觀(社會倫理、企業倫理、研究倫理)

C. 資訊管理學系課程特色：
1.強調學生在服務業管理的 Know how
2.強化學生在服務業e化的應用能力
3.培養學生在資訊科技的規劃、分析、設計與操作之應用能力

本課程目標：
根據管理學院與資管系之教育目標(A1、A2、A3、A4)及發展特色(C2、C3)，本課程可使學生於修課中了解資訊安全在目前電腦與通訊時代中的重要性，並透過密碼技術的包裝，使得電子商務訊息、文件的儲存、傳播能獲得最完善的保護。
本課程對核心能力培養如下:
(1) 專業能力: 學習這門課後，學生將在資訊安全、網路安全與電子商務安全應用上有明顯的專業素養與相關能力。
(2) 洞析能力: 培養探究如何提升電子商務相關應用的資訊安全技術與管理之能力。
(3) 溝通能力: 培養團隊成員進行溝通協調以完成本課程期末專題的能力。
(4) 表達能力: 培養各團隊表達成員間共同合作所獲致期末專題成果的能力。

課程大綱

1. 電子商務安全整體架構
2. 基礎數學
3. 對稱式密碼系統 – DES、Triple DES、IDEA and AES
4. 非對稱密碼系統 – RSA、ElGamal and Elliptic Curve Cryptosystem
5. 赫序函數(Hash Functions)及數位簽章演算法
6. 通行碼識別與資源存取控制
7. 個體鑑別與金鑰交換協定
8. 秘密分享機制與應用
9. 群體導向密碼系統 – 會議金鑰分配系統、安全廣播系統、多重簽章與群體簽章
10. 密碼學技術未來發展趨勢 – 自我認證公開金鑰系統、簽密法
11. Web安全機制 – SSL/TLS、SET
12. 網際網路安全機制 – IPSec
13. 無線區域網路安全機制(WLAN) – IEEE 802.11i
14. 行動電子商務安全機制 – WAP/WTLS、電子付款、電子拍賣
15. 電子投票系統/電子郵件安全技術
16. 防火牆技術
17. 病毒、病蟲、駭客入侵等系統安全防範機制

基本能力或先修課程

計算機概論、電腦網路

課程與系所基本素養及核心能力之關連

- 理論演繹與歸納分析
- 企業ｅ化系統研發能力
- 資訊技術開發能力
- 問題分析與解決能力
- 專案規劃與執行能力
- 專業閱讀與撰寫能力
- 溝通與表達能力

教學計畫表

系所核心能力	權重(%)【A】	檢核能力指標(績效指標)	教學策略	評量方法及配分權重	核心能力學習成績【B】	期末學習成績【C=B*A】

理論演繹與歸納分析	25%	1.具備資訊管理的主要理論知識。 2.能以理論為依據推論未知的事實。 3.能利用科學分析某些現象之間的相關屬性。	講述法 小組討論 小組合作 學生上台報告 專題報告	分組報告: 20% 期中考: 30% 期末考: 30% 作業: 10% 課程參與度: 10%	加總: 100	25
資訊技術開發能力	25%	1.具備最新的資訊管理技術。 2.能利用資訊技術設計與實作應用系統。	講述法 小組討論 小組合作 學生上台報告 專題報告	分組報告: 20% 期中考: 30% 期末考: 30% 作業: 10% 課程參與度: 10%	加總: 100	25
問題分析與解決能力	25%	1.能定義問題及改善目標。 2.能收集解決問題的相關資料。 3.能應用科學方法解析資料。 4.能設計並實施改善問題的方案。	講述法 小組討論 小組合作 學生上台報告 專題報告	分組報告: 20% 期中考: 30% 期末考: 30% 作業: 10% 課程參與度: 10%	加總: 100	25
專業閱讀與撰寫能力	25%	1.能理解、使用及反思專業性文章。 2.能書寫流暢的專業性文章。	講述法 小組討論 小組合作 學生上台報告 專題報告	分組報告: 20% 期中考: 30% 期末考: 30% 作業: 10% 課程參與度: 10%	加總: 100	25

成績稽核

期中考: 30%
期末考: 30%
分組報告: 20%
作業: 10%
課程參與度: 10%

教科書(尊重智慧財產權，請用正版教科書，勿非法影印他人著作)

書名	作者	譯者	出版社	出版年
Network Security Essentials: Applications and Standards	William Stallings		Prentice-Hall Inc.	2007
Cryptography and Network Security: Principles and Practice	William Stallings		Prentice-Hall Inc.	2006

參考教材及專業期刊導讀(尊重智慧財產權，請用正版教科書，勿非法影印他人著作)				
書名	作者	譯者	出版社	出版年
Secure Computers and Networks: Analysis, Design, and Implementation	E. A. Fisch		CRC Press	2003

上課進度		分配時數(%)				
週次	教學內容	講授	示範	習作		實驗	其他
1	電子商務安全整體架構(1)	0	0	0	0	0
2	電子商務安全整體架構(2)	0	0	0	0	0
3	電子商務安全整體架構(3)	0	0	0	0	0
4	對稱式密碼系統 — DES、Triple DES、IDEA and AES	0	0	0	0	0
5	非對稱密碼系統 — RSA、ElGamal and Elliptic Curve Cryptosystem	0	0	0	0	0
6	赫序函數(Hash functions)及數位簽章演算法	0	0	0	0	0
7	通行碼識別與資源存取控制	0	0	0	0	0
8	Midterm paper presentation(1)	0	0	0	0	0
9	Midterm paper presentation(2)	0	0	0	0	0
10	秘密分享機制與應用	0	0	0	0	0
11	密碼學技術未來發展趨勢 — 自我認證公開金鑰系統、簽密法	0	0	0	0	0
12	行動電子商務安全機制 — WAP/WTLS、電子付款、電子拍賣	0	0	0	0	0
13	無線區域網路安全機制(WLAN)	0	0	0	0	0
14	電子投票系統/電子郵件安全技術	0	0	0	0	0
15	防火牆技術與病毒、病蟲、駭客入侵等系統安全防範機制	0	0	0	0	0
16	Final paper presentation(1)	0	0	0	0	0
17	Final paper presentation(2)	0	0	0	0	0
18	Final exam	0	0	0	0	0