表 A10-1 一般及專業理論課程綱要表

系科名稱： 資訊管理系

科目名稱：資訊安全

英文科目名稱：Information Security

學年、學期、學分數：	第四學年、第一學期、3 學分

先修科目或先備能力：

教學目標：

資訊安全與隱私問題是電腦與通訊網路系統中相當重要的課題。本課程旨在使學生了解在電腦與通訊網路上安全環境之設立，並能實際應用於資訊保護系統之設計。

教材大綱：

1、網路安全威脅 2、密碼理論 3、傳統式和公開式密碼 4、密碼應用技術和實例 5、公開金鑰基礎建設(PKI) 6、IP Security

單元主題	內容綱要	教學參考 節數	備註
資訊安全的簡介	了解何謂資訊安全	3	
古典加密技術	古典加密技術-取代和置換	3	
區段加密與資料加密標準	DES 的介紹	6	
有限體	Finite Field 的介紹	3	
進階加密標準	AES 的介紹	6	
使用對稱式加密達成保密性	對稱式加密系統的介紹	3	
數論介紹		3	
公開鑰匙密碼學與RSA	RSA 的介紹	3	
鑰匙管理與其他的公開鑰匙密碼系統	公開金鑰基礎建設與RSA 的介紹	6	
雜湊演算法	SHA-1 和MD5 的介紹	3	
訊息確認與雜湊函數	訊息確認碼的介紹	3	
數位簽章與確認性協定	數位簽章的應用	3	
確認性應用		3	
IP 安全機制	IPSec 的介紹	3	
電子郵件的安全性		3	
合計		54	

※教學目標(歸納為四項)：分別為知識(Knowledge)、技能(Skills)、態度(Attitude)、其他各一項

※單元主題：為各項知能之彙整

※內容綱要：為各項知能即一般知識、職業知識、態度；專業技術安全知識；專業基礎知識，加上補充之知能（表 4-18 上未列，但為達知識或技能的完整性課程中需教授之能力），撰寫方式係以不含動詞的知能內容方式呈現

※三者之關係：教學目標＞單元主題＞內容綱要

檢核項目	**是否符合**
1.是否將科目名稱、上課時數及學分數填入本表	是☑ 否☐
2.是否將教學目標、綱要名稱或單元名稱填入本表	是☑ 否☐
3.所填入的行業知能是否有考慮學生學習的順序性、邏輯性、連貫性、完整性	是☑ 否☐
4.除了表 4-16 所敘述的行業知能，是否有考慮到其他的知能，以成為一門完整學科	是☑ 否☐