0971學期 課程基本資料

系所 / 年級	資科系碩士班 1年級	課號 / 班別	61M00031 / A
學分數	3學分	選 / 必修	選修
科目中文名稱	資訊安全	科目英文名稱	Information security
主要授課老師	劉兆樑	開課期間	一學期
人數上限	19 人	已選人數	19人

起始週 / 結束週 / 上課地點 / 上課時間

第1週 / 第18週 / I428 / 星期2第07節
第1週 / 第18週 / I428 / 星期2第08節
第1週 / 第18週 / I428 / 星期2第09節

教學綱要

一、教學目標(Objective)	使學生了解資訊安全之基本概念以及常用之數學技術，以期同學對資訊安全有整體的概念。同時介紹密碼學運用到資訊安全領域的相關技術，內容包含訊息確認、數位簽章、數位憑證、認證系統與公鑰基礎架構等。
二、先修科目(Pre Course)	
三、教材內容(Outline)	讓學生瞭解資訊安全理論基礎，透過介紹各類密碼系統後進而瞭解各自優缺點與應用範疇，最後具備把資訊安全觀念應用於各領域之基本能力。
四、教學方式(Teaching Method)	講授、研討
五、參考書目(Reference)	網路安全精要： 標準與應用賴榮樞譯普林斯頓國際有限公司 http://williamstallings.com/NetSec2e.html 近代密碼學及其應用賴溪松、韓亮、張真誠旗標出版公司

2008/9/17	導論	劉兆樑
2008/9/24	對稱式加密法（DES）	劉兆樑
2008/10/1	對稱式加密法（DES）	劉兆樑
2008/10/8	對稱式加密法(AES)	劉兆樑
2008/10/15	對稱式加密法(AES)	劉兆樑
2008/10/22	對稱式加密法(Blowfish & RC5)	劉兆樑
2008/10/29	訊息認證	劉兆樑
2008/11/5	安全雜湊函數及HMAC	劉兆樑

六、教學進度**(Syllabi)**

2008/11/12	期中考	劉兆樑
2008/11/19	公開金鑰加密法（原理）	劉兆樑
2008/11/26	公開金鑰加密法（演算法）	劉兆樑
2008/12/3	數位簽章, 金鑰管理	劉兆樑
2008/12/10	認證之應用	劉兆樑
2008/12/17	電子郵件安全（PGP）	劉兆樑
2008/12/24	電子郵件安全（S/MIME）	劉兆樑
2008/12/31	IP安全	劉兆樑
2009/1/7	期末研討	劉兆樑
2009/1/14	期末研討	劉兆樑

七、評量方式**(Evaluation)**

平時成績30% 期中考40% 期末報告30%

八、講義位址**(http://)**

九、教育目標

重新查詢

亞洲大學 41354 台中市霧峰區柳豐路500號 TEL: 886 + (0)4 + 2332-3456 FAX: 886 + (0)4 + 2331-6699