

重新查詢

友善列印

0971學期 課程基本資料

系所 / 年級	資工系 3年級	課號 / 班別	64U00044 / A
學分數	3學分	選 / 必修	選修
科目中文名稱	密碼學	科目英文名稱	Cryptography
主要授課老師	陳興忠	開課期間	一學期
人數上限	68 人	已選人數	69人

起始週 / 結束週 / 上課地點 / 上課時間

第1週 / 第18週 / I526 / 星期二第05節
第1週 / 第18週 / I526 / 星期二第06節
第1週 / 第18週 / I526 / 星期二第07節

請各位同學遵守智慧財產權觀念；請勿非法影印。

教學綱要

一、教學目標(Objective)

本課程的教學目標是引導並訓練學生學會密碼學之基本概念及常用之技術，使同學能完整的掌握到當代密碼學的基礎理論與相關應用方法。其中特別訓練學生具備密碼學的數理基礎素養，能進一步推導密碼學一般演算法的能力，例如秘密金鑰系統、公開金鑰系統、秘密分享、橢圓曲線密碼、

二、先修科目(Pre Course)

三、教材內容(Outline)

本課程的授課主要目的為，引導學生了解密碼學之基本概念及常用之技術，希望能使同學對當代密碼學的基礎與應用於資訊安全相關技術之推導有一完整的概念。本課程的科目概要是以下列主題為：1. 密碼學概論 2. 密碼學數學基礎 3. 密碼學的基礎與技術 4. 公開金鑰基礎建設 5

四、教學方式(Teaching Method)

講授、媒體運用、實(驗)習、專題實作、研討

五、參考書目(Reference)

電腦鑑識與數位證據--資安技術、科技犯罪的預防、鑑定與重建現場王旭正、柯永瀚博碩文化

2008/9/17	密碼學概論	陳興忠
2008/9/24	密碼學數學基礎	陳興忠
2008/10/1	密碼學的基礎與技術	陳興忠
2008/10/8	公開金鑰基礎建設	陳興忠
2008/10/15	橢圓曲線密碼	陳興忠
2008/10/22	數位簽章	陳興忠
2008/10/29	電子付款與交易證據	陳興忠
2008/11/5	期中考	陳興忠

六、教學進度(Syllabi)

2008/11/12	量子密碼	陳興忠
2008/11/19	秘密分享 I	陳興忠
2008/11/26	秘密分享 II	陳興忠
2008/12/3	User Authentication Algorithms I	陳興忠
2008/12/10	User Authentication Algorithms II	陳興忠
2008/12/17	The Security Issues in WLAN	陳興忠
2008/12/24	The Security Issues in 2G-GSM	陳興忠
2008/12/31	The Security Issues 3G/3.5G-UMTS	陳興忠
2009/1/7	The Security Issues in WiMAX	陳興忠
2009/1/14	期末考	陳興忠

七、評量方式(Evaluation)

評分方式: - 出席率: 25 % - 平時作業與測驗: 15 % - 期中考: 30 % - 期中考: 30 %

八、講義位址(<http://>)

九、教育目標

重新查詢