

重新查詢

友善列印

0982學期 課程基本資料

系所 / 年級	光通系碩專班 1年級	課號 / 班別	78E00034 / 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	李正吉	開課期間	一學年之下學期
人數上限	11 人	已選人數	5人

起始週 / 結束週 / 上課地點 / 上課時間

第1週 / 第18週 / I633 / 星期1第11節
第1週 / 第18週 / I633 / 星期1第12節
第1週 / 第18週 / I633 / 星期1第13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)

讓學生深入瞭解電腦系統的安全防衛措施、使用者身份鑑別技術、資料的私密性及完整性保護以及網路通訊安全等安全機制，並使學生對電腦犯罪之對策和電腦病毒之防治有更深入的瞭解。希望能培育學生具有更深入且完整的資訊與網路安全概念，並具有建置一安全資訊系統之能力。

二、先修科目(Pre Course)

三、教材內容(Outline)

使用學了解資訊安全相關論文之研究

四、教學方式(Teaching Method)

準時出席上課，攜帶課本及筆記，抱持認真的學習態度，分組討論。

五、參考書目(Reference)

2010/2/23	Introduction	李正吉
2010/3/2	Mathematics of cryptography	李正吉
2010/3/9	Symmetric-key ciphers	李正吉
2010/3/16	Symmetric-key ciphers	李正吉
2010/3/23	AES	李正吉
2010/3/30	Asymmetric-key ciphers	李正吉
2010/4/6	Asymmetric-key ciphers	李正吉
2010/4/13	Message integrity and message authentication	李正吉

六、教學進度(Syllabi)	2010/4/20 Test	李正吉
	2010/4/27 Digital signature	李正吉
	2010/5/4 Entity authentication	李正吉
	2010/5/11 SSL & TLS	李正吉
	2010/5/18 PGP	李正吉
	2010/5/25 IPsec	李正吉
	2010/6/1 Key management	李正吉
	2010/6/8 Paper reviewing	李正吉
	2010/6/15 Paper reviewing	李正吉
	2010/6/22 Paper reviewing	李正吉

七、評量方式(Evaluation) 期中考(30%) 期末考(30%) 平常作業(20%) 期末報告(10%) 學習態度(10%)

八、講義位址(<http://>)

九、教育目標

重新查詢