朝陽科技大學
103學年度第2學期教學大綱

當期課號	7370			中文科名	密碼學
授課教師	李金鳳			開課單位	資訊管理系
學分數	3	修課時數	3	開課班級	日間部博士班1年級 A班
修習別	專業選修				
類別	英語授課				

本課程與系所培養學生核心能力關聯度	高度關聯	中高關聯	中度關聯	中低關聯	低度關聯
資訊資源整合與策略應用之能力。	✔				
組織溝通與資訊領導之能力。				✔	
獨立思考、分析與解決問題之研究能力。				✔	
國際視野與終身學習之能力。				✔	

本課程培養學生下列知識：

密碼學的介紹將以觀念與理論背景的介紹，建立學生的密碼學基礎，再引入密碼系統、數值簽章、密秘共享等基礎的密碼知識。 1. 知識: 讓學生具有密碼學之專業知識 2. 技能：使學生熟悉常見密碼學之相關技術並了解如何判別密碼學之優缺點，及現行應用領域 3. 態度：培養學生獨立研讀密碼學相關論文並提出創新的概念或運用 4. 其他：作為研究及實務運用的基礎

1.讓學生具有密碼學之專業知識
2.學生需了解如何判別密碼學之優缺點及現行應用領域
3.讓學生熟悉常見密碼學、數位簽章、認證之相關技術
4.讓學生能獨立研讀密碼學相關論文並提出創新的概念或運用

The course introduces concepts and theoretical background, the establishment of cryptography based on the reintroduction password system, numerical signature, and the secret sharing.

每週授課主題

第01週：Introduction and Why Cryptography
第02週：對稱式密碼技術: Classical Encryption Techniques
第03週：對稱式密碼技術: Block Ciphers and The Data Encryption
第04週：Standard (DES)
第05週：對稱式密碼系統應用: Contemporary Symmetric Ciphers(AES 等)
第06週：對稱式密碼系統應用與分析: Confidentiality and Analysis by Usin
第07週：數論介紹: Introduction to Number Theorem
第08週：數論介紹: Introduction to Number Theorem
第09週：期中Presentation Project
第10週：公開金鑰密碼技術: Public-key Cryptography
第11週：金鑰管理: Key Management and Other Public-key Cryptosy
第12週：訊息認證: Massage Authentication and Hash Functions
第13週：期中考
第14週：數位簽章: Digital Signatures
第15週：數位簽章: Digital Signatures
第16週：網路安全技術: Authentication Applications--數位憑證技術
第17週：網站/網頁安全 Web Security (SSL and TLS)
第18週：期末orall報告

成績及評量方式

其他(期末專題製作)：：25%
隨堂模擬測驗 及平時作業：40%
學習態度及出席：10%
期中考：25%

證照、國家考試及競賽關係

本課程無證照、國家考試及競賽資料。

主要教材

1. 書名：Cryptography and Network Security 作者：Behrouz A. forouzan 出版社：東華書局/新月圖書 (教科書)

參考資料

本課程無參考資料!

建議先修課程

本課程無建議先修課程

教師資料

教師網頁：http://www.cyut.edu.tw/~lcf
E-Mail： lcf@cyut.edu.tw
Office Hour：
星期三,第5~6節,地點:T2-1030;
星期四,第5~6節,地點:T2-1030;
分機:4293