

朝陽科技大學
100學年度第2學期教學大綱

| | | | |
|------|------|------|--------------|
| 當期課號 | 7410 | 中文科名 | 密碼學 |
| 授課教師 | 楊伏夷 | 開課單位 | 資訊工程系 |
| 學分數 | 3 | 修課時數 | 3 |
| 修習別 | 專業選修 | 開課班級 | 日間部碩士班1年級 A班 |
| 類別 | 一般課程 | | |

| 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 |
|-------------------|------|------|------|------|------|
| 資訊系統、晶片與整合電路之專業知識 | ✓ | | | | |
| 專題研究策劃與執行能力 | ✓ | | | | |
| 資訊工程專業論文撰寫能力 | | | | | ✓ |
| 創新思考及獨立解決問題能力 | | | | ✓ | |
| 跨領域協調整合能力 | | | | | ✓ |
| 工程倫理素養與國際觀 | | ✓ | | | |
| 領導、管理及規劃能力 | | | | ✓ | |
| 時事議題理解及培養終身學習能力 | | | | | ✓ |

本課程培養學生下列知識：

密碼學課程規劃兼顧理論與實務，學生首先熟悉抽象代數群環體基本概念，再學習對稱式加密技術與業界標準，瞭解公開金鑰密碼技術與常用的協定，解析雜湊函數的演算技術及標準，實務課程則分析實際的應用範疇，例如身分認證、秘密分享、金鑰協定、電子現金等，課程目標為：

- 1.瞭解群環體的特性與構造
- 2.熟悉對稱式加密技術
- 3.瞭解公開金鑰密碼協定
- 4.熟悉雜湊函數的特性與構造
- 5.瞭解應用如身分認證、秘密分享、金鑰協定

This course is an introduction to the basic theory and practice of cryptographic techniques used in computer security. The students will realize the following important topics after finishing this course: Number theory, Symmetric Cryptosystem (DES, Triple DES, AES), Public-key Cryptosystem (DH,RSA,DSS), secure hash function (SHA), and digital signature. Moreover, the Internet security and electronic commerce are also include in this course. Finally, some recent papers will be discussed.

每週授課主題

- 第01週：Integers -- properties and fundamental algorithms
- 第02週：Integers -- properties and fundamental algorithms
- 第03週：Congruences and Residue Class Ring
- 第04週：Encryption
- 第05週：Probability and Perfect Secrecy
- 第06週：DES and AES
- 第07週：Prime Number Generation
- 第08週：Public-Key Encryption
- 第09週：期中考
- 第10週：Public-Key Encryption
- 第11週：Factoring and Discrete Logarithms
- 第12週：Cryptographic Hash Functions
- 第13週：Digital Signatures
- 第14週：Digital Signatures
- 第15週：Other systems
- 第16週：Presentation of selected recent papers
- 第17週：Presentation of selected recent papers
- 第18週：期末考

成績及評量方式

- 期中考：30%
- 期末考：30%
- 口頭報告：20%
- 隨堂模擬測驗與平時作業及出席：20%

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

2.Introduction to Cryptography(教科書)

參考資料

書名：Handbook of Applied Cryptography 作者：A. Menezes, P. van Oorschot, and S. Vanstone 出版年(西元)：出版社：CRC Press

書名：Introduction to Modern Cryptography 作者：M. Bellare and P. Rogaway 出版年(西元)：出版社：Lecture note

建議先修課程

1.離散數學

教師資料

教師網頁：<http://www.cyut.edu.tw/~yangfy/>

E-Mail：yangfy@cyut.edu.tw

Office Hour：

星期二,第1~2節,地點:E-316.6;

星期三,第1~2節,地點:E-316.6;

分機:4760、3071

[關閉](#) [列印](#)

尊重智慧財產權，請勿不法影印。