

**朝陽科技大學**  
**106學年度第2學期教學大綱**

當期課號	7436	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
		開課班級	日間部碩士班1年級 A班
修習別	專業選修		
類別	一般課程		

本課程與系所培養學生能力指標關聯度：

核心能力	能力指標	高度關聯	中度關聯	低度關聯
資訊系統、晶片與整合電之專業知識。	具備資訊系統結構化程式設計的能力。		✓	
專題研究策劃與執行能力。	具有分析、規劃與設計專題之能力。		✓	
創新思考及獨立解決問題能力。	具備創新思考之基本能力。		✓	
工程倫理素養與國際觀。	具備正確的工程倫理觀念。		✓	

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：Overview
- 第02週：Symmetric Ciphers
- 第03週：Symmetric Ciphers
- 第04週：Symmetric Ciphers
- 第05週：Number Theory
- 第06週：Public-Key Cryptography and RSA
- 第07週：Public-Key Cryptography and RSA
- 第08週：Other Public-Key Cryptosystems
- 第09週：期中考
- 第10週：Other Public-Key Cryptosystems
- 第11週：Other Public-Key Cryptosystems
- 第12週：Cryptographic Hash Functions
- 第13週：Digital Signatures
- 第14週：Message Authentication Codes
- 第15週：User Authentication
- 第16週：Network Access Control and Cloud Security
- 第17週：Presentation of selected recent papers
- 第18週：期末考

成績及評量方式

平常成績(出席, 作業, 小考)：40%  
Programming: Big Integers, AES, RSA, EIG：60%

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.Cryptography and Network Security 6eW. StallingsPearson978-0-273-79335-96e(教科書)

## 參考資料

本課程無參考資料!

## 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](mailto:yangfy@cyut.edu.tw)

Office Hour：

星期一,第1節,地點:G-809;

星期二,第3~4節,地點:G-809;

星期三,第4節,地點:G-809;

分機:4760

[\[關閉\]](#) [\[列印\]](#)

尊重智慧財產權，請勿不法影印。