# 南台科技大學 98 學年度第 2 期課程資訊

| | |
|---|---|
| 課程名稱 | 進階密碼學 |
| 課程編碼 | 90M07801 |
| 系所代碼 | 09 |
| 開課班級 | 碩研資管一甲 碩研資管二甲 |
| 開課教師 | 李南逸 |
| 學分 | 3.0 |
| 時數 | 3 |
| 上課節次地點 | 三 2 3 4 教室 L405 |
| 必選修 | 選修 |
| 課程概述 | 本課程即是針對密碼學的原理與實務部分做深入淺出的介紹。 |
| 課程目標 | 從早期古典密碼學出發，然後介紹區塊加密器、進階加密標準，然後介紹基礎數論與 RSA 公開金匙密碼系統，並介紹金匙管理的技術與方法，最後再談及數位簽章的技術。 |
| 課程大綱 | 基礎數論<br>公開金匙密碼學與 RSA<br>金匙管理<br>訊息認證與雜湊函數<br>雜湊演算法<br>數位簽章 |
| 英文大綱 | Number theory<br>Public key cryptography and RSA<br>Key management<br>Message authentication and hash functions<br>Hash algorithm<br>Digital signature |
| 教學方式 | 課堂教授,分組討論,口頭報告, |
| 評量方法 | 自行設計測驗,口頭報告,課堂討論,課程參與度(出席率), |
| 指定用書 | Introduction to Cryptography and Network Security |
| 參考書籍 | |
| 先修科目 | |
| 教學資源 | |
| 注意事項 | |
| 全程外語授課 | 0 |
| 授課語言 1 | 華語 |
| 授課語言 2 | |

| | |
|---|---|
| **輔導考照 1** | |
| **輔導考照 2** | |