南台科技大學 102 學年度第 2 學期課程資訊

課程名稱	進階密碼學
課程編碼	G0M04E01
系所代碼	0G
開課班級	碩研資管一甲 碩研資管二甲碩研資工一甲碩研資工二甲
開課教師	李南逸
學分	3.0
時數	3
上課節次地點	四 2 3 4 教室 E0303
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 公開金匙密碼學與 RSA 金匙管理 訊息認證與雜湊函數 雜湊演算法 數位簽章
英文大綱	Number theory Public key cryptography and RSA Key management Message authentication and hash functions Hash algorithm Digital signature
教學方式	
評量方法	
指定用書	
參考書籍	
先修科目	NO
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**	