南臺科技大學 105 學年度第 2 學期課程資訊

課程名稱	密碼學概論
課程編碼	G0D08201
系所代碼	0G
開課班級	四技資工三甲 四技資工三乙
開課教師	鄭錦楸
學分	3.0
時數	3
上課節次地點	一 5 6 7 教室 C301
必選修	選修
課程概述	介紹傳統密碼與近代密碼的演進發展，以及其設計原理。
課程目標	
課程大綱	1.對稱式加密法 2.區塊加密與資料加密標準(DES) 3.有限體 4.進階加密標準(AED) 5.現代加密技術 6.利用對稱式加密達成機密性 7.數論 8.公開金鑰密碼學與 RSA 9.金鑰管理與其他公開金鑰密碼系統 10.訊息確認與雜湊函數 11.雜湊演算法 12.數位簽章與確認性協定
英文大綱	1.Classical encryption techniques 2.Block ciphers and data encryption standard(DES) 3.Finite field 4.Advanced encryption standard(AES) 5.Contemporary symmetric ciphers 6.Confidentiality using symmetric encryption 7.Number theory 8.Public-key cryptography and RSA 9.Key management and other public-key cryptosystems 10.Message authentication and hash functions 11.Hash algorithms 12.Digital signatures and authentication protocols
教學方式	
評量方法	

指定用書	網路安全與密碼學概論
參考書籍	
先修科目	有修過 "離散數學"與"機率論" 尤佳
教學資源	
注意事項	一、課堂教授 二、本課程" 密碼學概論" 成績之計算方式如下: 學期成績=期中考成績 * 30% + 期末考成績 * 40% + 平時成績 * 30%，平時成績= (出席率成績 * 8 + N 次平時考成績 + M 次作業成績) * 1/(8+N+M)，出席率成績= 100 分 - 曠課節數 (兩次遲到 算一次曠課 注意事項：需有看診醫生證明才可用病假銷去曠課)，期中考與期末考之出題原則 ： 題庫為主，教材為輔。
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	