

朝陽科技大學 093學年度第1學期教學大綱
Cryptography 密碼學

當期課號	7590	Course Number	7590
授課教師	簡宏宇	Instructor	CHIEN,HUNG YU
中文課名	密碼學	Course Name	Cryptography
開課單位	資訊管理系碩士在職專班一A	Department	
修習別	選修	Required/Elective	Elective
學分數	3	Credits	3
課程目標	密碼學的介紹將以觀念與理論背景的介绍，建立學生的密碼學基礎，再引入密碼系統、數值簽章、密秘共享等基礎的密碼知識。	Objectives	This course will introduce the basics of number theory, symmetric key/public key cryptosystem, and the security model and analysis techniques.
教材	課本: N. Smart - Introduction of Cryptography, 高立代理; 參考書: 近代密碼學及其應用 賴溪松等著 出版書局: 旗標; 講義: download from web site; 投影片	Teaching Materials	
成績評量方式	期中考 25% 作業&小考 25% 課堂參與 15% 期末報告 35%	Grading	Mid-term exam. 25% Final report 35% quiz & Homework 25% Participation 15%
教師網頁	-		
教學內容	密碼學觀念, 數論, 訊息理論, 密碼協定, 標準, 串流加密, 橢圓曲線密碼學, 論文研讀	Syllabus	Cryptography concept, number theory, information theory, security protocol, standards, stream cipher, ECC, paper study

尊重智慧財產權，請勿非法影印。