朝陽科技大學 092學年度第2學期教學大綱
Cryptography 密碼學

當期課號	7293	Course Number	7293
授課教師	洪國寶	Instructor	
中文課名	密碼學	Course Name	Cryptography
開課單位	網路與通訊研究所碩士班一A	Department	
修習別	選修	Required/Elective	Elective
學分數	3	Credits	3
課程目標	此課程將教導學生了解近代密碼學的發展，主題包括加密演算法、資料完整性、認證和身份識別、數位簽章、數論、密碼協定以及真實世界使用的安全系統，例如: RSA。我們也會選擇一些相關的論文來研讀並於課堂上討論	Objectives	This course is aimed to introduce students to a broad exposure to advanced operating systems topics. Topics to be discussed in the course include protection, security, memory management, operating system kernels, file systems, synchronization, naming, and distributed systems.
教材	講授	Teaching Materials	lecture
成績評量方式	Homework 15% (You may collaborate when solving the homework, however when writing up the solutions you must do so on your own.) Project 20% (Presentation and/or paper required) Midterm exam 25% (Open book and notes) Final exam 30% (Open book and notes) Class participation 10%	Grading	Homework 15% (You may collaborate when solving the homework, however when writing up the solutions you must do so on your own.) Project 20% (Presentation and/or paper required) Midterm exam 25% (Open book and notes) Final exam 30% (Open book and notes) Class participation 10%
教師網頁			
教學內容	The objective of this course is to give a general treatment of the essential core areas of cryptography. I will provide a reasonable amount of mathematical background where it is needed. The course material is of use to computer and communication engineers who are interested in embedding security into an information system. 1. Introduction 2. Conventional encryption, classical techniques, modern techniques, algorithms 3. Public-key encryption, hash functions, message authentication, digital signatures, and authentication protocols 4. Entity authentication and key distribution 5. Key management 6. Zero Knowledge Protocols 7. Pseudo Random Number Generartors 8. Selection of advanced topics	Syllabus	The objective of this course is to give a general treatment of the essential core areas of cryptography. I will provide a reasonable amount of mathematical background where it is needed. The course material is of use to computer and communication engineers who are interested in embedding security into an information system. 1. Introduction 2. Conventional encryption, classical techniques, modern techniques, algorithms 3. Public-key encryption, hash functions, message authentication, digital signatures, and authentication protocols 4. Entity authentication and key distribution 5. Key management 6. Zero Knowledge Protocols 7. Pseudo Random Number Generartors 8. Selection of advanced topics