朝陽科技大學 091學年度第2學期教學大綱
Cryptography 密碼學

當期課號	7368	Course Number	7368
授課教師	曾育民	Instructor	TSENG,YUH MIN
中文課名	密碼學	Course Name	Cryptography
開課單位	資訊工程系碩士班一A	Department	
修習別	選修	Required/Elective	Elective
學分數	3	Credits	3
課程目標	本課程主要介紹密碼學基礎理論作一一介紹，學生在完成本課程後，將可了解關於密碼學幾個主要的主題：數論，對稱式加密技術(如DES, Triple DES)等，並補充最新之AES對稱式加密技術，也包含公開金鑰密碼協定(DH,RSA,DSS)及雜湊函數(如MD5、SHA)，數位簽章等。另外，針對密碼學基礎有瞭解後，由於網際網路是一個公開的通訊通道，容易遭受到入侵與破壞，因此有必要瞭解現今網路安全的應用與技術，本課程除了介紹密碼學的基本觀念之外，還包括Kerberos、PGP、S/MIME、IP安全機制、SSL、SET等運用作一說明。最後也包含最近論文之研討。	Objectives	This course is an introduction to the basic theory and practice of cryptographic techniques used in computer security. The students will realize the following important topics after finishing this course: Number theory, Symmetric Cryptosystem (DES, Triple DES, AES), Public-key Cryptosystem (DH,RSA,DSS), secure hash function (MD5, SHA), and digital signature et al.. Moreover, the Internet security and electronic commerce are also include in this course. Finally, some recent papers will be discussed.
教材	Class room Slides	Teaching Materials	Class room Slides
成績評量方式	1.期中論文書面報告(Midterm-Report): 15% 2.期中考(Midterm exam.): 20% 3.期末考(Final exam.): 30% 4 期末論文報告(Presentation of selected recent papers): 25% 5.課堂參與(Participation):10%	Grading	1.期中論文書面報告(Midterm-Report): 15% 2.期中考(Midterm exam.): 20% 3.期末考(Final exam.): 30% 4 期末論文報告(Presentation of selected recent papers): 25% 5.課堂參與(Participation):10%
教師網頁			
教學內容	This course is an introduction to the basic theory and practice of cryptographic techniques used in computer security. The covered issues in this course consist of Cryptosystem, Cryptanalysis, Probability and Shannon's theory, DES, AES, Secure hash function, Number theory, RSA and Factoring problem, Public-key system (Discrete logarithm problem), and digital signature. Finally, some recent papers will be discussed.	Syllabus	This course is an introduction to the basic theory and practice of cryptographic techniques used in computer security. The covered issues in this course consist of Cryptosystem, Cryptanalysis, Probability and Shannon's theory, DES, AES, Secure hash function, Number theory, RSA and Factoring problem, Public-key system (Discrete logarithm problem), and digital signature. Finally, some recent papers will be discussed.