朝陽科技大學 095學年度第2學期教學大綱
Cryptography 密碼學

當期課號	7383	Course Number	7383
授課教師	陳金鈴	Instructor	CHEN,CHIN LING
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	教材：1.Cryptography and Network Security: Principles and Practices(4TH ed.),W.Stallings, Prentice Hall, 2006. (開發圖書公司) 2.補充講義。 參考書籍：1.密碼學與網路安全-原理與實務(中譯本第三版),巫坤品、王青青 譯, 碁峰資訊,2005. 2.Applied Cryptography,B.Schneier,Wiley,1995. 3.近代密碼學及其應用，賴溪松、韓亮、張真誠，松崗，2006.	Teaching Materials	1.Cryptography and Network Security: Principles and Practices(4TH ed.),W.Stallings,Prentice Hall, 2006. 2.Lectures
成績評量方式	1.Homework 15% 2.Project 20% (Presentation and/or paper required) 3.Midterm exam 25% 4.Final exam 30% 5.Class participation 10%	Grading	1.Homework 15% 2.Project 20% (Presentation and/or paper required) 3.Midterm exam 25% 4.Final exam 30% 5.Class participation 10%
教師網頁			
教學內容	本課程首先針對密碼學基礎理論作一一介紹，從對稱式加密技術(如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)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。	Syllabus	Introduction Conventional encryption: principles Conventional encryption: DES Conventional encryption : AES Related issues of conventional encryption Introduction to number theory Public-key cryptography: principles, encryption and key exchange: RSA, DHKE Hash functions and Message authentication: SHA-1, HMAC Digital signatures: RSA, DSA, ElGamal Secret-key authentication service: Kerberos Public-key certificate service: PKI, CA, X.509 Secure electronic transaction protocol: SET Web security: SSL IP security: IPSec Virtual private network (VPN) System security: firewall. Finally, some recent papers will be discussed.

尊重智慧財產權，請勿非法影印。