朝陽科技大學 098學年度第1學期教學大綱
Cryptography 密碼學

當期課號	7780	Course Number	7780
授課教師	楊伏夷	Instructor	YANG,FUW YI
中文課名	密碼學	Course Name	Cryptography
開課單位	資訊工程系碩士在職專班一A	Department	
修習別	選修	Required/Elective	Elective
學分數	3	Credits	3
課程目標	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	1. Introduction to Cryptography, J. A. Buchmann 2. Handbook of Applied Cryptography, A. Menezes, P. van Oorschot, and S. Vanstone 3. Introduction to Modern Cryptography, M. Bellare and P. Rogaway 4. Introduction to Cryptography with Java Applets, D. Bishop	Teaching Materials	1. Introduction to Cryptography, J. A. Buchmann 2. Handbook of Applied Cryptography, A. Menezes, P. van Oorschot, and S. Vanstone 3. Introduction to Modern Cryptography, M. Bellare and P. Rogaway 4. Introduction to Cryptography with Java Applets, D. Bishop
成績評量方式	1.期中論文書面報告(Midterm-Report): 15% 2.期中考(Midterm exam.): 30% 3.期末考(Final exam.): 30% 4 期末論文報告(Presentation of selected recent papers): 25%	Grading	1.期中論文書面報告(Midterm-Report): 15% 2.期中考(Midterm exam.): 30% 3.期末考(Final exam.): 30% 4 期末論文報告(Presentation of selected recent papers): 25%
教師網頁	http://www.cyut.edu.tw/~yangfy/index.htm		
教學內容	本課程主要介紹密碼技術的基礎理論與實務，內容除了近代密碼學之外，也包含一些相關領域的結果：如線性代數、代數、數論、機率理論。課程會詳細討論知名的密碼基本元素：如DES、AES、RSA、DSS、MD5、SHA，當然也包含最近刊登論文之研討。 1. Integers 2. Congruences and Residue Class Rings 3. Encryption 4. Probability and Perfect Secrecy 5. DES and AES 6. Prime Number Generation 7. Public-Key Encryption 8. Factoring and Discrete Logarithms 9. Cryptographic Hash Functions 10. Digital Signatures	Syllabus	This course is an introduction to the basic theory and practice of cryptographic techniques used in computer security. The course will explain the basic techniques of modern cryptography, including the necessary mathematical results from linear algebra, algebra, number theory, and probability theory. Also, some famous cryptographic primitives will be studied in details such as: DES, AES, RSA, DSS, MD5, SHA. Finally, some recent papers will be discussed.