朝陽科技大學 091學年度第1學期教學大綱
Information Security 資訊安全技術

當期課號	2788	**Course Number**	2788
授課教師	曾育民	**Instructor**	TSENG,YUH MIN
中文課名	資訊安全技術	**Course Name**	Information Security
開課單位	資訊工程系(四日)三A	**Department**	
修習別	選修	**Required/Elective**	Elective
學分數	3	**Credits**	3
課程目標	本課程主要介紹資訊安全的技術，學生在完成本課程後，將可了解關於資訊安全技術介紹，其主要涵蓋的範圍有：1. 資訊安全技術簡介 2. 數論 3. 各種密碼系統簡介4. 公開金匙密碼系統 5. 對稱性加密法 6. 數位簽章 7. 資安技術標準	**Objectives**	The goal of this course is to provide the students with a basic knowledge of information security. The students will realize the following important topics after finishing this course: 1. Introduction to information security. 2. Number theory 3. Cryptography systems, 4. Public key systems, 5. Symmetric cryptography systems, 6. Digital signature, 7. Security standards.
教材	使用單槍投影機課堂上課	**Teaching Materials**	Slides
成績評量方式	1.個人作業: 20% (請參閱作業題目、格式及繳交日期,含上課表現) 2.期中考: 35% (筆試) 3.期末考: 25% (筆試) 4.分組期末報告或Demo: 20%	**Grading**	HomeWork: 20% Midterm 35% Final 25% Project 20%
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。	**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

尊重智慧財產權，請勿非法影印。