朝陽科技大學 098學年度第1學期教學大綱
Information Security 資訊安全技術

當期課號	2854	Course Number	2854
授課教師	陳興忠	Instructor	CHEN,HSING CHUNG
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	書名 : 網路安全與密碼學 作者 : Atul Kahate 校閱:黃銘祥 譯者:楊政穎 出版社 : 旗標出版股份有限公司	Teaching Materials	書名 : 網路安全與密碼學 作者 : Atul Kahate 校閱:黃銘祥 譯者:楊政穎 出版社 : 旗標出版股份有限公司
成績評量方式	評分方式: - 出席率: 20% - 平時作業與測驗: 20 % - 期中考: 30 % - 期中考: 30 %	Grading	評分方式: - 出席率: 20% - 平時作業與測驗: 20 % - 期中考: 30 % - 期中考: 30 %
教師網頁	_		
教學內容	本課程的教學內容是以下列主題爲： 1. 資訊安全技術介紹 2. 對稱密碼(Symmetric Encryption)系統與非對稱密碼(Asymmetric Encryption)系統簡介 3. 古典密碼-Caesar Cipher 4. 古典密碼-Monoalphabetic Cipher 5. 古典密碼-Polyalphabetic Cipher 6. 古典密碼-Rotor Machine 7. 古典密碼-Transposition Cipher 8. 近代密碼-Data Encryption Standard 9. Data Encryption Standard 加密實習 10. 現代密碼--密碼學基礎數學 11. Diffie與Hellman密碼架構 12. 現代密碼-RSA Public Key Cryptosystem導論 13. RSA PKC 的數學推導 14. RSA加密的實習 15. RSA簽章的數學推導 16. RSA簽章的實習 17. RSA簽章可能的僞造方法與防制方案	Syllabus	The goal of this course are listed as below. 1. Introduction of information security 2. Symmetric Encryption and Asymmetric Encryption 3. Caesar Cipher 4. Monoalphabetic Cipher 5. Polyalphabetic Cipher 6. Rotor Machine 7. Transposition Cipher 8. Data Encryption Standard 9. Diffie and Hellman Scheme 10. RSA Public Key Cryptosystem 11. RSA PKC 12. User Authentication Algorithms 13. The Security Issues in WLAN，Wireless WAN(2G-GSM,3G/3.5G-UMTS) and WiMAX