朝陽科技大學 092學年度第1學期教學大綱
Networking Security 網路安全

當期課號	7308	Course Number	7308
授課教師	洪國寶	Instructor	
中文課名	網路安全	Course Name	Networking Security
開課單位	網路與通訊研究所碩士班一A	Department	
修習別	選修	Required/Elective	Elective
學分數	3	Credits	3
課程目標	密碼學觀念, 資安觀念及協定, 網安協定, 防火牆實習	Objectives	Cryptography concept, security protocol, attack, firewall practice
教材	講授	Teaching Materials	lecture
成績評量方式	Homework 15% (You may collaborate when solving the homework, however when writing up the solutions you must do so on your own.) Project 20% (Presentation and/or paper required) Midterm exam 25% (Open book and notes) Final exam 30% (Open book and notes) Class participation 10%	Grading	Homework 15% (You may collaborate when solving the homework, however when writing up the solutions you must do so on your own.) Project 20% (Presentation and/or paper required) Midterm exam 25% (Open book and notes) Final exam 30% (Open book and notes) Class participation 10%
教師網頁			
教學內容	The objective of this course is to examine both the principles and practice of cryptography and computer network security. The course material is of use to computer and communication engineers who are interested in embedding security into an information system. 1. Introduction (Chapter 1) 2. Conventional encryption: classical techniques, modern techniques, algorithms, confidentiality using conventional encryption (Chapters 2—7) 3. Public-key encryption and hash functions: public-key cryptography, number theory, message authentication and hash functions, hash and MAC algorithms, digital signatures and authentication protocols (Chapters 8—13) 4. Network security practice: authentication applications, electronic mail security, IP security, Web security, anonymous communications (Chapters 14—17) 5. Wireless network security 6. System security: intruders, viruses, and worms, firewalls (Chapters 18—20).	Syllabus	The objective of this course is to examine both the principles and practice of cryptography and computer network security. The course material is of use to computer and communication engineers who are interested in embedding security into an information system. 1. Introduction (Chapter 1) 2. Conventional encryption: classical techniques, modern techniques, algorithms, confidentiality using conventional encryption (Chapters 2—7) 3. Public-key encryption and hash functions: public-key cryptography, number theory, message authentication and hash functions, hash and MAC algorithms, digital signatures and authentication protocols (Chapters 8—13) 4. Network security practice: authentication applications, electronic mail security, IP security, Web security, anonymous communications (Chapters 14—17) 5. Wireless network security 6. System security: intruders, viruses, and worms, firewalls (Chapters 18—20).