



課 綱 Course Outline
資訊管理學系學士班

中文課程名稱 Course Name in Chinese	密碼學與網路安全				
英文課程名稱 Course Name in English	Cryptography and Network Security				
科目代碼 Course Code	IM_41740	班 別 Degree	學士班 Bachelor's		
修別 Type	學程 Program	學分數 Credit(s)	3.0	時 數 Hour(s)	3.0
先修課程 Prerequisite					
課程目標 Course Objectives					
<p>密碼學與網路安全將以資訊安全技術為主進行授課，主要課程參與對象預期為「對資訊安全系統發開與密碼學技術研發有興趣的同學」，本課程為技術導向，冀本課程能堅實修課學生的資訊安全技術能力，並開啟一條與資訊安全技術有所關聯之未來道路供學生審酌。</p> <p>This course focuses on the issues of Symmetric Encryption Techniques, Block Cipher, Number Theory, Public-key Encryption, Hash Function, Digital Signatures, Authentication, TCP/IP and Security, Web Security and Intrusion Detection Systems etc.</p>					
系教育目標 Dept.'s Education Objectives					
1	<p>培育具備團隊合作、創造與思考以及國際視野能力之人才。 Cultivate the personnel with the capability of teamwork, creative thinking and international vision</p>				
2	<p>培育具備資訊專業知識與技術能力之人才。 Cultivate the personnel with the capability of professional knowledge and technical skill</p>				
3	<p>培育具備商業管理知識與應用能力之人才。 Cultivate the personnel with the capability of business management and application</p>				
4	<p>培育具備整合資訊科技與管理知識之專業人才。 Cultivate the personnel with the capability of integration of information technology and management</p>				
系專業能力 Basic Learning Outcomes				<p>課程目標與系專業能力相關性 Correlation between Course Objectives and Dept.'s Education Objectives</p>	

A	具備資訊管理基礎與跨學域的應用能力。 Cultivate the personnel with the capability of basic and interdisciplinary information management	○
B	具備以資訊科技為核心，擁有高度專業技術與國際視野之能力。 Cultivate professional personnel with international perspective and the capability of using information technology	●
C	具備資訊管理創新、研發、企劃之資訊管理人才之整合能力。 Cultivate senior personnel with the capability of innovation, research and development and integrated planning	○
D	具備企業資訊化的能力。 Cultivate the personnel with the capability of computerization of enterprises	○
E	具備業界多媒體應用、網站經營以及資訊行銷所需之能力。 Cultivate the personnel with the capability of multimedia applications, website operations, and information marketing	
F	具備認知新興資訊產業發展所需之能力。 Cultivate the personnel with the capability for the emerging information industry	●

圖示說明 Illustration : ● 高度相關 Highly correlated ○ 中度相關 Moderately correlated

課程大綱
Course Outline

1. Symmetric Encryption Techniques, 1 to 2 Week
2. Block Cipher, 1 to 2 Weeks
3. Number Theory, 1 to 2 Week
4. Asymmetric Encryption Techniques, 1 to 2 Weeks
5. Hash Function, 1 Week
6. Digital Signatures, 1 to 2 Weeks
7. Authentication, 1 Week
8. TCP/IP and Security, 1 to 2 Weeks
9. Web Security, 1 Week
10. Intrusion Detection Systems, 1 Week

資源需求評估 (師資專長之聘任、儀器設備的配合 . . . 等)
Resources Required (e.g. qualifications and expertise, instrument and equipment, etc.)

無

課程要求和教學方式之建議
Course Requirements and Suggested Teaching Methods

課堂講授與實機示範

其他
Miscellaneous

1. 開設系級：資管四上
2. 開設學程：商業智慧與大數據學程
3. Textbook:
 - William Stallings, Cryptography and Network Security: Principles and Practices, Fifth Edition, Prentice Hall.
 - 資訊與網路安全概論，黃明祥、林詠章著，高立圖書。
 - 網站應用程式安全檢測，查士朝編著。