



教學計劃表 Syllabus

課程名稱(中文) Course Name in Chinese	密碼學與網路安全		學年/學期 Academic Year/Semester	114/2
課程名稱(英文) Course Name in English	Cryptography and Network Security			
科目代碼 Course Code	IM_41740	系級 Department & Year	學四	開課單位 Course-Offering Department
修別 Type	學程 Program	學分數/時間 Credit(s)/Hour(s)	3.0/3.0	
授課教師 Instructor	/侯佳利			
先修課程 Prerequisite				
課程描述 Course Description				
針對資訊安全相關理論，實務，法規進行說明。並針對密碼學的理论，原理，實作，實務應用進行講授，建立良好的資訊安全觀念與知識。				
課程目標 Course Objectives				
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。				
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.				
系專業能力 Basic Learning Outcomes				課程目標與系專業能力相關性 Correlation between Course Objectives and Dept.'s Education Objectives
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				
授課進度表 Teaching Schedule & Content				
週次 Week	內容 Subject/Topics			備註 Remarks
1	課程大綱說明 威脅模型			
2	資訊安全的概念與實務			

3	常見攻擊與工具	
4	密碼學基礎數學	
5	古典密碼到現代密碼	
6	雜湊函數與完整性	
7	對稱式加密理論與實作1	
8	對稱式加密理論與實作2	
9	期中考試週 Midterm Exam	
10	金鑰管理與密碼學工程 I	
11	公開金鑰密碼理論與實作1	
12	公開金鑰密碼理論與實作2	
13	PKI 與憑證：信任鏈的運作與管理	
14	網頁安全TLS/HTTPS	
15	網頁安全Web 與 API 安全	
16	系統與網路攻擊面與資訊安全檢測	
17	期末考試週 Final Exam	
18	彈性教學	

教學策略 Teaching Strategies

- 課堂講授 Lecture
 分組討論 Group Discussion
 參觀實習 Field Trip
- 其他 Miscellaneous: 實作

教學創新自評 Teaching Self-Evaluation

創新教學(Innovative Teaching)

- 問題導向學習(PBL)
 團體合作學習(TBL)
 解決導向學習(SBL)
- 翻轉教室 Flipped Classroom
 磨課師 Moocs

社會責任(Social Responsibility)

- 在地實踐 Community Practice
 產學合作 Industry-Academia Cooperation

跨域合作(Transdisciplinary Projects)

- 跨界教學 Transdisciplinary Teaching
 跨院系教學 Inter-collegiate Teaching

- 業師合授 Courses Co-taught with Industry Practitioners

其它 other:

學期成績計算及多元評量方式 Grading & Assessments

配分項目 Items	配分比例 Percentage	多元評量方式 Assessments							
		測驗 會考	實作 觀察	口頭 發表	專題 研究	創作 展演	卷宗 評量	證照 檢定	其他
平時成績(含出缺席) General Performance (Attendance Record)	10%	✓	✓				✓		
期中考成績 Midterm Exam	30%	✓							
期末考成績 Final Exam	30%	✓							
作業成績 Homework and/or Assignments	20%		✓	✓					
其他 Miscellaneous (_____)	10%			✓	✓				

評量方式補充說明

Grading & Assessments Supplemental instructions

教科書與參考書目 (書名、作者、書局、代理商、說明)

Textbook & Other References (Title, Author, Publisher, Agents, Remarks, etc.)

課程教材網址(含線上教學資訊, 教師個人網址請列位於本校內之網址)

Teaching Aids & Teacher's Website(Including online teaching information.
Personal website can be listed here.)

其他補充說明 (Supplemental instructions)