淡江大學１１２學年度第１學期課程教學計畫表

課程名稱	電腦密碼學 CRYPTOGRAPHY	授課教師	黃心嘉 HWANG SHIN-JIA
開課系級	智應一碩士班Ａ TEIEM1A	開課資料	實體課程 選修 單學期 3學分
課程與SDGs關聯性	SDG4 優質教育		

系（ 所 ） 教 育 目 標

一、培養獨立研究解決問題。

二、提昇研發能量創意設計。

三、厚植資訊網路專業知能。

四、養成自發自主終生學習。

本課程對應院、系(所)核心能力之項目與比重

A. 獨立解決問題能力。(比重：20.00)
B. 獨立研究創新能力。(比重：20.00)
C. 論文撰寫發表能力。(比重：20.00)
D. 資訊網路研發能力。(比重：20.00)
E. 專案計畫管理能力。(比重：10.00)
F. 自主終生學習能力。(比重：10.00)

本課程對應校級基本素養之項目與比重

1. 全球視野。(比重：10.00)
2. 資訊運用。(比重：20.00)
3. 洞悉未來。(比重：20.00)
4. 品德倫理。(比重：10.00)
5. 獨立思考。(比重：10.00)
6. 樂活健康。(比重：10.00)
7. 團隊合作。(比重：10.00)
8. 美學涵養。(比重：10.00)

課程簡介	本課程的目的在提供資訊安全基礎的理論背景, 並研讀最近的深度學習在資安的研究成果。
	The purpose of this course is to give the fundamental theoretical background for information security. The current research results using deep learning are also introduced.

本課程教學目標與認知、情意、技能目標之對應

將課程教學目標分別對應「認知（Cognitive）」、「情意（Affective）」與「技能(Psychomotor)」的各目標類型。

一、認知(Cognitive)：著重在該科目的事實、概念、程序、後設認知等各類知識之學習。
二、情意(Affective)：著重在該科目的興趣、倫理、態度、信念、價值觀等之學習。
三、技能(Psychomotor)：著重在該科目的肢體動作或技術操作之學習。

序號	教學目標(中文)	教學目標(英文)
1	學生學習最近研究成果, 並透過口頭報告與討論進一步學習。	Students learn the current research results. Through the oral reports and discussions to enhance depth of students' studies.
2	學生學習密碼學與資訊安全的基本理論應用, 並透過口頭報告與討論進一步學習。	Students leans appliaciotns of the fundamental background on cryptography and infromation security. Through the oral reports and discussions to enhance depth of students' studies.
3	增進學生資訊科學專業英文閱讀能力。	Enhancing students' ability to read technical English especially in Computer Sciences.

教學目標之目標類型、核心能力、基本素養教學方法與評量方式

序號	目標類型	院、系(所)核心能力	校級基本素養	教學方法	評量方式
1	技能	ABCDEF	1234	講述、討論	測驗、討論(含課堂、線上)、報告(含口頭、書面)
2	技能	ABCDEF	578	講述、討論	測驗、討論(含課堂、線上)
3	技能	ABCD	12345678	講述、討論	測驗、討論(含課堂、線上)

授 課 進 度 表

週次	日期起訖	內 容 (Subject/Topics)	備註
1	112/09/11～112/09/17	Ch 1 Introduction to Cryptography and Data Security (Pelzl)	

2	112/09/18～ 112/09/24	Ch 1 Modular Arithmetic, Groups, Finite Fields, and Probability (Smart)	
3	112/09/25～ 112/10/01	Ch 6 Introduction to Public-Key Cryptography (Pelzl)	
4	112/10/02～ 112/10/08	Ch 7 The RSA Cryptosystem (Pelzl)	
5	112/10/09～ 112/10/15	Ch 8 Public-Key Cryptosystems Based on the Discrete Logarithm Problem (Pelzl)	小考
6	112/10/16～ 112/10/22	Chapter 9. Information-Theoretic Security (Smart)	
7	112/10/23～ 112/10/29	Chapter 11. Defining Security (Smart)	
8	112/10/30～ 112/11/05	Chapter 11. Defining Security (Smart)	
9	112/11/06～ 112/11/12	Chapter 17. Cryptography Based on Really Hard Problems (Smart)	
10	112/11/13～ 112/11/19	Chapter 17. Cryptography Based on Really Hard Problems (Smart)	期中考
11	112/11/20～ 112/11/26	Ch 9 Elliptic Curve Cryptosystems (Pelzl)	
12	112/11/27～ 112/12/03	Ch 10 Digital Signatures (Pelzl)	
13	112/12/04～ 112/12/10	Ch 10 Digital Signatures (Pelzl)	
14	112/12/11～ 112/12/17	Ch 10 Digital Signatures (Pelzl)	小考
15	112/12/18～ 112/12/24	Ch 10 Digital Signatures (Pelzl)	
16	112/12/25～ 112/12/31	Ch 11 Hash Functions (Pelzl)	
17	113/01/01～ 113/01/07	最近研究成果報告(預錄報告影片上傳)	
18	113/01/08～ 113/01/14	最近研究成果報告(預錄報告影片上傳)	

課程培養關鍵能力	自主學習、資訊科技
跨領域課程	
特色教學課程	
課程教授內容	程式設計或程式語言(學生有實際從事相關作業或活動) ＡＩ應用

修課應注意事項	出席與討論為評分考量之一。 報告內容為評分考量之一。 若自己負責報告時卻缺席，若無不可避免的理由，該次報告是零分。
教科書與教材	自編教材:簡報 採用他人教材:教科書
參考文獻	Cryptography and Network Security: Principles and Practice, 7th Ed., William Stallings, Pearson, 2017 “Introduction to Cryptography: Principle and Applications,” 3rd Ed., Hans Delfs and Helmut Knebl, New York: Springer-Verlag, 2010. “Protocols for Authentication and Key Establishment,” Colin Boyd and Anish Mathuria, New York: Springer, 2003. "Understanding Cryptography A Textbook for Students and Practitioners", Christof Paar, Jan Pelzl (2010)
學期成績計算方式	◆出席率： 10.0 % ◆平時評量：40.0 % ◆期中評量：20.0 % ◆期末評量： % ◆其他〈口頭報告〉：30.0 %
備　考	「教學計畫表管理系統」網址：https://info.ais.tku.edu.tw/csp 或由教務處首頁→教務資訊「教學計畫表管理系統」進入。 **※不法影印是違法的行為。請使用正版教科書，勿不法影印他人著作，以免觸法。**