淡江大學１０９學年度第２學期課程教學計畫表

課程名稱	密碼學 CRYPTOLOGY	授課教師	黃心嘉 HWANG SHIN-JIA
開課系級	資工一碩士班Ａ TEIXM1A	開課資料	以實整虛課程 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、厚植資訊工程專業知能。

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：40.00)

D. 資訊工程研發能力。(比重：40.00)

本課程對應校級基本素養之項目與比重

2. 資訊運用。(比重：40.00)

4. 品德倫理。(比重：20.00)

5. 獨立思考。(比重：40.00)

課程簡介	本課程的目的在提供密碼學與安全基礎的理論背景, 介紹最近的研究成果。
	The purpose of this course is to give the fundamental theorical background for cryptography and security. The current research results 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	ABD	245	講述、討論	測驗、討論(含課堂、線上)
2	技能	ABD	245	講述、討論	測驗、討論(含課堂、線上)
3	技能	ABD	245	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 (採數位教學之週次，請填「線上非同步教學」)
1	110/02/22～110/02/28	Ch 1 Introduction to Cryptography and Data Security (Pelzl)	
2	110/03/01～110/03/07	Ch 1 Modular Arithmetic, Groups, Finite Fields, and Probability (Smart)	
3	110/03/08～110/03/14	Ch 6 Introduction to Public-Key Cryptography (Pelzl)	線上非同步教學
4	110/03/15～110/03/21	Ch 7 The RSA Cryptosystem (Pelzl)	線上非同步教學
5	110/03/22～110/03/28	Ch 8 Public-Key Cryptosystems Based on the Discrete Logarithm Problem (Pelzl)	
6	110/03/29～110/04/04	Chapter 9. Information-Theoretic Security (Smart)	
7	110/04/05～110/04/11	Chapter 11. Defining Security (Smart)	

8	110/04/12～ 110/04/18	Chapter 17. Cryptography Based on Really Hard Problems (Smart)	
9	110/04/19～ 110/04/25	最近研究成果報告	
10	110/04/26～ 110/05/02	Ch 9 Elliptic Curve Cryptosystems (Pelzl)	
11	110/05/03～ 110/05/09	Ch 10 Digital Signatures (Pelzl)	
12	110/05/10～ 110/05/16	Ch 11 Hash Functions (Pelzl)	
13	110/05/17～ 110/05/23	Ch 13 Key Establishment (Pelzl)	線上非同步教學
14	110/05/24～ 110/05/30	Ch 12 Message Authentication Codes (MACs)(Pelzl)	線上非同步教學
15	110/05/31～ 110/06/06	最近研究成果報告	
16	110/06/07～ 110/06/13	最近研究成果報告	
17	110/06/14～ 110/06/20	最近研究成果報告	
18	110/06/21～ 110/06/27	最近研究成果報告	

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。
教學設備	電腦、投影機
教科書與 教材	"Cryptography Made Simple," Nigel P. Smart, Springer, 2016.
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)
批改作業 篇數	篇（本欄位僅適用於所授課程需批改作業之課程教師填寫）
學期成績 計算方式	◆出席率： 40.0 ％ ◆平時評量： ％ ◆期中評量： ％ ◆期末評量： ％ ◆其他〈口頭報告〉：60.0 ％

備　考	1.「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。 2.依「專科以上學校遠距教學實施辦法」第2條規定：「本辦法所稱遠距教學課程，指每一科目授課時數二分之一以上以遠距教學方式進行」。 3.依「淡江大學數位教學施行規則」第3條第2項，本校遠距教學課程須為「於本校遠距教學平台或同步視訊系統進行數位教學之課程。授課時數包含課程講授、師生互動討論、測驗及其他學習活動之時數」。 4.如有課程臨時異動(含遠距教學、以實整虛課程之上課時間及教室異動)，請依規定向教務處提出申請。 **※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。**