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	鄭　堯 YAO CHENG
開課系級	數學系數學四Ａ TSMAB4A	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、專業知識傳授。 二、基礎教育人才養成。 三、獨力創新思維。 四、自我能力表現。 五、團隊合作精神。 六、多元自我學習。

本課程對應院、系(所)核心能力之項目與比重
A. 認知與理解數學的基礎知識。(比重：60.00) B. 具備獨立與邏輯思考能力。(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：50.00) 5. 獨立思考。(比重：50.00)

課程簡介	這個課程會涵蓋下列的主題： (1)數論中的一些基本概念如歐式演算法和同餘. (2)基礎密碼學以及RSA系統 (3)糾錯碼的原理以及量子編碼
	This course will cover the following topics: (1)Elementary concepts in number theory such as Euclidean algorithm and congruence. (2)Introduction to cryptography and RAS system. (3)Error-correcting code and quantum algorithm.

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	(1)基礎數論(1~5週) (2)基礎密碼學以及RSA系統(6~9週) (3)糾錯碼以及量子密碼(11~14週)	(1)Elementary number theory(weeks 1~5). (2)Introduction to cryptography and RSA system(weeks 6~9). (3)Error-correcting code and quantum cryptography(weeks 11~14)

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	認知	AB	25	講述	測驗

授 課 進 度 表

週次	日期起訖	內 容 (Subject/Topics)	備註
1	110/02/22～110/02/28	1.3 The Euclidean algorithm. 1.4 Counting in different bases.	
2	110/03/01～110/03/07	2. Computational complexity.	
3	110/03/08～110/03/14	3.1 Congruence: fundamental properties. 3.2 Elementary applications of congruence. 3.3 Linear congruences. 3.4 The Chinese remainder theorem.	
4	110/03/15～110/03/21	4.1 Prime numbers. 4.2 Prime numbers and congruences. 4.3 Representation of rational numbers in an arbitrary base. 4.5 Factorisation in an integral domain.	
5	110/03/22～110/03/28	5 Finite fields and polynomial congruences.	
6	110/03/29～110/04/04	7.1 The classic ciphers. 7.2 The analysis of the ciphertext. 7.3 Mathematical setting of a cryptosystem	
7	110/04/05～110/04/11	7.4 Some classic ciphers based on modular arithmetic. 7.5 The basic idea of public key cryptography. 7.6 The knapsack problem and its applications to cryptography	
8	110/04/12～110/04/18	7.7 The RSA system. 7.8 Variants of RSA system and beyond.	
9	110/04/19～110/04/25	7.9 Cryptography and elliptic curves.	
10	110/04/26～110/05/02	期中考試週	

11	110/05/03～ 110/05/09	8.1 Birthday greetings. 8.2 Taking photos in space or tossing coins, we end up at codes. 8.3 Error-correcting codes. 8.4 Bounds on the invariants	
12	110/05/10～ 110/05/16	8.5 Linear codes. 8.6 Cyclic codes. 8.7 Goppa codes.	
13	110/05/17～ 110/05/23	9.1 A first foray into the quantum world: Young's experiment. 9.2 Quantum computers. 9.3 Vernam's cipher	
14	110/05/24～ 110/05/30	9.4 A short glossary of quantum mechanics. 9.5 Quantum cryptography	
15	110/05/31～ 110/06/06	畢業考試週	
16	110/06/07～ 110/06/13	---	
17	110/06/14～ 110/06/20	---	
18	110/06/21～ 110/06/27	---	

修課應注意事項	
教學設備	(無)
教科書與教材	Elementary number theory, cryptography and codes by M. Welleda Baldoni, Ciro Ciliberto, G.M. Piacentini Cattaneo, Daniele Gewurz. 2008
參考文獻	
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：20.0 % ◆期中評量：20.0 % ◆期末評量：20.0 % ◆其他〈 〉： %
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。**