淡江大學１００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	高金美 KAU CHIN-MEI
開課系級	數學系數學四Ａ TSMAB4A	開課資料	選修 單學期 3學分

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。

系（ 所） 核 心 能 力

A. 認知數學的基礎知識。

B. 理解數學的基礎知識。

C. 具備獨立與邏輯思考能力。

D. 理解機率，統計方面的基礎知識。

E. 具有利用電腦當輔助工具，解決數學及統計上的專業問題。

F. 具備資料蒐集與分析的知識。

G. 理解進階數學科學的能力。

課程簡介	在此密碼學課程中,我們將先了解密碼學的原理,進而知道對稱式金鑰加密技術, 與非對稱式金鑰加密技術, 最後介紹密碼學的雜湊函數如何能提供其他安全服務.
	In this Cryptology course, we will introduce the symmetric-key encipherment, asymmetric-key encipherment, and Integrity, authentication and key management.

本課程教學目標與目標層級、系(所)核心能力相關性

一、目標層級(選填)：
(一)「認知」(Cognitive 簡稱C)領域：C1 記憶、C2 瞭解、C3 應用、C4 分析、C5 評鑑、C6 創造
(二)「技能」(Psychomotor 簡稱P)領域：P1 模仿、P2 機械反應、P3 獨立操作、P4 聯結操作、P5 自動化、P6 創作
(三)「情意」(Affective 簡稱A)領域：A1 接受、A2 反應、A3 重視、A4 組織、A5 內化、A6 實踐

二、教學目標與「目標層級」、「系(所)核心能力」之相關性：
(一)請先將課程教學目標分別對應前述之「認知」、「技能」與「情意」的各目標層級，惟單項教學目標僅能對應C、P、A其中一項。
(二)若對應「目標層級」有1~6之多項時，僅填列最高層級即可(例如：認知「目標層級」對應為C3、C5、C6項時，只需填列C6即可，技能與情意目標層級亦同)。
(三)再依據所訂各項教學目標分別對應其「系(所)核心能力」。單項教學目標若對應「系(所)核心能力」有多項時，則可填列多項「系(所)核心能力」。
(例如：「系(所)核心能力」可對應A、AD、BEF時，則均填列。)

序號	教學目標(中文)	教學目標(英文)	相關性	
			目標層級	系(所)核心能力
1	此課程主要是希望學生在有了數學的知識後,了解甚麼是密碼, 又這些密碼的建立中使用了哪些數學.	In this course we hope that students can understand what is cryptography and what is the mathematics in the cryptography. They can find how people use mathematics in the cryptography.	C4	ABCE

教學目標之教學方法與評量方法

序號	教學目標	教學方法	評量方法
1	此課程主要是希望學生在有了數學的知識後,了解甚麼是密碼, 又這些密碼的建立中使用了哪些數學.	講述、討論、實作	紙筆測驗、實作、報告、上課表現

本課程之設計與教學已融入本校校級基本素養與核心能力	
淡江大學校級基本素養與核心能力	內涵說明
◆ 表達能力與人際溝通	有效運用中、外文進行表達，能發揮合作精神，與他人共同和諧生活、工作及相處。
◆ 科技應用與資訊處理	正確、安全、有效運用資訊科技，並能蒐集、分析、統整與運用資訊。
◇ 洞察未來與永續發展	能前瞻社會、科技、經濟、環境、政治等發展的未來，發展與實踐永續經營環境的規劃或行動。
◆ 學習文化與理解國際	具備因應多元化生活的文化素養，面對國際問題和機會，能有效適應和回應的全球意識與素養。
◆ 自我了解與主動學習	充分了解自我，管理自我的學習，積極發展自我多元的興趣和能力，培養終身學習的價值觀。
◆ 主動探索與問題解決	主動觀察和發掘、分析問題、蒐集資料，能運用所學不畏挫折，以有效解決問題。
◇ 團隊合作與公民實踐	具備同情心、正義感，積極關懷社會，參與民主運作，能規劃與組織活動，履行公民責任。
◇ 專業發展與職涯規劃	掌握職場變遷所需之專業基礎知能，管理個人職涯的職業倫理、心智、體能和性向。

授 課 進 度 表

週次	日期起訖	內 容 (Subject/Topics)	備註
1	101/02/13～101/02/19	密碼基礎數學I	
2	101/02/20～101/02/26	傳統對稱式金鑰加密法	
3	101/02/27～101/03/04	密碼基礎數學II	
4	101/03/05～101/03/11	現代對稱式金鑰加密法	
5	101/03/12～101/03/18	資料加密標準	
6	101/03/19～101/03/25	進階加密標準	
7	101/03/26～101/04/01	進階加密標準	
8	101/04/02～101/04/08	運用現代對稱式金鑰加密法之加密技術	
9	101/04/09～101/04/15	運用現代對稱式金鑰加密法之加密技術	
10	101/04/16～101/04/22	期中考試週	
11	101/04/23～101/04/29	密碼基礎數學III	
12	101/04/30～101/05/06	非對稱式金鑰密碼學	

13	101/05/07～ 101/05/13	非對稱式金鑰密碼學	
14	101/05/14～ 101/05/20	非對稱式金鑰密碼學	
15	101/05/21～ 101/05/27	畢業考試週	
16	101/05/28～ 101/06/03	----	
17	101/06/04～ 101/06/10	----	
18	101/06/11～ 101/06/17	----	

修課應 注意事項	不能請假
教學設備	電腦、其它(黑板)
教材課本	Cryptography and Network Security, Behrouz A. Forouzan, Mc Graw Hill,
參考書籍	
批改作業 篇數	6 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： 15.0 % ◆平時評量：15.0 % ◆期中評量：30.0 % ◆期末評量：30.0 % ◆其他〈報告〉：10.0 %
備 考	「教學計畫表管理系統」網址：http://info.ais.tku.edu.tw/csp 或由教務處首頁〈網址：http://www.acad.tku.edu.tw/index.asp/〉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。**