淡江大學１０４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. 認知與理解數學的基礎知識。

B. 具備獨立與邏輯思考能力。

C. 理解機率，統計方面的基礎知識。

D. 具有利用電腦當輔助工具，解決數學及統計上的專業問題。

E. 具備資料蒐集與分析的知識。

F. 理解進階數學科學的能力。

課程簡介	在此課程中我們將觀察數學如何被用在密碼的設計及破解中, 及目前已有的對稱式金鑰加密技術與非對稱式金鑰加密之技術及其應用.
	In tis course, we will see how important Mathematics is in the design of cryptography. We will understand what are Symmetric-key Encipherment and Asymmetric-key Encipherment, and how they can be applied.

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	希望學生藉由此課程了解數學理論在密碼的建構中的重要性,同時知道一些基本加密技術.	Hope students can understand how important Mathematics is in the construction of cyptography. At the same time, they can understand some basic encipher techniques and how they have been applied.	C3	AB

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	希望學生藉由此課程了解數學理論在密碼的建構中的重要性,同時知道一些基本加密技術.	講述、討論、問題解決	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	
淡江大學校級基本素養	內涵說明
◆ 全球視野	培養認識國際社會變遷的能力，以更寬廣的視野了解全球化的發展。
◆ 資訊運用	熟悉資訊科技的發展與使用，並能收集、分析和妥適運用資訊。
◆ 洞悉未來	瞭解自我發展、社會脈動和科技發展，以期具備建構未來願景的能力。
◆ 品德倫理	了解為人處事之道，實踐同理心和關懷萬物，反省道德原則的建構並解決道德爭議的難題。
◆ 獨立思考	鼓勵主動觀察和發掘問題，並培養邏輯推理與批判的思考能力。
◆ 樂活健康	注重身心靈和環境的和諧，建立正向健康的生活型態。
◆ 團隊合作	體察人我差異和增進溝通方法，培養資源整合與互相合作共同學習解決問題的能力。
◇ 美學涵養	培養對美的事物之易感性，提升美學鑑賞、表達及創作能力。

授 課 進 度 表

週次	日期起訖	內 容 (Subject/Topics)	備註
1	105/02/15～105/02/21	密碼基本認識	
2	105/02/22～105/02/28	傳統對稱式金鑰加密法	
3	105/02/29～105/03/06	傳統對稱式金鑰加密法	
4	105/03/07～105/03/13	現代對稱式金鑰加密法	
5	105/03/14～105/03/20	現代對稱式金鑰加密法	
6	105/03/21～105/03/27	資料加密標準	
7	105/03/28～105/04/03	教學行政觀摩週	
8	105/04/04～105/04/10	資料加密標準	
9	105/04/11～105/04/17	資料加密標準	
10	105/04/18～105/04/24	期中考試週	
11	105/04/25～105/05/01	RSA密碼系統	
12	105/05/02～105/05/08	橢圓曲線密碼系統	

13	105/05/09～ 105/05/15	數位簽章	
14	105/05/16～ 105/05/22	身分確定	
15	105/05/23～ 105/05/29	畢業考試週	
16	105/05/30～ 105/06/05	----	
17	105/06/06～ 105/06/12	----	
18	105/06/13～ 105/06/19	----	

修課應注意事項	隨時注意教學支援平台上的公告。
教學設備	電腦、投影機、其它(黑板或白板)
教材課本	
參考書籍	
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： 20.0 % ◆平時評量：20.0 % ◆期中評量：30.0 % ◆期末評量：30.0 % ◆其他〈 〉： %
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/CS/main.php〉業務連結「教師教學計畫表上傳下載」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。**