淡江大學１１２學年度第２學期課程教學計畫表

課程名稱	資訊安全 INFORMATION SECURITY	授課教師	黃心嘉 HWANG SHIN-JIA
開課系級	資工三Ｂ TEIXB3B	開課資料	實體課程 必修 單學期 2學分
課程與SDGs關聯性	SDG4 優質教育		

系（ 所 ） 教 育 目 標

一、通達專業知能。

二、熟練實用技能。

三、展現創意成果。

本課程對應院、系(所)核心能力之項目與比重

A. 程式設計應用能力。(比重：10.00)

B. 數學推理演繹能力。(比重：30.00)

C. 資訊系統實作能力。(比重：30.00)

D. 網路技術應用能力。(比重：10.00)

E. 資訊技能就業能力。(比重：20.00)

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：10.00)
4. 品德倫理。(比重：20.00)
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	本課程為資訊安全與密碼學的入門課程, 學生可以學到資訊安全與密碼學的基本知識, 與相關的背景理論, 足以研習網路安全或系統安全等課程
	This course introduce the basic concpets and theory for information security and cryptography. After this course, stundents will be ability to join the course about Intenet security or system security.

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	學生學習資訊安全觀念與架構。	Students learns the information security concept and architecture.
2	學生學習數論與有限體的基本觀念。	Students learn basic concepts in number theory and finite fields.
3	學生學習對稱式密碼系統與操作模式, 也要求自行了解。	Students learn sysmetric cryptosystems and operation modes. Students are required to first collect specificaiton about AES and then coding AES cryptosystem.
4	學生學習公開金鑰密碼學。	Students learn Public-key crypography.

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	ABCDE	12345678	講述、討論	測驗
2	認知	AB	245	講述、討論	測驗
3	技能	ABC	125	講述、討論	測驗、作業
4	技能	AB	1234567	講述、討論	測驗

授 課 進 度 表

週次	日期起訖	內 容 (Subject/Topics)	備註
1	113/02/19～113/02/25	課程介紹、單元一Information and Network Security Concepts	
2	113/02/26～113/03/03	單元二Introduction to Number Theory	

3	113/03/04～ 113/03/10	單元二 Introduction to Number Theory	
4	113/03/11～ 113/03/17	單元二 Introduction to Number Theory	
5	113/03/18～ 113/03/24	單元三 Classical Encryption Techniques	
6	113/03/25～ 113/03/31	單元三 Classical Encryption Techniques	小考
7	113/04/01～ 113/04/07	單元五 Finite Fields	
8	113/04/08～ 113/04/14	單元五 Finite Fields	
9	113/04/15～ 113/04/21	期中考試週	
10	113/04/22～ 113/04/28	單元六 Advance Encryption Standard	
11	113/04/29～ 113/05/05	單元七 Block Cipher Operation	
12	113/05/06～ 113/05/12	單元七 Block Cipher Operation	
13	113/05/13～ 113/05/19	單元九Public-Key Cryptography and RSA	小考
14	113/05/20～ 113/05/26	單元九Public-Key Cryptography and RSA	
15	113/05/27～ 113/06/02	單元十Other Public-Key Cryptosystems	
16	113/06/03～ 113/06/09	期末提前考	線上微課程
17	113/06/10～ 113/06/16	期末考試週(本學期期末考試日期 為:113/6/11-113/6/17)	線上微課程
18	113/06/17～ 113/06/23	教師彈性教學週(應安排學習活動如補救教學、專題學 習或者其他教學內容, 不得放假)	線上微課程

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)

修課應注意事項	※非法影印是違法的行為。請使用正版教科書，勿非法影印他人著作，以免觸法。 1.小考或是隨堂考務必在檢討前完成請假補考，逾期不給予補考。補考須提出請假的可佐證證明，經老師許可後，方可補考，並在一週內完成補考，逾期不候，且補考成績超過60分部分打八折。 2.本課程大量使用iClass公告注意事項或舉行不會事先通知的隨堂考，請同學務必注意iClass的電子郵件通知與公告。隨堂考成績將不採計最低分的成績，但是也沒有補考。 3.各項成績會在iClass上公告，請在當公告當周更正成績，逾期不候。 4.期末與學期成績會在期末考後5天內公佈，有問題者須於公佈當天找老師，逾期不候。 5.若是整組作業，需要整組出席評分時，若有小組非不可避免因素而缺席，缺席者該次作業零分。 6、實習課作業抄襲，實習課零分，考試作弊(含線上考試關鏡頭或是私自上網找資料)該考試零分。 7.因應遠距線上考試的需求，同學請準備有前鏡頭的桌機或是筆電，還有前鏡頭的手機或是平板電腦。 8.正課點名不扣出席分，供了解同學學習狀況與期末加分考量；但是不實點名會扣出席分，每次學成分數扣一分。 TibaMe課程名稱： 1.從實務出發－企業網路安全建置與技術展示| 資安線上課程 2.國際資安認證介紹
教科書與教材	採用他人教材:教科書 教材說明: Cryptography and Network Security: Eighth Edition, Global Edition by William Stallings
參考文獻	The Design of RijndaeL: AES – The Advanced Encryption Standard, Joan Daemen and Vincent Rijmen, Springer; 2002 Ed.
學期成績計算方式	◆出席率： 10.0 % ◆平時評量：30.0 % ◆期中評量：25.0 % ◆期末評量：25.0 % ◆其他〈TibaMe課程名稱： 1.從實務出發－〉：10.0 %
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。**