淡江大學１０９學年度第１學期課程教學計畫表

課程名稱	資訊安全導論 INTRODUCTION TO INFORMATION SECURITY	授課教師	黃心嘉 HWANG SHIN-JIA
開課系級	資工三Ｐ TEIXB3P	開課資料	實體課程 選修 單學期 3學分

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

E. 資訊技能就業能力。(比重：100.00)

本課程對應校級基本素養之項目與比重

2. 資訊運用。(比重：100.00)

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。	Studnets 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, 包含公開金鑰密碼系統、數位簽章法、雜湊函數與訊息檢查碼。	Sduents learns Public-key crypography inlcuding public-key cryptosystems,digitial signature schemes,hash functions, and message authentication codes.

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	E	2	講述、討論	測驗
2	認知	E	2	講述、討論	測驗
3	技能	E	2	講述、討論	測驗、作業
4	技能	E	2	講述、討論	測驗

授 課 進 度 表

週次	日期起訖	內 容 (Subject/Topics)	備註
1	109/09/14～109/09/20	課程介紹、單元一Computer and Network Security Concepts	
2	109/09/21～109/09/27	單元三Classical Encryption Techniques 單元四Block Ciphers and the Data Encryption Standard	
3	109/09/28～109/10/04	單元二 Introduction to Number Theory	
4	109/10/05～109/10/11	單元二 Introduction to Number Theory	
5	109/10/12～109/10/18	單元五 Finite Fields	
6	109/10/19～109/10/25	單元五 Finite Fields	
7	109/10/26～109/11/01	單元六Advance Encryption Standard	
8	109/11/02～109/11/08	單元六 Advance Encryption Standard	
9	109/11/09～109/11/15	單元六 Advance Encryption Standard	繳交AES規格書報告
10	109/11/16～109/11/22	期中考試週	
11	109/11/23～109/11/29	單元七 Block Cipher Operation	
12	109/11/30～109/12/06	單元七 Block Cipher Operation	
13	109/12/07～109/12/13	單元九Public-Key Cryptography and RSA	

14	109/12/14～ 109/12/20	單元十Other Public-Key Cryptosystems	
15	109/12/21～ 109/12/27	單元十Other Public-Key Cryptosystems	
16	109/12/28～ 110/01/03	單元十一Cryptographic Hash Functions	AES分組程式作業驗收
17	110/01/04～ 110/01/10	單元十二Message Authentication Codes	AES分組程式作業驗收
18	110/01/11～ 110/01/17	期末考試週	

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.除不可避免因素外，考試補考需事先告知申請，經老師許可後，方可補考，並在考試日後一週內完成補考，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隨堂考，請同學務必注意iClass的電子郵件通知與公告。 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.作業抄襲或是考試作弊，除該作業或考試0分外，第一次學期分數扣10分，第二次扣20分，第三次扣40分。
教學設備	電腦、投影機
教科書與教材	Cryptography and Network Security: Principles and Practice, 7th Ed., William Stallings, Pearson, (Global Edition)
參考文獻	The Design of RijndaeL: AES - The Advanced Encryption Standard, Joan Daemen and Vincent Rijmen, Springer; 2002 Ed.
批改作業篇數	2 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： 5.0 %　◆平時評量：30.0 %　◆期中評量：20.0 % ◆期末評量： % ◆其他〈書面(20%)與程式作業(25%)〉：45.0 %
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。**