The Principle and Application of Secret Sharing
秘密分享原理與應用

阮夙姿
科三422. #4875
Tel:0928523527
三BCD / 科三108

Introduction

課程目標:

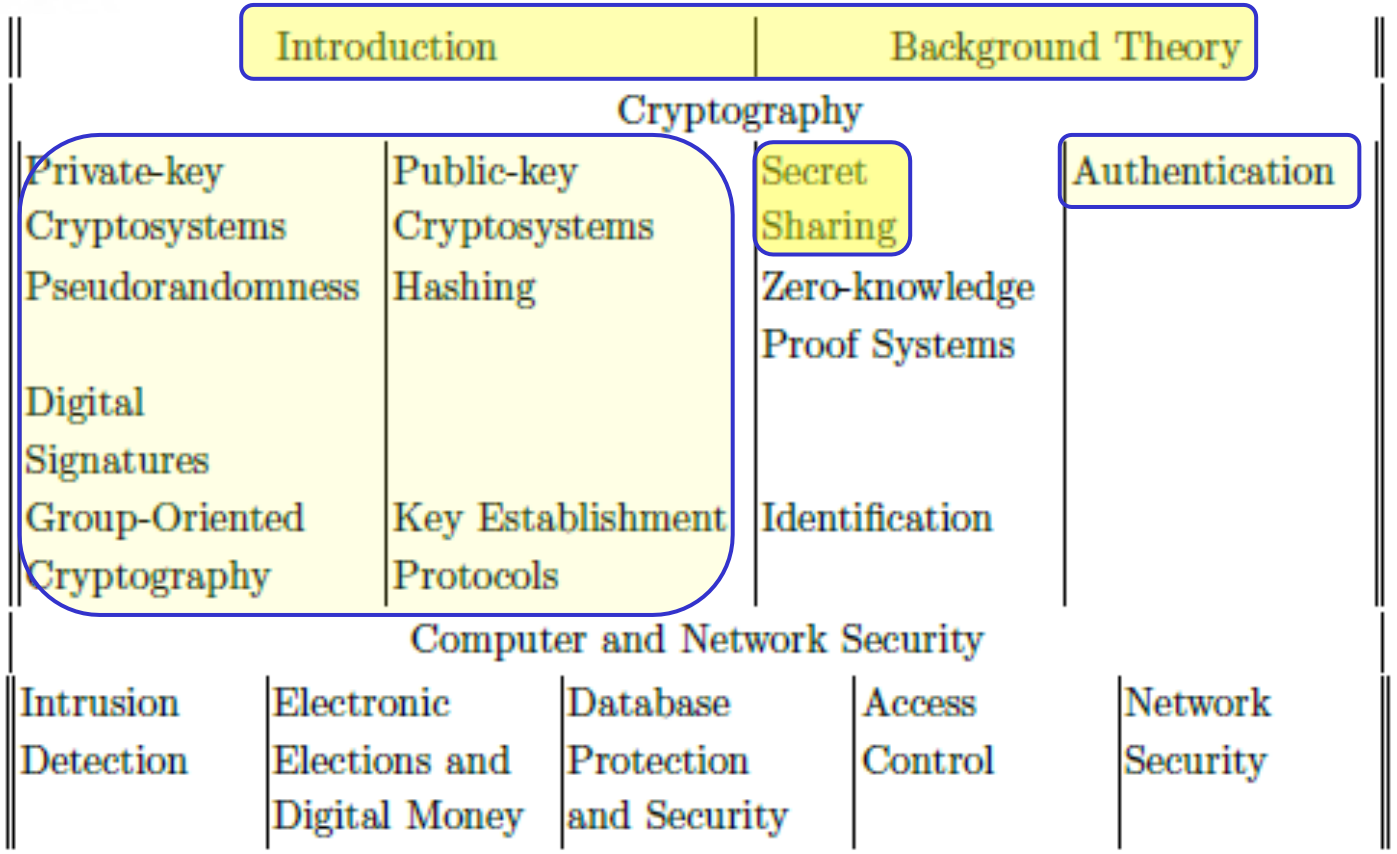
- 本課程首先將介紹古典的加密技術之原理與方法，之後將學習秘密分享及視覺密碼的基礎與進階方法、並進一步介紹各式增強功能將如何解決使用者所需。

- 於課程的進展中，將介紹秘密分享的方法之原理，以期培養學生具備資訊科學基礎數理知識；並具備應用之能力；以培養符合資訊產業需求的工程技術人才。

- 本課程需依照提出的問題，實際撰寫程式，藉以學習解決問題的方法。以期培養學生具備程式設計基礎知識並應用於設計及實作的能力；以培養具備前瞻資訊科技研發能力的人才。

Introduction

Source: J. Pieprzyk, T. Hardjono, J. Seberry, "Fundamentals of Computer Security", Springer, 2003.



Introduction

- 師生晤談時間：三 ZE
- 主要教科書：賴溪松, 韓亮, 張真誠, 近代密碼學及其應用, 旗標, 2003.
- 重要參考書籍：

1. Grimaldi, Discrete and Combinatorial Mathematics 5/e, Addison-Wesley(歐亞代理), 2003.
2. Wei Qi Yan, Jonathan Weir, Visual Cryptography and Its Applications, 2015, bookboon.com.
3. Stelvio Cimato, Ching-Nung Yang, Visual Cryptography and Secret Image Sharing, CRC, 2017. ($11000，國內部分圖書館有)
4. Feng Liu, Wei Qi Yan, Visual Cryptography for Image Processing and Security: Theory, Methods, and Applications, Hardcover, Springer, 2014. ($4000，無)
5. Wenbo Mao. Modern Cryptography: Theory and Practice. Prentice Hall, 2003.
6. 相關論文.

Introduction

- 課程內容： 預計將介紹下列各項

1. A brief introduction to modern cryptography
2. Number Theory
3. Classical Encryption Systems
4. (t, n)-threshold Secret Sharing Scheme / General Secret Sharing Scheme
5. Secret Sharing Scheme with Various Functions
6. Classical Visual Cryptography / Visual Cryptography for Multiple Secrets
7. Visual Cryptography with Various Functions
8. Progressive Visual Cryptography
9. XOR-based Visual Cryptography

秘密分享原理與應用課程

核心能力 與 課程地圖

暨大資工系 教育目標

研究所教育目標

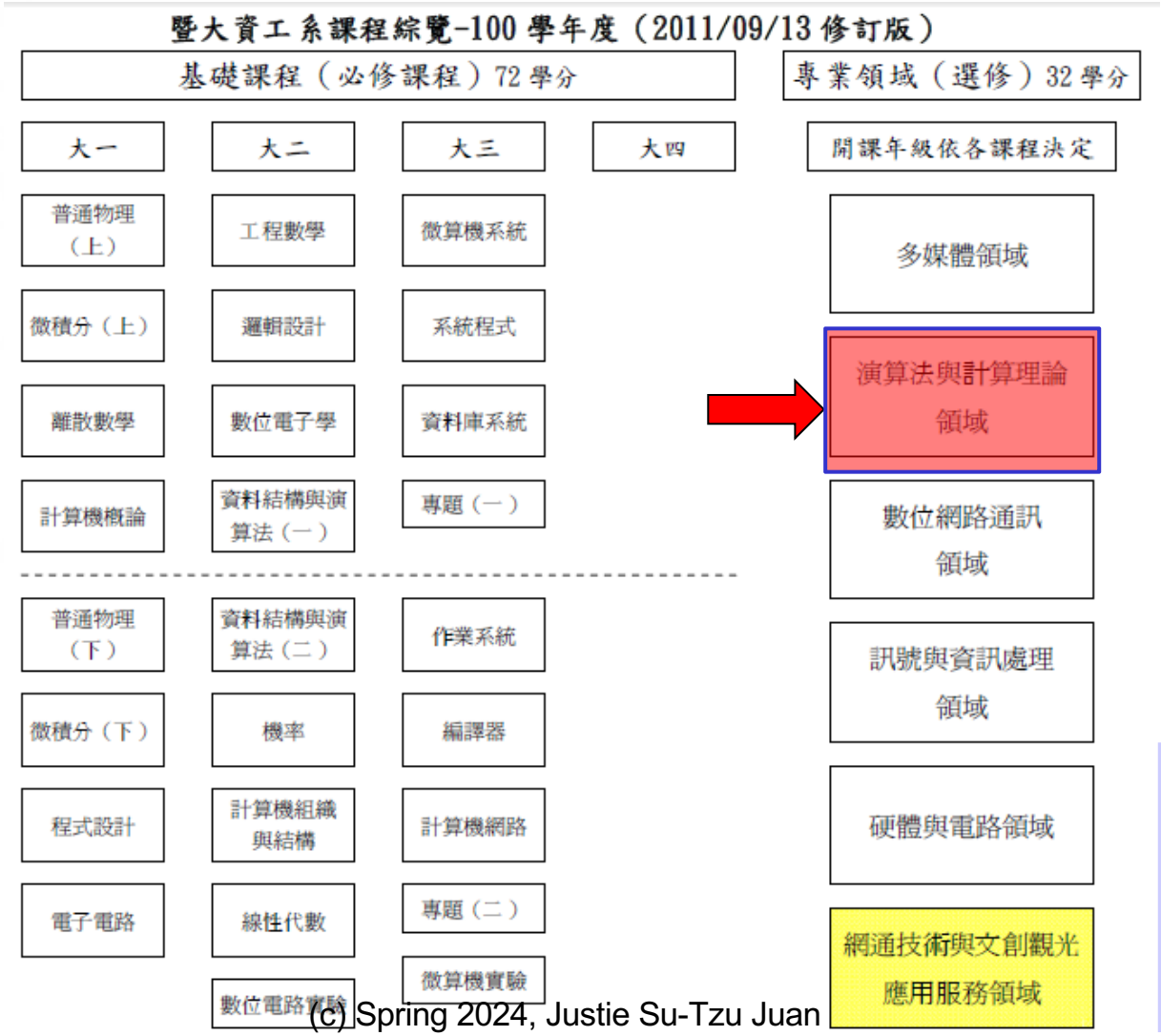
1. 配合國家經濟發展，培養符合資訊產業需求的工程技術人才
2. 配合國家科技及學術發展，培養具備前瞻資訊科技研發能力的人才
3. 配合全球永續發展潮流，培養具備國際視野、工程倫理、人文關懷及社會責任的科技人才

暨大資工系 核心能力

研究所核心能力

1. 具備資訊科學基礎數理知識並應用於發掘、分析與解釋數據的能力
2. 具備程式設計之基礎知識並應用於設計及實作資訊軟體的能力
3. 具備使用英文閱讀資訊領域技術文件及學術論文的能力
4. 具備團隊合作及獨立執行資訊工程領域學術研究的能力
5. 具備撰寫學術論文的能力
6. 理解資訊工程專業倫理、敬業態度、環境保護及社會責任

暨大資工系 課程地圖（部分）



全校共同課程14學分
通識領域課程17學分
專業選修 >= 32學分
未來發展（職涯）

暨大科技學院 核心能力

- 1.專業知識與實務技能
- 2.創新與獨立思考能力
- 3.溝通表達與團隊合作精神
- 4.專業倫理與社會責任認知
- 5.掌握國際趨勢與全球視野

暨大學生 八大基本素養與核心能力

- （一）道德思辨與實踐能力
- （二）人際溝通與表達能力
- （三）獨立思考與創新能力
- （四）人文關懷與藝術涵養
- （五）專業知能與數位能力
- （六）團隊合作與樂業倫理
- （七）全球視野與尊重多元文化
- （八）社區參與與公民責任

Introduction

- 評量方式：最高分99
  平時成績10% + 作業(含程式作業三次) 60% + 期末報告30% + 加分作業
  大學部及格60, 研究生及格70
- 進度:
  4/3, 5/1, 5/29：繳交程式作業
  6/5：期末報告
- 助教： 羅安惠 : 計算理論研究室R307-1 (分機4862)
  Office Hour : 四12:10-13:00
- 網頁: http://www.csie.ncnu.edu.tw/~jsjuan/courses.html