



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 / 科三301



Introduction

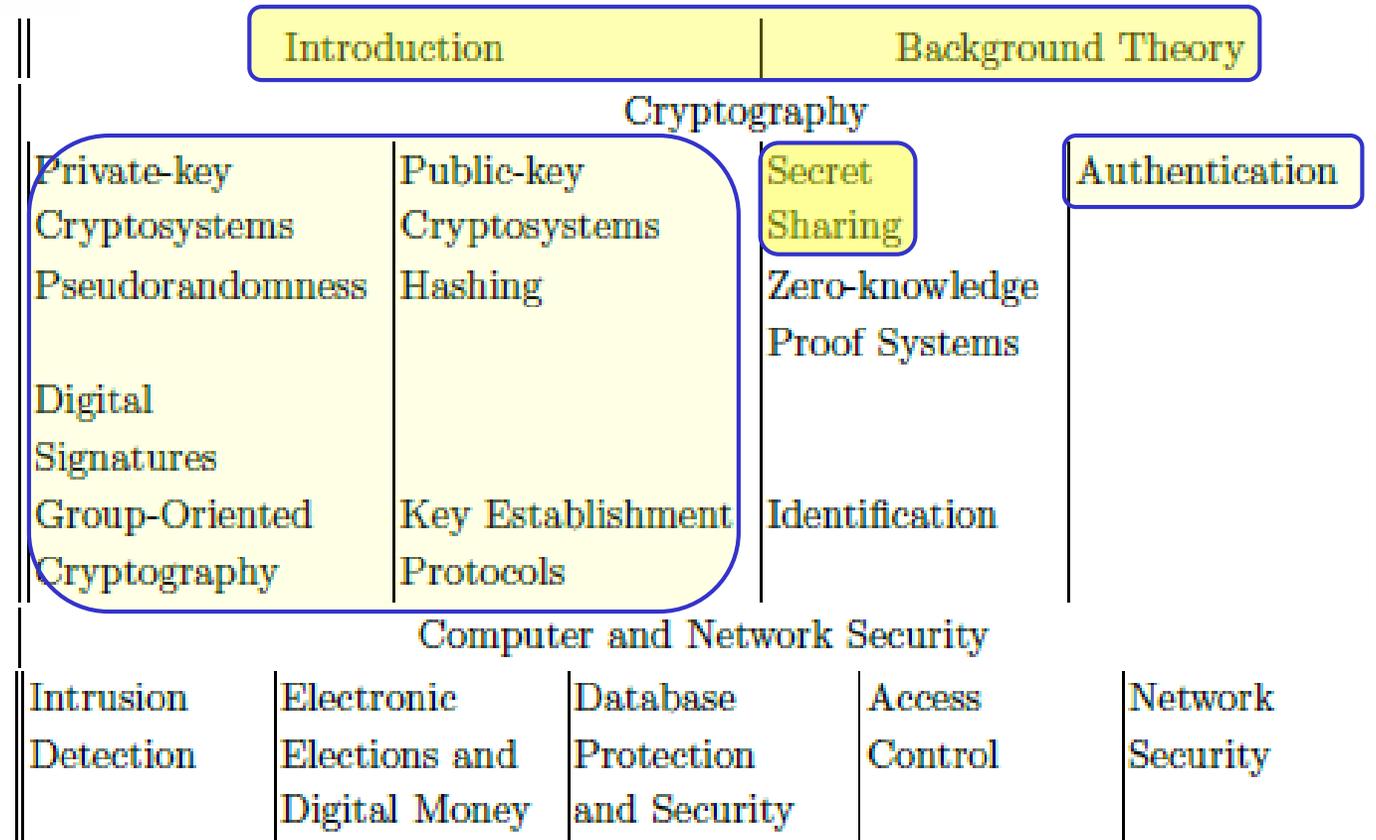
課程目標:

- 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；並具備應用與開創之能力；以培養具備前瞻資訊科技研發能力的人才。
- 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；以培養符合資訊產業需求的工程技術人才。



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. Wenbo Mao. Modern Cryptography: Theory and Practice. Prentice Hall, 2003.
 3. Wei Qi Yan, Jonathan Weir, Visual Cryptography and Its Applications, 2015, bookboon.com.
 4. Stelvio Cimato, Ching-Nung Yang, Visual Cryptography and Secret Image Sharing, CRC, 2017. (\$11000, 國內部分圖書館有)
 5. Feng Liu, Wei Qi Yan, Visual Cryptography for Image Processing and Security: Theory, Methods, and Applications, Hardcover, Springer, 2014. (\$4000, 天瓏)
 6. 相關論文.



Introduction

- 課程內容：預計將介紹下列各項
 1. Overview of Cryptography
 2. Fundamental and Technology of Cryptography
 3. Secret Sharing Scheme with Various Functions
 4. The Geometric Approach for Sharing Secrets
 5. Perfect SSS for Graph-Based Structure
 6. Visual Secret Sharing Scheme
 7. Visual Cryptography with Various Functions
 8. 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

研發潛能
理論能力

產業需求
實作能力

人的本質
自己以外

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



暨大資工系 課程地圖 (部分)

暨大資工系課程總覽-113學年度入學新生

基礎課程 (必修課程) 49 學分

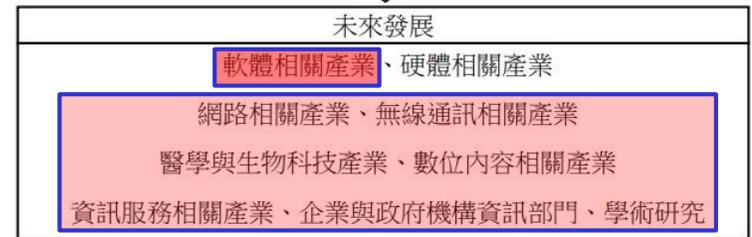
	大一	大二	大三	大四
上學期	微積分(上)	資料結構與演算法 (一)	系統程式	
	離散數學	邏輯設計與實驗 (二)	專題 (一)	
	計算機概論		計算機組織與結構	
下學期	微積分(下)	線性代數	作業系統	
	程式設計	資料結構與演算法 (二)	微算機實驗	
	邏輯設計與實驗 (一)		專題 (二)	
	機率			

開課年級依各課程決定，修課建議請參考專業選修課程地圖

專業選修課程 至少 42 學分

專業選修課程 至少 42 學分

未來發展





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10% + 程式作業 45% + 期末報告35% + 加分作業
大學部及格60, 研究生及格70
- 進度：
10/29, 11/19, 12/17：繳交程式作業
12/24：期末報告
- 助教：羅安惠：計算理論研究室R307-1 (分機4862)
Office Hour：二 13:10-14:00
- 網頁：<http://www.csie.ncnu.edu.tw/~jsjuan/courses.html>



Introduction

- **作業 1 (下下周上課前繳交) :**

請閱讀 “Grimaldi, Discrete and Combinatorial Mathematics 5/e, Addison-Wesley(歐亞代理), 2003.” 書中 4-3, 14-1, 14-2, 14-3, 16-1, 16-2, 16-3。並撰寫下列作業:

4-3 no.23, 27;

14-1 no.9; 15;

14-2 no.13;

14-3 no.15, 19, 20, 21, 32;

16-1 no.19;

16-2 no.15;

16-3 no.8, 9, 13