資訊安全研究所

應用密碼學(Applied Cryptography)

Instructor: Amir Rezapour

科號： 11220IIS 500400	學分：3	上課時間： WaWbWc	上課地點：遠距

- 課程目標(Course Objective)：

  This course is intended for graduate students. This course will cover the basics of symmetric cryptography, public-key cryptography, hash functions, message authentication codes, digital signatures, key management and distribution, and other fundamental cryptographic primitives. Then, we use the primitives to build provable secure protocols such as identification schemes, zero-knowledge proofs, commitment schemes, secret sharing, and electronic election system. By learning some existing secure protocols, you'll learn how to build provable secure systems.

- 授課內容(Course Description)：
- Introduction
- Symmetric-key encryption
- Algebra & number theory basics
- Public-key cryptography
- Probabilistic algorithms
- Cryptographic protocols
- One-way function and basic assumptions
- Bit-security of one-way functions
- One-way functions and pseudorandomness
- Provably secure encryption
- Probably secure digital signature

- 參考書籍(Textbook/References):
  - ✧ Hans Delfs, Helmut Knebl, *Introduction to Cryptography: Principles and Applications* (2nd Ed.), Springer, 2007.
  - ✧ Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone. *Handbook of applied cryptography*. CRC press, 2018.
  - ✧ William Stallings, *Network Security Essentials: Application and Standards [4th Ed.]*, Pearson & Prentice Hall, 2010.

- 授課方式 (Requirements): 講授
  - ✧ Computer Networks

- ✧ Introduction to Algorithms
- ✧ Probability

- 評分方式(methods of grading):

  - ✧ Four Homework Assignments
  - ✧ Exams
    i. Mid-Term
    ii. Final
  - ✧ Evaluation
    i. Homework: 50% +
       1. Assignments 50%
       2. Practical experiments $2 \times 10\%$ [bonus points]
    ii. Mid-Term 25%
    iii. Final 25%