Introduction to Cryptography

Wen-Guey Tzeng
Computer Science Department
National Yang Ming Chiao Tung University

Course basics

- Course time: T2F56
- Venue: ED117
- TA: to be announced
- Office hours: 2:00-3:30pm (Tu), 2:00-3:30pm (W)
- Grading
  - Homework (including program exercises)
  - Midterm
  - Final

Objective and prerequisite

- Objective
  - Learn cryptography
  - Use crypto for security assurance to systems and networks
- Prerequisite
  - Probability
  - C++ programming
  - Data structure and computer algorithm

Syllabus

- Introduction
- Number theory
- Classic encryption
- Block cipher and DES
- Finite field
- AES
- Block cipher operations
- Random bit generation and stream cipher
- Public key cryptography and RSA
- Other public-key systems
- Cryptographic hash functions
- Digital signatures
- Key management and distribution
- Supplements
  - Quantum factorization
  - Quantum key distribution