IERG4150
Intro. to Cryptography

Sherman Chow
Chinese University of Hong Kong
Fall 2022
Lecture 0: Logistics and Motivation

Contacts

- Email: smchow@ie.cuhk.edu.hk
  - Prepend subject of the email with [IERG4150]
  - Use your institutional email for correspondences
- Office: 808, Ho Sin Hang Engineering Building (SHB)
  - Please make a prior appointment
- Teaching assistant:
  - Minxin DU (dm018, SHB726)
  - Tutorial session: TBA

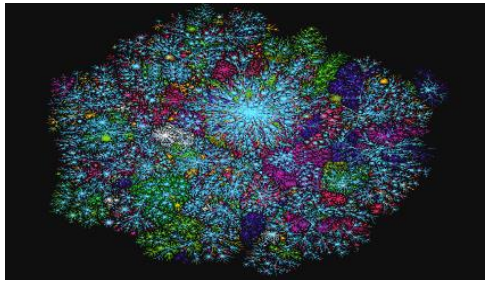
Platforms

- Course website
  - http://staff.ie.cuhk.edu.hk/~smchow/4150
  - redirected from course.ie.cuhk.edu.hk/~ierg4150 (IE VPN)
- Piazza for online discussion
  - be constructive and friendly
- Blackboard for course material
- Announcement sent via Blackboard to your CUHK mail

What is Cryptography?

- From Greek: “kryptos” (secret) and “grapho” (writing)
- Originally, the “art” of “secret writing”
- You don’t know how to read
- You don’t know how to write
- Control access (learning & influencing) to “information”
- So, only cipher/encryption and (digital) signature?
- Much more!

Why study Cryptography?



- Data is always under transmission
- Internet/cloud storage
- Outsourcing computation/storage
- ~3 billion Facebook users
  - was 500 million when I draft this slide
- 5 billion Internet users
  - was 2 billion a decade ago
- Everyone's data is digitalized!
  - personal info., credit card, health record, *etc*.

Data Confidentiality

- Many massive security breaches
- *E.g.*, PlayStations got hacked (April 2011)
  - Sony said that the credit card numbers were encrypted, but the hackers might have made it into the main database [CNN]
- It is as secure as its **weakest link**.

I have faith. Why can't I trust in them?

- Conflict of interests
  - R&D, insider info, strategic plan
  - Government agencies
- The Law
  - Medical records (HIPAA)
    - Health Insurance Portability & Accountability Act
  - Financial records (SOX)
    - Sarbanes–Oxley Act
  - Consumer records (CCPA)
    - California Consumer Privacy Ac

What are you trusting?

- Data is stored in more than one server
  - Trusting all servers / insiders / other tenants
- Relying on the server for access control
  - Horizontal or vertical privilege escalation
- A company have many employees
  - Careless/Cheating employees
- Encryption (number-theoretic assumptions?)

Fundamentals of "Provable Security"

- Security: It is a nebulous concept, but not if you took this course

- Provable:
  - We can formally define what it means to be secure
  - and then mathematically prove claims about security
  - *e.g.*, logic of composing building blocks together in secure ways

- Fundamentals:
  - solid theoretical foundation applicable to most real-world situations
  - equipped to (self-)study more advanced topics in cryptography

What this course is *not* about

- How to make your computer "secure"
- How to securely implement crypto lib. / deploy a secure system
- How to hack, *e.g.*, crack a password-protected account

- We do not discuss specific crypto software or Internet protocols
  - *e.g.*, HTTPS, SSH, SSL/TLS, IPsec, PGP, Tor, Signal, Bitcoin, BitLocker, …
- What caused the vulnerabilities in TEE (*e.g.*, Intel SGX), *etc*.

- We do not discuss cryptanalysis of "symmetric-key" primitives
  - *e.g.*, hash function, pseudorandom number generator, AES, *etc*.

“Prerequisites”

- Mathematically inclined
  - No advanced math. background is assumed
  - However, “mathematical maturity” is expected
    - familiarity with logics and comfortable with mathematical proof
    - *e.g.*, logic operators (AND, OR, XOR), proof technique: *e.g.*, contrapositivity
  - Knowledge of Basic (Discrete) Probability
    - perhaps some simple combinatorics
  - You should recall/revisit your middle-school (?) math
    - *e.g.*, power arithmetic
  - A quick review of Number Theory will be given
    - revisit your primary-school (?) math, *e.g.*, simple modular arithmetic

Course outcome

- You know a suite of cryptographic tools for your problem.
- You know what you are talking about when you are saying "an (encryption) scheme XXX is secure."
- You can make sense out of a specification of cryptographic scheme and should be able to program it.
- You can "cryptanalyze" a cryptographic scheme.
  - Hopefully, your implementation will be free from any silly mistake.
- Be interested in cryptography!

Crypto. as a scientific discipline [Shamir]

Is thriving as a scientific area of research:

- Taught at most major universities
- Attracts many excellent students
- Discussed at many conferences
- Published in hundreds of papers (e.g., http://eprint.iacr.org)
- Major conferences have >500 attendees
  - (Major trade shows have >10,000 attendees)
- Received the ultimate seal of approval from the CS community
  - Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman, 2002
  - Silvio Micali and Shafi Goldwasser, 2012
  - // Lesile Lamport (distributed system, Lamport signature), 2013

Cryptographic Conferences

- IACR Flagship Conferences: *Crypto, EuroCrypt, AsiaCrypt*
- IACR Specialist Conferences:
  - *CHES (Cryptographic Hardware and Embedded Systems)*
  - *FSE (Fast Software Encryption)*
  - *PKC (Public Key Cryptography)*
  - *TCC (Theory of Cryptography Conference)*
- Conferences in Cooperation with IACR (e.g.:) *AfricaCrypt, CANS, LatinCrypt, MyCrypt, Selected Areas in Cryptography (SAC), InsCrypt, Financial Crypt., Post Quantum Crypt.*
- Others: *ACISP, ACNS, ACSW-AISC, CT-RSA, ECC, ICICS, ICITS, ICISC, IndoCrypt, ISC, ISPEC, SCN, Pairing, ProvSec, Qcrypt, SCIS, SEC, SEcrypt, WISA, …*

Other Conferences with Crypto. Papers

- Security
  - ACM Conf. on Computer and Communications Security (CCS)
  - IEEE Security & Privacy (S&P/"Oakland")
  - Usenix Security
  - ISOC Network and Distributed System Security (NDSS)
  - ACSAC, ESORICS, EuroS&P, PETS, WiSec, SACMAT, …
- Network/Distributed Computing/WWW
  - IEEE Infocom
  - IEEE Intl. Conf. on Distributed Computing Systems (ICDCS)
  - ACM Principles of Distributed Computing (PODC)
  - ACM The Web Conference
- Theory
  - IEEE Foundations of Computer Science (FOCS)
  - ACM Symposium on Theory of Computing (STOC)
  - ACM Conf. on Innovations in Theoretical Computer Science (ITCS)

Tentative Assessment

- ≥3 Assignments (40%)
  - *e.g.*, exercises in the textbook (and more)
- Mid-Term Exam × 1 (20%)
- Final Exam × 1 (40%)
- (Online) Class Participation ?
  - (tiny bonus for top 10% participants)

Tentative Schedule (1)

- 01: Sep 5 (Mon), 7 (Wed)
  - Cryptography as a Scientific Discipline, One-Time Pad
- Sep 12 [Mid-Autumn Holiday]
- 02: Sep 14 (Wed), 19 (Mon) [Homework 1 assigned]
  - The Basics of Provable Security
- 03: Sep 21, 26
  - Secret Sharing
- 04: Sep 28, Oct 3
  - Basing Cryptography on Intractable Computations
- 05: Oct 5, 10 [Homework 2 assigned]
  - Pseudorandom Generators

Tentative Schedule (2)

- 06: Oct 12, 17: Pseudorandom Functions & Block Ciphers
- 07: Oct 19: Chosen Plaintext Attacks (a shorter chapter), Oct 24 [Revision?]
- 08: Oct 26: [Mid-Term]
- 09: Oct 31 (Mon), Nov 2 (Wed): Mode of Operations [Homework 3]
- 10: Nov 7, 9: Chosen Ciphertext Attacks
- 11: Nov 14, 16: Message Authentication Codes, and Hash Functions
  - [Homework 4 ? / Project ?]
- 12: Nov 21, 23: RSA & Digital Signatures (a long chapter)
- 13: Nov 28, 30: Diffie-Hellman Key Agreement and, Public-Key Encryption
  - (2 short and related chapters)

Textbooks

- [**Required**, but free] The Joy of Cryptography
  - https://joyofcryptography.com
- Another recommended textbook
  - Introduction to Modern Cryptography
  - http://www.cs.umd.edu/~jkatz/imc.html
- A Graduate Course in Applied Cryptography
  - http://toc.cryptobook.us
- Handbook of Applied Cryptography
  - http://cacr.uwaterloo.ca/hac
- A Computational Intro. to Number Theory and Algebra
  - http://shoup.net/ntb
- "Lecture Notes on Cryptography"
  - https://cseweb.ucsd.edu/~mihir/papers/gb.pdf

Class Policy

- Read the textbook
  - the slides, while using the same style and terminology, are meant for teaching but *not* for other purposes, say, revision cram notes
- No plagiarism
  - at the very least, you need paraphrasing
- Work independently
  - discussion is allowed, but write your own solution
- Any questions?