IERG4150
Intro. to Cryptography

Sherman Chow
Chinese University of Hong Kong
Fall 2024
Lecture 0: Intro. to Intro. to Cryptography

Rundown

- Prologue:
  - Contacts and Platforms
  - Historical Origins of Crypto
  - Defining Cryptography
- Security Goals
- Modern Applications
- Cryptographic Primitives
- Unique Aspects of Cryptographic Security
  - Adversarial Thinking
  - Precision and Formality
  - Threat Model
- Cryptographers' Mindset
  - Question Everything
  - Interdisciplinary Nature
  - Security vs. Usability
  - Long-term Thinking

Contacts and Platforms

- smchow[at]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:
  - Ying-yu Pan (py022, SHB726)
  - Tutorial session: Thur 3:30-4:30 pm

  at the lecture venue (Sci. Ctr. L4)

- http://staff.ie.cuhk.edu.hk/~smchow/4150
- 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!

Historical Origins of Cryptography

- Showcase humanity's age-old need for secure comm.
- Military uses of diplomatic concerns
- Cryptography has ancient origins, dating back to:
- Polybius square originally used for fire signaling
  - a device invented by Cleoxenus and Democleitus
  - made famous by the Greek historian and scholar Polybius
- Romans employed crypto. methods like Caesar cipher

Caesar Cipher

- Consider the 26 alphabets of English
- Encoded them as a number in [0, 25]
- E(m) → $m + k$ mod 26
- D(c) → c – k mod 26
- salad -> wepeh (k = 4)

- Review concepts:
  - Encoding (is not encryption)
  - Modular arithmetic

- Vulnerable to Frequency Analysis
  - w/ knowledge of plaintext distribution

Vigenère Cipher

- Variants of Caesar Cipher
- Idea: not always map a plaintext to the same ciphertext
- Plaintext: AttackAtDawn (case insensitive)
- Key: Lemon
- Key "Sequence": LEMONLEMONLE
- Ciphertext: LXFOPVEFRNHR

- How to attack?

Enigma

- Caesar and Vigenère Ciphers are both polyalphabetic
- Based on Substitution
- So does Enigma

“Rail-Fence” Cipher via Transposition

```
DISGRUNTLED EMPLOYEE
         ↓
D   R   L   E   O
 I G U T E   M L Y E
  S   N   D   P   E
         ↓
DRLEOIGUTE MLYESNDPE
```

Cryptography as Science

- used to be the “Art of Secret Writing”
- exemplified by historical methods like the Caesar cipher
- often lacked a systematic scientific foundation
  - or the “security foundation” is so weak offering practically nothing
- Cryptography, in contrast, is based on mathematical principles and rigorously tested algorithms, making it a scientific discipline.
  - involves the systematic study and development of techniques to protect information and ensure secure communication.
- This contrast highlights how modern cryptography has evolved with practical applications in the digital age.

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

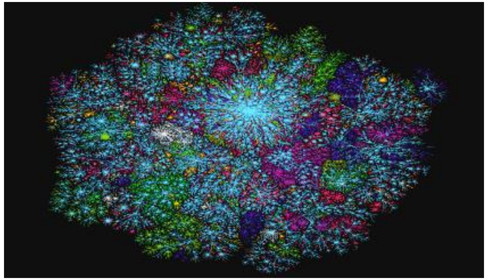
Cryptographic Conferences

- 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, Privacy
  - ACM Conf. on Computer and Communications Security (CCS)
  - IEEE Security & Privacy (S&P/"Oakland")
  - Usenix Security
  - ISOC Network and Distributed System Security (NDSS)
  - ACSAC, CODASPY, CSF, ESORICS, EuroS&P, PETS, RAID, SACMAT, WiSec, …
- 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)
  - IEEE International Symposium on Information Theory (ISIT)

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**.

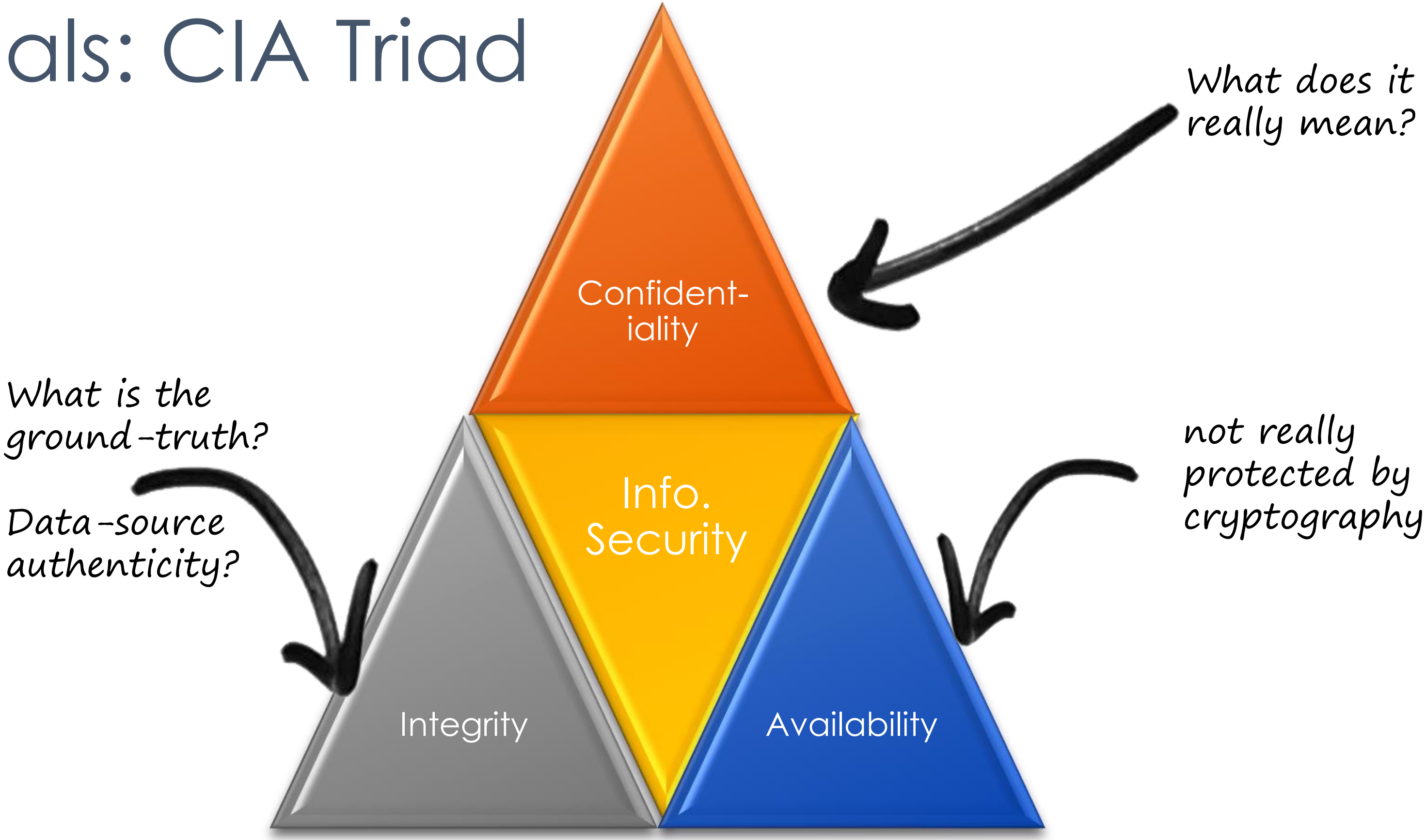
I have faith. Why can't I trust in them?

- Conflict of interests
  - R&D, insider info, strategic plan
  - Government agencies
- The Law
  - **S**arbanes–**Ox**ley Act: Financial records
  - **H**ealth **I**nsurance **P**ortability & **A**ccountability **A**ct: Medical data
  - **C**alifornia **C**onsumer **P**rivacy **A**ct: Consumer records
  - **G**eneral **D**ata **P**rotection **R**egulation

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?)

Goals: CIA Triad



Confidentiality

- Protect information from unauthorized access
- Encryption/Cipher converts plaintext into ciphertext
- making it unreadable w/o an appropriate decryption key

- The information can be sensitive personal information
- or it can be a secret key for some other functionality
  - like a decryption key
  - or an authentication key, see next slide

Integrity and Authentication

- A sealed letter provides confidentiality and **integrity**
- Altering the content requires tampering with the seal ($P \Rightarrow Q$)
- If the seal looks fine, the content hasn't been altered ($\neg Q \Rightarrow \neg P$)

logically equivalent

implication/inference

- **Authentication**: authentic information, so, like integrity
- What if the whole envelope is replaced?
  - The content has not been altered, literally
  - but it's not authentic
- Authentication links to the entity originated the communication
- Entity authentication: just to make sure the identity of the entity

Cryptographic Primitives / Building Blocks

- **Encryption** provides confidentiality, *e.g.*,:
  - *One-time* pad (OTP): the only perfectly secure scheme, the key is *as long as* the message
  - Pseudorandom (sequence) generator (PRG), pseudorandom function ("many PRGs")
  - Advanced Encryption Standard (AES) for **secret-key** encryption
  - Rivest-Shamir-Adleman (RSA) for **public-key** encryption

- (Cryptographic) **Hash functions** provides integrity
  - generates fixed-length hash values or "digests" (digital fingerprints) of input data
  - widely used in password storage: passwords remain hidden even if the database is stolen

- Authentication mechanisms/tools provide authenticity
- **Message authentication code** (MAC) for secret-key approaches, *e.g.*, HMAC
- **Digital signatures** for public-key approaches, *e.g.*, RSA, digital signature algorithm

Real-World Applications

- Secure Messaging Apps: End-to-end encryption ensures that only the intended recipient can decrypt and read messages.
- Online Banking: Digital certificates authenticate the bank's website and secure transactions through encryption.
- E-commerce: Digital signatures guarantee the authenticity of legal documents in online transactions.
- Data Encryption in Healthcare:
  - Encryption safeguards sensitive patient records,
  - making them accessible only to authorized medical professionals,
  - with historical roots in the need for wartime secrecy.

Modern Relevance

- Emerging Applications:
  - from online communications to financial transactions
- Evolving Threats and Challenges:
  - Ransomware, bad use of encryption!
  - Metadata leakage in communication, *e.g.*, who talks to whom
- Emerging Technologies in Cryptography:
  - Post-quantum cryptography addresses the potential threat from quantum computers to current encryption methods.
- Emerging Platforms: cloud, edge, meta-verse?
- Emerging Needs: machine learning over encrypted data?

Unique Aspects of Cryptographic Security

- What makes cryptography different from, *e.g.*, engineering?

- Adversarial Thinking:
  - Engineering a product best for its users
  - The design should remain “reliable” against adversarial users
- Precision and Formality:
  - Engineering may want a product works 99.9% of all scenarios
  - The adversarial user makes that 0.1% happen
- Threat Model

Adversarial Thinking

- Security professionals anticipating threats to a physical facility
- Think about designing security sys. for a high-value jewelry store
- Security experts don't assume all visitors are honest.
- They plan for potential burglars with sophisticated tools.

- Cryptography anticipates “digital” adversaries who are
  - highly capable
  - highly motivated
  - with advanced techniques trying to compromise data

Precision and Formality

- In cryptography, precision is crucial.
- We use mathematical proofs to prove security
- just as architects and engineers use precise blueprints to design buildings

- Example 1: Think of designing a safe, it depends on physical strength
- Cryptographers rely on mathematical algorithms to ensure security.

- Example 2: Traditional engineers ensure the stability of a building.
- Cryptographers secure network communication or data at rest.

- A cryptosystem is "secure"? We need precise language or precise model

- A cryptosystem uses MAC as a tool, MAC is secure means the whole system is secure?

Threat Model

- Brute-force attack
  - How many number of trials for a 3-digit pin lock?
  - What are the possible patterns to unlock a phone by drawing a figure touching each of the 9 dots in a square rid at most once?
- Adaptive attack (another dimension, can still be brute-force)
  - Civil engineers assume earthquake, typhoon, *etc.*
  - but do not assume the typhoon is under control (of mythical being?)
  - An adversary sends different encrypted http packets to a webserver
  - The webserver might behave differently
    - valid decryption, then perform action
    - invalid decryption, then quickly return error

Cryptographers: Professional Paranoid

- A mindset shift is required to study cryptography.
- We approach every problem with a healthy dose of skepticism.
- Assuming something is secure because it appears to be?
- No! We rigorously challenge it.
- This mindset leads to in-depth analysis and proof of security.
- We don't just aim for things to "work"; we aim for mathematical proofs that something is secure under well-defined conditions.
- Is the security model comprehensive enough?
- What does it mean in the real-world?

Simple Analysis: Online Banking

- When you log in to your bank account, you expect it to be secure.
- In cryptography, we don't take this for granted.

- We question how the bank ensures your data's security, prompting us to examine encryption, authentication, and access control methods to prevent unauthorized access.

Interdisciplinary Nature

- Cryptography combines elements from mathematics, computer science, and engineering.

- Embracing this interdisciplinary approach helps us create robust solutions without requiring in-depth expertise in any single field.

- Consider securing a wi-fi network. It's a collaborative effort:
- Cryptographers work on the math/algo. that encrypt the data
- Network engineers configure the routers
- Computer scientists ensure the encryption software runs.

Security vs. Usability

- Think about designing a secure login system for a smartphone.
- Traditional engineering might prioritize convenience, allowing users to easily access their device.
- In cryptography, we must balance usability with security.
- Cryptographers need to ensure that even if a smartphone is lost or stolen, an attacker can't easily access sensitive information.
- This requires a different mindset, where security often trumps convenience.

Long-Term Thinking

- Consider encrypting health records in healthcare systems
- Cryptographers must think long-term, ensuring that patient data remains confidential for many years.
- This differs from some engineering disciplines where components can be easily upgraded.
- Cryptography aims to provide security that withstands the test of time
- requiring a unique mindset that anticipates future advancements in technology and potential attacks.

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!

Tentative Assessment

- ≥3 Assignments (40%)
  - *e.g.*, exercises in the textbook (and more)
- Mid-Term Exam × 1 (20%)
- Final Exam × 1 (40%)
- Class Participation (at most 10%?)
  - Physical Attendance?
  - Tiny bonus for top 10% online “contributors”?

Unique Focus/Challenge of this Course

- We focus on provable security, so you need to do proof.
- Not the “mathematic derivations” proof you did before.
- Logical thinking is important.
- Some “Mechanical” (?!) Common tricks will be listed.
  - This is a level-4 course. Being a “robot” won’t take you far.

- “Crack” the crypto scheme if it is insecure.
- Creativity? More like you check with “ground-truth” rules.

Motivation (1/3)

- **Life-long education**: University students are not just learning how to apply knowledge but also how to think critically.
  - Understanding the theory behind cryptography will set you apart, equipping you with skills that go beyond simple application and into the realm of innovation.
- **Become "cool"**: Cryptography is a rare and highly valued skill in today's digital world.
  - By mastering these concepts, you'll be on the path to becoming a sought-after expert, someone who can proudly say they're building expertise in one of the most critical areas of cybersecurity.

Motivation (2/3)

- **Become a "hacker"**: With a strong understanding of crypto, you'll have the skills to identify and fix weaknesses in systems, even those designed by tech giants.
  - This knowledge empowers you to contribute to creating more secure and reliable digital environments.
- **Become a Guardian of Privacy and Security**: In a world where data breaches and cyber threats are becoming more common, the role of a cryptographer is more crucial than ever.

Motivation (3/3)

- **Be a Pioneer in a Rapidly Evolving Field**: Cryptography is at the forefront of the digital revolution.
  - By studying it now, you're positioning yourself as a pioneer in a field that is constantly evolving.
  - You'll be equipped to tackle challenges that don’t even exist yet, making you a leader in securing the future of technology.
- **Unlock Diverse Career Opportunities**: Cryptography can be a gateway to diverse career opportunities.
  - e.g., from working in cutting-edge tech companies to contributing to national security
- **Speak with confidence**: Understanding security proofs gives you the confidence to not only speak knowledgeably but also to make informed decisions that can ensure security in the real world.

Tentative Schedule (1)

- 01: Sep 3 (Tue), 5 (Thur)
  - Security, Motivation, Cryptography as Science, One-Time Pad
- 02: Sep 10, 12
  - The Basics of Provable Security
- 03: Sep 17, 19 [Homework 1 assigned]
  - Secret Sharing (this chapter is math-intensive!)
- 04: Sep 24, Sep 27
  - Basing Cryptography on Intractable Computations
- 05: Oct 1 [Holiday, Homework 2 assigned]
- 06: Oct 3 (Thur), 8 (Tue): Pseudorandom Generators

Tentative Schedule (2)

- 07: Oct 10 (Thur), 15 (Tue): Pseudorandom Functions & Block Ciphers
- 08: Oct 17: Chosen Plaintext Attacks (a shorter chapter)
- **Oct 22: [*Tentative* Mid-Term]**
- 09: Oct 24, Oct 29: Mode of Operations [Homework 3]
- 10: Oct 31, Nov 5: Chosen Ciphertext Attacks
- 11: Nov 7, 12: Message Authentication Codes, and Hash Functions
  - [Homework 4? / Project?]
- 12: Nov 14, 19: RSA & Digital Signatures (a long chapter)
- 13: Nov 21, 26: Diffie-Hellman Key Agreement and, Public-Key Encryption
  - (2 short and related chapters)
- Nov 28 [Revision? Applications?]

Textbooks / Notes

- [**Required**, but free] The Joy of Cryptography
  - https://joyofcryptography.com
- Another suggested 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 Introduction to Cryptography" (CMU)
  - https://cs.cmu.edu/~goyal/15356/lecture_notes.pdf
- "Lecture Notes on Cryptography" (UCSD)
  - 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
- The use of AI: use only with *explicit* acknowledgement
  - departmental policy at the moment, subject to change