ECE/CS 407
Cryptography

About Me

Ning Luo, CSL 457, https://ningoluo.github.io/
Email: nl27@illinois.edu

- Assistant Professor, UIUC 2024-now
- Postdoc, Northwestern University 2023-2024
- PhD, Yale University 2017-2022

Research: Cryptography, Formal Methods, Automated Reasoning, Achieve privacy and security in practical settings

Course Information

Time and Location:

TTh 5:00-6:20 pm, ECEB 3013

My office hour: Upon on request

TA: Pranav Rajpal

Office hour: TBD

Resources

- **Webpage**:

- **Canvas** https://courses.grainger.illinois.edu/ece407/fa2026/
  - Slides and files
  - Assignment submission and grading
  - Announcements
  - In-class quizzes

- **Piazza**
  - https://piazza.com/illinois/fall2026/csece407
  - Access Code: MD5 of "I love cryptography"
  - Do not know MD5? Shame on you!

Prerequisites

- **CS 225**: Introduction to Data Structures and Algorithms
- **CS/ECE 374**: Introduction to Algorithms and Models of Computation

Prerequisite overrides will be considered on a case-by-case basis. We expect that you are familiar with basic probability, modular arithmetic.

Grading Policy

- **In-Class Quizzes (10%)**
  - Average of all quiz scores, scaled to 100
- **Homework (20%)**
  - 5 assignments
  - Submit a single PDF compiled from LaTeX — no Word, Google Docs, or photos
  - No late submissions
  - **AI tools are NOT allowed unless stated otherwise**
- **Midterm Exam (20%)**
  - In class
  - You must pass the midterm to pass the course
- **Final Exam (30%)**
  - Cumulative
- **Final Project (20%)**
  - Design a cryptographic application of the course content
  - **AI tools ARE allowed**

4 credit hours project

Paper review and report:

You will read and write reviews of papers in the cryptography literature.

Please make an appointment with me on your paper selection.

https://registrar.illinois.edu/registration/registration-process/variable-credit-hours/

Ethics & Academic Integrity

Collaboration. Homeworks are to be submitted individually. However, you may collaborate with up to **one** other student on homework assignments. On each homework submission, **declare your collaborator** (if any). In your collaboration you are expected to discuss the homework, not merely copy answers. Plagiarism will not be tolerated

https://studentcode.illinois.edu/

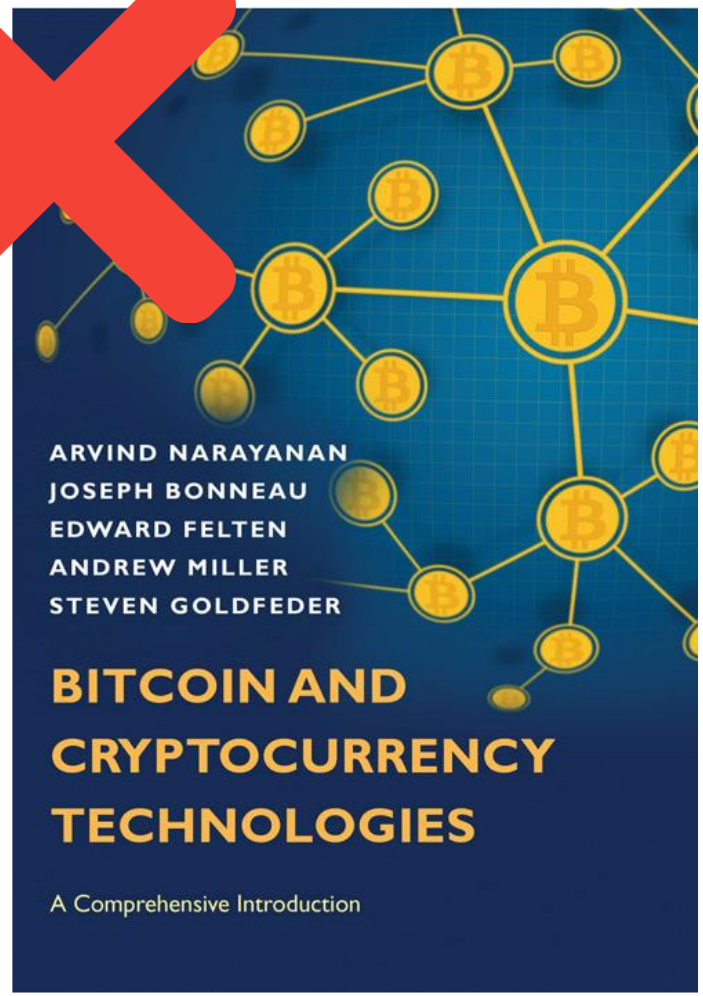
Emergencies

Emergencies can happen anywhere and at any time, so it's important that we take a minute to prepare for a situation in which our safety could depend on our ability to react quickly. Take a moment to learn the different ways to leave this building. If there's ever a fire alarm or something like that, you'll know how to get out and you'll be able to help others get out. Next, figure out the best place to go in case of severe weather – we'll need to go to a low-level in the middle of the building, away from windows. And finally, if there's ever someone trying to hurt us, our best option is to run out of the building. If we cannot do that safely, we'll want to hide somewhere we can't be seen, and we'll have to lock or barricade the door if possible and be as quiet as we can. We will not leave that safe area until we get an Illini-Alert confirming that it's safe to do so. If we can't run or hide, we'll fight back with whatever we can get our hands on. If you want to better prepare yourself for any of these situations, visit police.illinois.edu/safe. Remember you can sign up for emergency text messages at emergency.illinois.edu.

Diversity, Equity, and Inclusion

We in the Illinois ECE community are committed to understanding, empathizing with, and respecting each other, embracing the many differences among us.

What is this course **not** about?





Why cryptography?

Industry News
August 25, 2025

Share

Cloudflare secures sensitive
without fully restricting AI usa

Cloudflare announced new capabilities for Cloudflare One, its zero
designed to help organizations securely adopt, build and deploy en
generative AI applications.

Shadow IT: SaaS analytics READ ONLY

The personal details of nearly 200 million voters have been accidentally exposed in the largest U.S. leak of voter data, according to a security expert.

Information on more than 198 million American voters was left exposed to the Internet by a firm working on behalf of the Republican National Committee (RNC) in their efforts to elect Donald Trump, reports Chris Vickery, a cyber-risk researcher at UpGuard.

FedEx Customer Data Left Publicly Exposed on Cloud Storage Server

By: Sean Michael Kerner | February 16, 2018

Yet another cloud data leak is discovered, this time it's 119,000 documents with
npany Bongo

WSJ PRO

GOP Defends Ban on State AI Laws Over Data-Privacy Concerns

A proposed 10-year moratorium on state protections against the misuse of artificial intelligence is risky without federal regulations in place, opponents say

By Angus Loten

May 21, 2025 5:55 pm ET | WSJ PRO

Share Resize Listen (2 min)



A House energy and commerce subcommittee held a hearing on states' role in governing AI, data

news releases, and mainstream news articles. The list i
n are also listed. The various methods used in the brea

nillion by 2020, with the global annual cost forecast to b
ion unique email addresses and 21 million unique pass

Organization type	Method
government	hacked
web	hacked
financial	hacked
financial	inside job
social network	poor security
social network	accidentally uploaded
financial service company	poor security
healthcare	poor security
local search	unprotected api
healthcare	poor security/inside job
Clinical Laboratory	poor security
retail	hacked
Telephone directory	unknown
arts group	poor security
financial	hacked
academic	hacked
advertising	hacked
transport	hacked
telecoms	hacked
gaming	accidentally published
gaming	hacked
banking	poor security
transport	hacked
transport	hacked
healthcare	hacked

Blank Media Games	2018	7,633,234	gaming	hacked
BMO and Simplii	2018	90,000	banking	poor security
British Airways	2018	380,000	transport	hacked
Cathay Pacific Airways	2018	9,400,000	transport	hacked
Centers for Medicare & Medicaid Services	2018	75,000	healthcare	hacked

Why cryptography?

- Confidentiality
  - Keeping data and resources hidden
- Integrity
  - Data integrity (integrity)
  - Origin integrity (authentication)
- Availability
  - Denial-of-service attacks

Cryptography

1.1 Definition *Cryptography* is the study of **mathematical** techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication.

- **Encryption**: Converting plaintext into ciphertext using a secret key, so only authorized parties can recover the original message.
- **Decryption**: Reversing encryption to get back the plaintext, also requiring a secret key.
- **Digital Signatures**: Allowing a party to prove that a message truly came from them and has not been modified.
- **Hash Functions**: Mapping data of any size to a fixed-size value in a way that is hard to reverse or manipulate, often used for integrity checking.
- **Key Exchange**: Protocols that let two or more parties agree on a shared secret key over an insecure channel (e.g., Diffie–Hellman).

Week	Tue (MM.DD)	Tuesday Topic	Thursday Topic
1	8.26	Introduction and background on cryptography	One-time pad, information-theoretic security
2	9.2	Stream ciphers	PRG, pseudorandomness, CPA
3	9.9	Block ciphers; DES and attacks	AES, block ciphers from PRG, pRP, pRF
4	9.16	One-time key vs. many-time key; modes of operation	Padding-oracle attacks
5	9.23	Message Authentication Codes (MAC)	Generic birthday attack, cryptographic hash
6	9.3	Merkle–Damgård paradigm; Merkle hash tree	HMAC, authenticated encryption
7	10.7	Midterm	First presentation
8	10.14	Number theory	Diffie–Hellman key exchange
9	10.21	Trapdoor permutations; public-key encryption	RSA-based public-key encryption
10	10.28	Discrete-log–based public-key encryption	Digital signatures
11	11.4	RSA signature and BLS signature	One-way functions, Lamport signature
12	11.11	Blind signatures	Multi-party computation (MPC)
13	11.18	Zero-knowledge proof	Indistinguishability obfuscation
14	11.25	Fall Break	—
15	12.2	Presentation	Final exam review

Symmetric key cryptography

Public key cryptography

Advanced topics

Textbook

- Introduction to Modern Cryptography, **3rd edition**, Jonathan Katz and and Yehuda Lindell.

- A Graduate Course in Applied Cryptography, Dan Boneh's and Victor Shoup

What is this course about?

Example: Shamir Secret Sharing

- **Setup: hide the secret in a random polynomial**
  - Secret s = 5, prime p = 11; pick a random slope a = 3, set f(x) = 5 + 3x mod 11
  - Shares: f(1) = 8, f(2) = 0, f(3) = 3
- **Any 2 shares recover the secret**
  - Lagrange on (1, 8) and (3, 3): f(0) = 8·7 + 3·5 = 71 = 5 mod 11
  - Two points determine a line, so the intercept f(0) is unique
- **Any 1 share reveals nothing**
  - From (2, 0) alone: every candidate s admits exactly one slope with s + 2a = 0
  - All 11 secrets stay equally likely — perfect privacy, no assumptions needed

Security comes from counting consistent polynomials — the basis of MPC.

All Background You Need for This Course

https://joyofcryptography.com/pdf/chap0.pdf

Exponentiation and log

- $x^a \cdot x^b = x^{a+b}$
- $(x^a)^b = x^{ab}$
- $\log_x ab = \log_x a + \log_x b$
- $a\log_x b = \log_x b^a$

- $x^a \cdot x^b$ is **not** equal to x^{ab} !!!

Prime Number

- Prime number $\boldsymbol{p}$:
  - $\boldsymbol{p}$ is an integer
  - $\boldsymbol{p} \geq 2$
  - The only divisors of $\boldsymbol{p}$ are 1 and $\boldsymbol{p}$
- Examples
  - 2, 7, 19 are primes
  - -3, 0, 1, 6 are not primes
- Prime decomposition of a positive integer $\boldsymbol{n}$:

$$\boldsymbol{n} = \boldsymbol{p}_1^{\boldsymbol{e}_1} \times \ldots \times \boldsymbol{p}_{\boldsymbol{k}}^{\boldsymbol{e}_{\boldsymbol{k}}}$$

- Example:
  - $200 = 2^3 \times 5^2$

Modular Arithmetic

- Modulo operator for a positive integer n

$$r = a \bmod n$$

equivalent to

$$a = r + kn$$

and

$$r = a - \lfloor a/n \rfloor n$$

- Example:

$$29 \bmod 13 = 3 \quad 13 \bmod 13 = 0 \quad -1 \bmod 13 = 12$$
$$29 = 3 + 2\times 13 \quad 13 = 0 + 1\times 13 \quad 12 = -1 + 1\times 13$$

Modular Arithmetic

- simplify intermediate values mod n

- $a + b + c + \cdots mod\ n = \big((a + b)\ mod\ n + c\big) mod\ n + \ \ldots . mod\ n$
- $a \cdot b \cdot c \cdot \ldots mod\ n = \big((a \cdot b)\ mod\ n \cdot c\big) mod\ n + \ \ldots . mod\ n$

Modular exponentiation

- $x^a \cdot x^b = x^{a+b} \bmod n$
- $(x^a)^b = x^{ab} \bmod n$

Asymptotic complexity

- Big O notation O(n), $O(2^n)$
  - E.g., for sufficiently large integer n, $O(2^n) > O(n^c)$

$$
\begin{aligned}
f(n) \text{ is } O(g(n)) &\overset{\text{def}}{\Leftrightarrow} \lim_{n\to\infty} \frac{f(n)}{g(n)} < \infty \\
&\Leftrightarrow \exists c > 0 : \text{for all but finitely many } n : f(n) < c \cdot g(n) \\
f(n) \text{ is } \Omega(g(n)) &\overset{\text{def}}{\Leftrightarrow} \lim_{n\to\infty} \frac{f(n)}{g(n)} > 0 \\
&\Leftrightarrow \exists c > 0 : \text{for all but finitely many } n : f(n) > c \cdot g(n) \\
f(n) \text{ is } \Theta(g(n)) &\overset{\text{def}}{\Leftrightarrow} f(n) \text{ is } O(g(n)) \text{ and } f(n) \text{ is } \Omega(g(n)) \\
&\Leftrightarrow 0 < \lim_{n\to\infty} \frac{f(n)}{g(n)} < \infty \\
&\Leftrightarrow \exists c_1, c_2 > 0 : \text{for all but finitely many } n : \\
&\qquad\qquad c_1 \cdot g(n) < f(n) < c_2 \cdot g(n)
\end{aligned}
$$

Binary representation

- 17 = 10001, 38 = 100110
- Bitlength of number k is $\log_2 k$
- Complexity of an algorithm taking an integer k as input is computed on its bitlength

Binary string

- $\{0,1\}^n$ denotes the set of n-bit binary string.

- $\oplus$ xor:
  - Same as addition mod 2

a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

$x \oplus x = 000\cdots$	XOR'ing a string with itself results in zeroes.
$x \oplus 000\cdots = x$	XOR'ing with zeroes has no effect.
$x \oplus 111\cdots = \overline{x}$	XOR'ing with ones flips every bit.
$x \oplus y = y \oplus x$	XOR is symmetric.
$(x \oplus y) \oplus z = x \oplus (y \oplus z)$	XOR is associative.

Probability

- *Event*: a particular occurrence in some experiment
  - $\Pr[E]$: probability of event E

- Conditional probability: probability that one event occurs, *given that* some other event occurred
  - $\Pr[A \mid B] = \Pr[A \; and \; B]/\Pr[B]$

- Two r.v.'s X, Y are *independent* if
  for all x, y: $\Pr[X = x \mid Y = y] = \Pr[X = x]$

Probability

- Law of total probability: say E_1, …, E_n are a *partition* of all possibilities. Then for any A:

$$\Pr[A] = {}_i\Pr[A \; and \; E_i] = \Sigma_i \Pr[A \mid E_i] \cdot \Pr[E_i]$$

- Bayes's theorem: $\Pr[A \mid B] \cdot \Pr[B] = \Pr[B \mid A] \cdot \Pr[A]$