CSCI 1515 Applied Cryptography

Course Homepage: https://cs.brown.edu/courses/csci1515/spring-2024/

- Introduce Staff
- Syllabus
- Introduction & Overview
- Q & A
Logistics

- **Lectures**: Friedman 208 & Zoom (recorded)
- **Office Hour**: 1-2 pm Mondays, CIT 511 & Zoom, or by appointment
- **TA Hours**: See course website (calendar)
- **EdStem / Gradescope / Course Website**
- **Prerequisites / Override**:
  - CSCI 200/220 & 300/300
  - Basic algorithms & Programming in C/C++
- **Textbooks**: See course website
Assignments

- **Projects:** Warm-up + 5 + Final
  - Only final project will be done in pairs
  - Capstone option for final project

- **Written Homeworks:** 5

- **Collaboration / Google / ChatGPT:**
  - Write up your own solution
  - Acknowledge everyone you've worked with
  - Credit all resources you've looked at

- **Late Policy:**
  - Projects 0-5: 4 total days, at most 2 days per project
    - Beyond that: 20% penalty per day
  - Homeworks: 3 total days, at most 1 day per homework
    - Beyond that: lose credit
  - Final Project: No extension
Grading

- 4% Project 0
- 20% Projects 1-2
- 36% Projects 3-5
- 25% Homeworks 1-5
- 15% Final Project
What is Cryptography (used for)?

Study of techniques for protecting (sensitive/important) information.

Where is Cryptography used in practice?

What guarantees do we want in these scenarios?
Secure Communication

"Let's meet @ 9am"

What security guarantee(s) do we want?
Message Secrecy

Alice

Encrypt

(plaintext)

M

C

(ciphertext)

Decrypt

Bob

C

(Eavesdropper)

m = ?

m
Historical Ciphers

Ex: Substitution Cipher

Alice  --- C --- Bob

A → M  A ← M
B → A  B ← A
C → K  C ← K
D → W  D ← W
Eve  m=?

Z → L  Z ← L
Public-Key Encryption

Alice

 Encrypt

M

C

C

Eve

m = ?

Decrypt

Bob

(public)

(secret)
Message Integrity

Alice 🌹

“Let's meet @ 9 am”

tamper with

Eve 🌹

Bob 🌹

Is it from Alice?
Secure Authentication

Alice → Login → Google

Is it from Alice?

Password-based Authentication
Two-Factor Authentication

Search/Gmail/...

Is it from Google?

http vs. https
Projects Overview

Project 0 (Warm-up): Basic Schemes

Project 1: Secure Messaging

Project 2: Secure Authentication

Project 3: Zero-Knowledge Proofs

Project 4: Secure Multi-Party Computation

Project 5: Fully Homomorphic Encryption (Post-Quantum Crypto)
Project 3: Zero-Knowledge Proofs

[Alice]

[Bob]

Coke & Pepsi
taste differently

There is a bug in your code

I have the secret key
for this ciphertext
Example: Coke & Pepsi

[ Alice □
[ Coke & Pepsi taste differently ]

Bob □

$\mathbf{b} \in \{0, 1\}$

b = 0, Coke

b = 1, Pepsi

If statement is true:

If statement is false:
Project 4: Secure Multi-Party Computation

Alice

Bob

Second date?

Who is richer?

Common friends?
Example: Private Dating

\[ x \in \{0, 1\} \]

\[ y \in \{0, 1\} \]

Diagram with labeled nodes and arrows.
Project 5: Fully Homomorphic Encryption

\[ C_1 = \text{Enc}(m_1) \]  
\[ C_2 = \text{Enc}(m_2) \]  
\[ c' = \text{Enc}(m_1 + m_2) \]  
\[ c'' = \text{Enc}(m_1 \cdot m_2) \]
Example: Privacy-Preserving Query

Server

Client

Encrypt

Decrypt

Search/ML/GPT/...

c' ← Eval(F, c)
Q & A

- CSCI 1510 (Introduction to Cryptography and Computer Security)
- MATH 1580 (Cryptography)

- Why C++?

- Class Participation

- What else are you interested in learning?