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 & 300/320  
  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 @ 9 am”

What security guarantee(s) do we want?
Message Secrecy  Symmetric-key Encryption

Alice  C  Bob

Encrypt  ↓  Decrypt

(plaintext)  m  m

(Eavesdropper)  Eve  m = ?

(plaintext)  m  m

(ciphertext)  C  C
Historical Ciphers

Ex: Substitution Cipher

Alice

Bob

A → M
B → A
C → K
D → W
Eve

m = ?
Eve

Z → L

A ← M
B ← A
C ← K
D ← W
Z ← L
Public-Key Encryption

Alice → Encrypt → C → Decrypt → Bob

Eve: m = ?

(public) → (secret)
Message Integrity

"Let's meet @ 9am"

Eve tamper with

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

Bob

[Coke & Pepsi
taste differently]

If statement is true: \( \Pr[\text{Alice answers correctly}] = 1 \)

If statement is false: \( \Pr[\ldots] = \left(\frac{1}{2}\right)^{100} \)
Project 4: Secure Multi-Party Computation

Alice: $x \in \{0, 1\}$
Bob: $y \in \{0, 1\}$
Charlie: $x \land y$

Who is richer?

Common friends?
Example: Private Dating

If $x = y = 1 \Rightarrow 11100$
Otherwise $\Rightarrow 11010$
Project 5: Fully Homomorphic Encryption

\[
\begin{align*}
C_1 &= \text{Enc}(m_1) \\
C_2 &= \text{Enc}(m_2) \\
C &= \text{Enc}(m_1 + m_2) \\
C'' &= \text{Enc}(m_1 \cdot m_2)
\end{align*}
\]
Example: Privacy-Preserving Query

Server

\[ \text{Encrypt} \]

\[ m \]

\[ c \]

\[ \text{Search/ML/GPT/…} \]

\[ c' \leftarrow \text{Eval}(F, c) \]

\[ c' \]

\[ \text{Decrypt} \]

\[ F(m) \]
Q & A

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

- Why C++?

- Class Participation

- What else are you interested in learning?