CSCI 1515 Applied Cryptography

Course Homepage: https://brownappliedcryptography.github.io/

- Introduce Staff
- Syllabus
- Q & A
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

“Alice” -> “Let’s meet @ 9am” -> Bob

Eve

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

Alice

plaintext \( m \) \( \rightarrow \) Encrypt \( \rightarrow \) ciphertext \( c \) \( \rightarrow \) Bob

Eavesdropper

\( m = ? \)

Decrypt

\( m \)
Historical Ciphers

Ex: Substitution Cipher

Alice → Bob

A → M
B → A
C → K
D → W

Eve

m = ?

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

Alice

 Encrypt

m

C

Eve

m = ?

Decrypt

Bob

C

m

(public)

(secret)
Message Integrity

Alice \( \rightarrow \) “Let’s meet @ 9 am” \( \rightarrow \) Bob

Eve \( \uparrow \text{tamper with} \)

Is it from Alice?
Secure Authentication

Alice → Login → Google

Is it from Alice?

Search/Gmail/... →

Is it from Google?
Projects Overview

Project 0 (Warm-up): Basic Schemes

Project 1: Secure Communication

Project 2: Secure Authentication

Project 3: Zero-Knowledge Proofs

Project 4: Secure Multi-Party Computation

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

Alice

Bob

Coca-Cola & Pepsi taste differently

There is a bug in your code

I have the secret key for this ciphertext
Ex: Coca-Cola & Pepsi

If statement is true:

If statement is false:

Coca-Cola & Pepsi

taste differently

\[ b \leq \frac{13}{20} \]

\[ b = 0, \text{ Coca-Cola} \]

\[ b = 1, \text{ Pepsi} \]
Project 4: Secure Multi-Party Computation

Alice

Who is richer?

Bob

Second date?

Common friends?
Ex: Private Dating

Symbols:
- Female: ♂
- Male: ♀
- Yes: ✔
- No: ☐
- Question Mark: ?

Diagram:
- Male (♂) with 'YES, 0, 13'
- Female (♀) with 'NO, 0, 13'
- Female (♀) with 'YES, 0, 13'
- Male (♂) with 'NO, 0, 13'
- Female (♀) with 'NO, 0, 13'
- Male (♂) with 'NO, 0, 13'
- Female (♀) with 'NO, 0, 13'
- Male (♂) with 'NO, 0, 13'

Nodes:
- D
- D
- 1
- 1
- 1

Connections:
- Red arrows from female to male with 'YES, 0, 13'
- Blue arrows from male to female with 'NO, 0, 13'

Question Mark:
- Female (♀) with question mark
- Male (♂) with question mark
Project 5: Fully Homomorphic Encryption

Alice

\[ \text{Encrypt} \]

Bob

\[ \text{Decrypt} \]

\[ C = \text{Enc}(m_1 + m_2) \]

\[ C_1 = \text{Enc}(m_1) \]

\[ C_2 = \text{Enc}(m_2) \]
Ex. Outsourced Computation

- Alice
- Server
- Encrypt
- Compute $f$
- $c' = \text{Enc}(f(m))$

Diagram:
- Alice sends $m$ to Encrypt, which computes $c = \text{Encrypt}(m)$
- Encrypt sends $c$ to Compute $f$.
- Compute $f$ computes $c'$ and sends it to Store $c$. Store $c$.
What else would you like to learn?

- Differential Privacy
- Crypto applications in machine learning
- Crypto techniques used in blockchain
Quick Survey

Do you know what this means:

- polynomial-time algorithm
- NP-hard problem
- a divides b \((a \mid b)\)
- greatest common divisor \(\text{gcd}(a,b)\)
- (Extended) Euclidean Algorithm
- Groups
- One-Time Pad
- RSA encryption/signature
- Diffie-Hellman key exchange
- SHA (hash functions)