CSCI 1515 Applied Cryptography

Course Homepage: https://cs.brown.edu/courses/csci1515/spring-2025/

This Lecture:

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

Logistics

- Lectures: Salomon 001 & Zoom (recorded)
- Office Hour: 4:30-5:30pm Mondays, CIT 511 & Zoom, or by appointment
- TA Hours: See course website (calendar)
- EdStem / Gradescope / Course Website
- Prerequisites / Override:
  CSCI 190/200 & 300/300, 220 highly recommended
  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: 2 late days for free per project
    Beyond that: 40% penalty per day
  - Homeworks: No extension
  - Final Project: No extension

Grading

- 1% Self Introduction
- 5% Project 0 (Cipher)
- 30% Projects 1 (Signal), 2 (Auth), 4 (PIR)
- 24% Projects 3 (Vote), 5 (Yaos)
- 25% Homeworks 1-5
- 15% Final Project

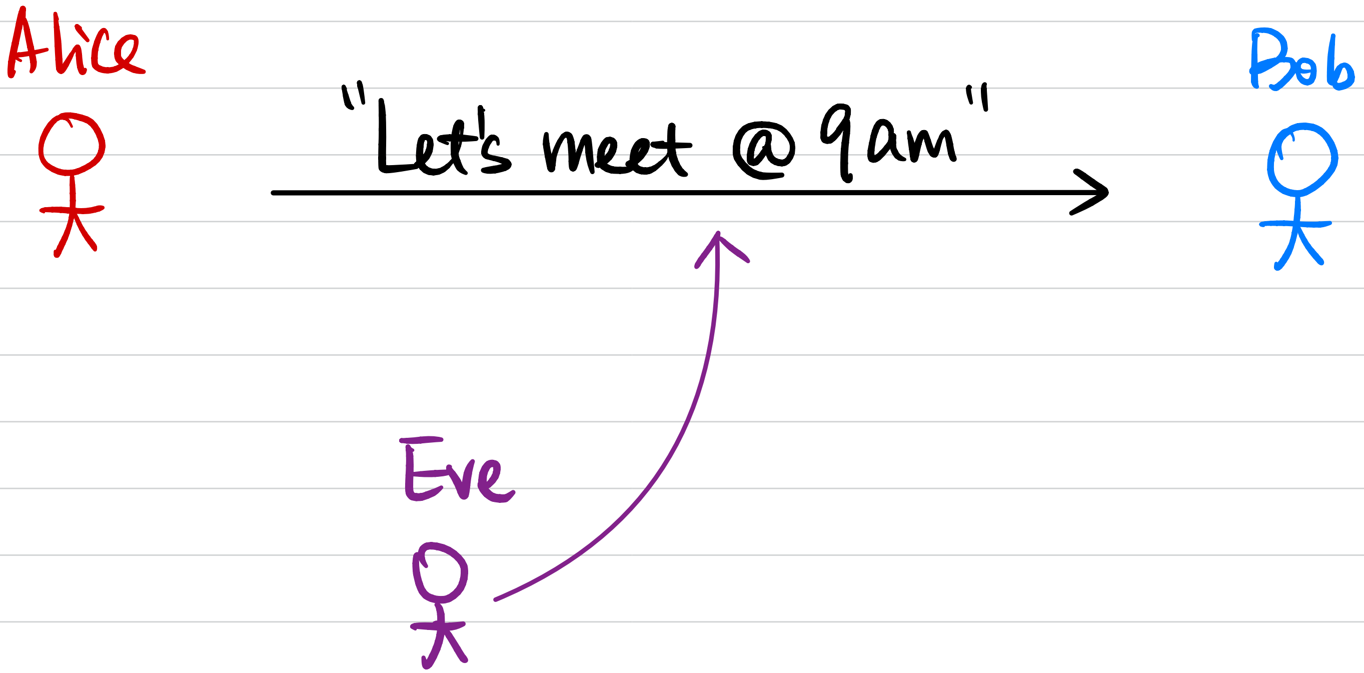
What is Cryptography (used for)?

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

Where is Cryptography used in practice?

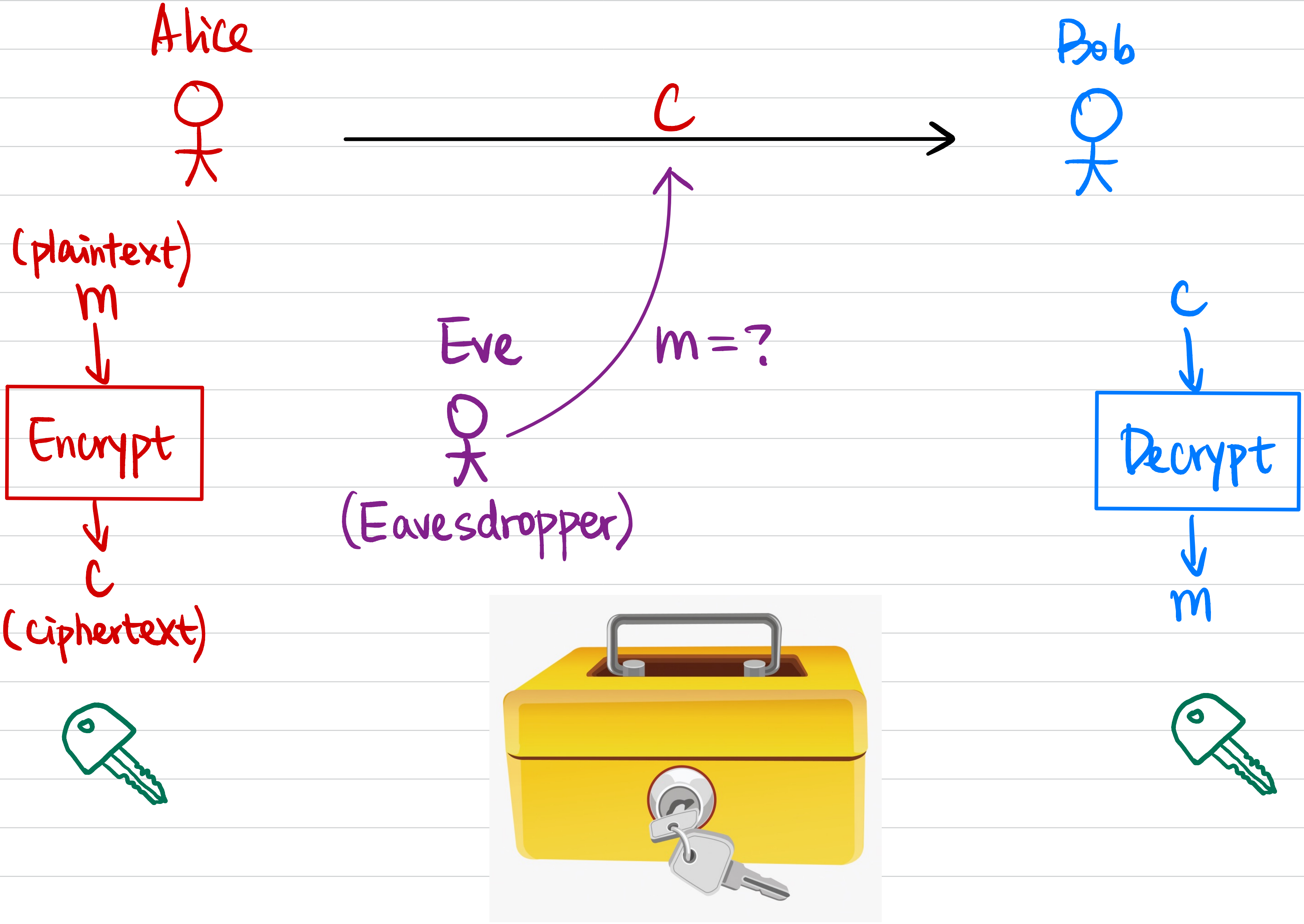
What guarantees do we want in these scenarios?

Secure Communication



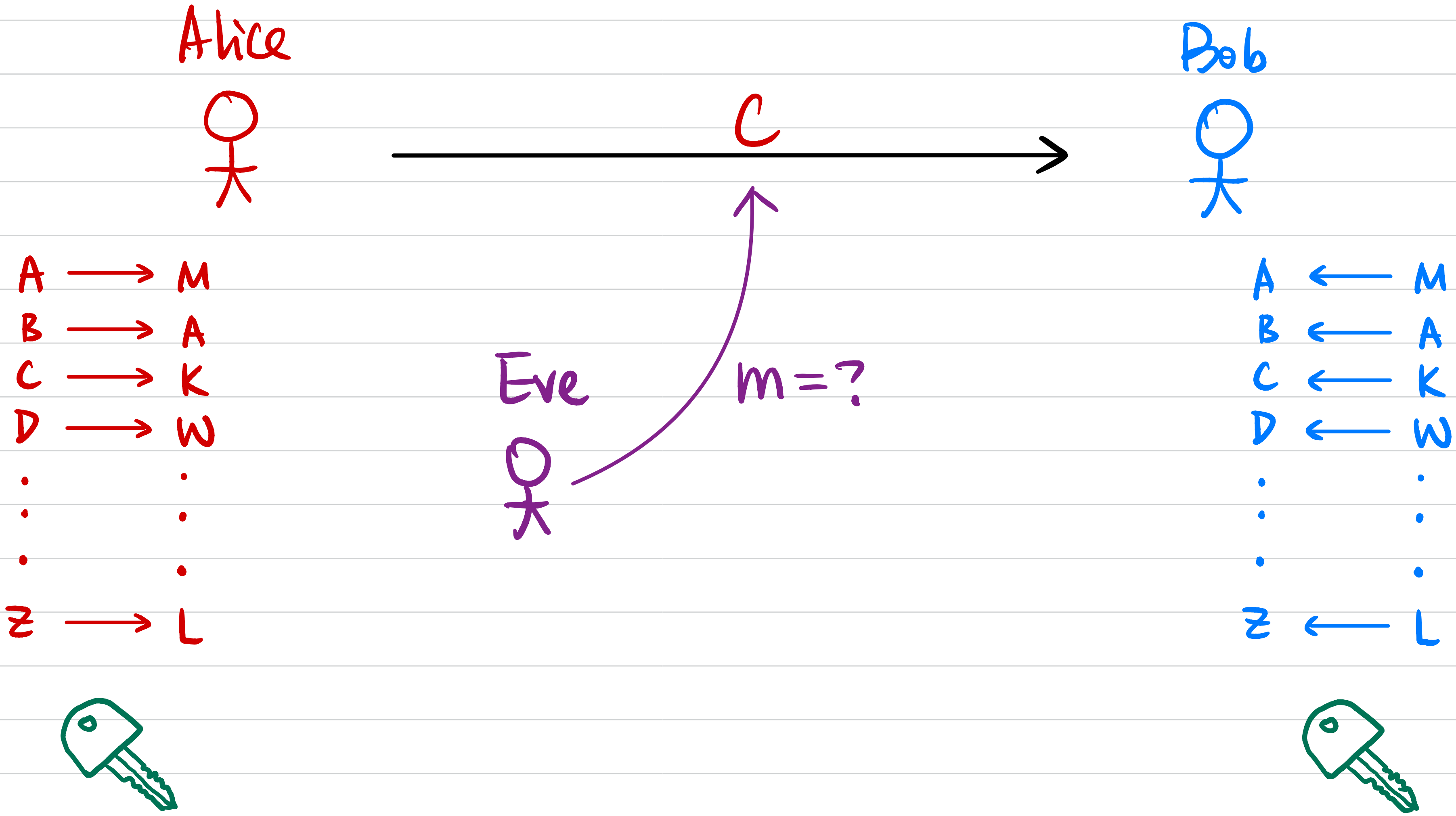
What security guarantee(s) do we want?

Message Secrecy

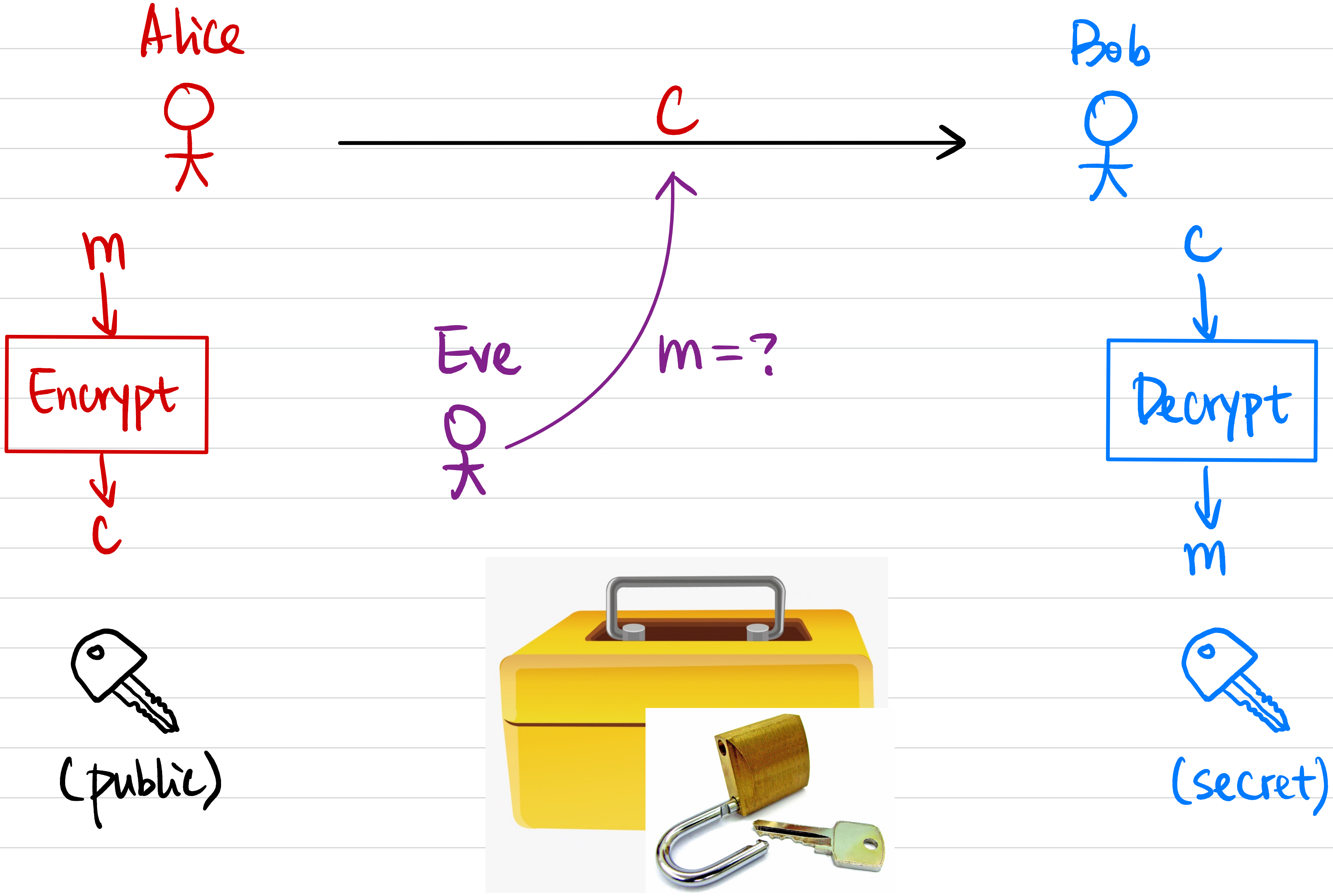


Historical Ciphers

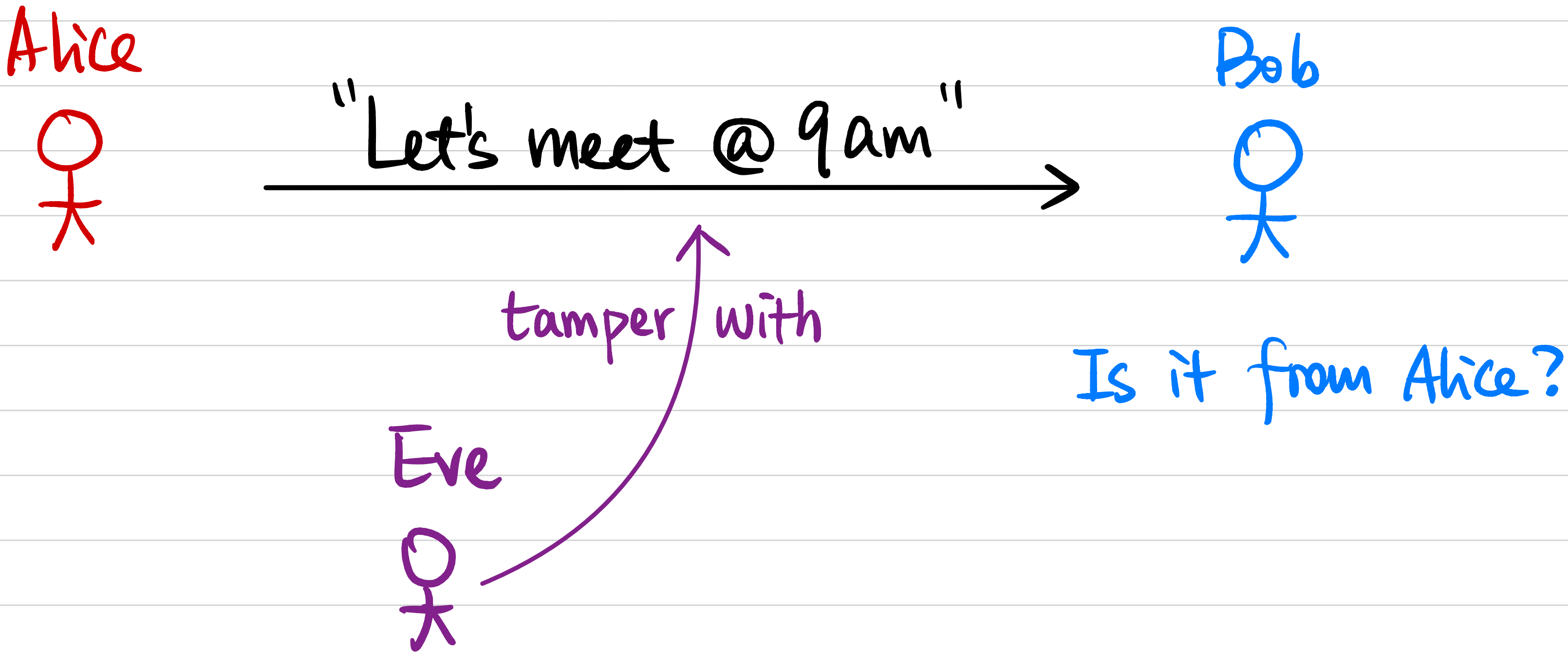
Ex: Substitution Cipher



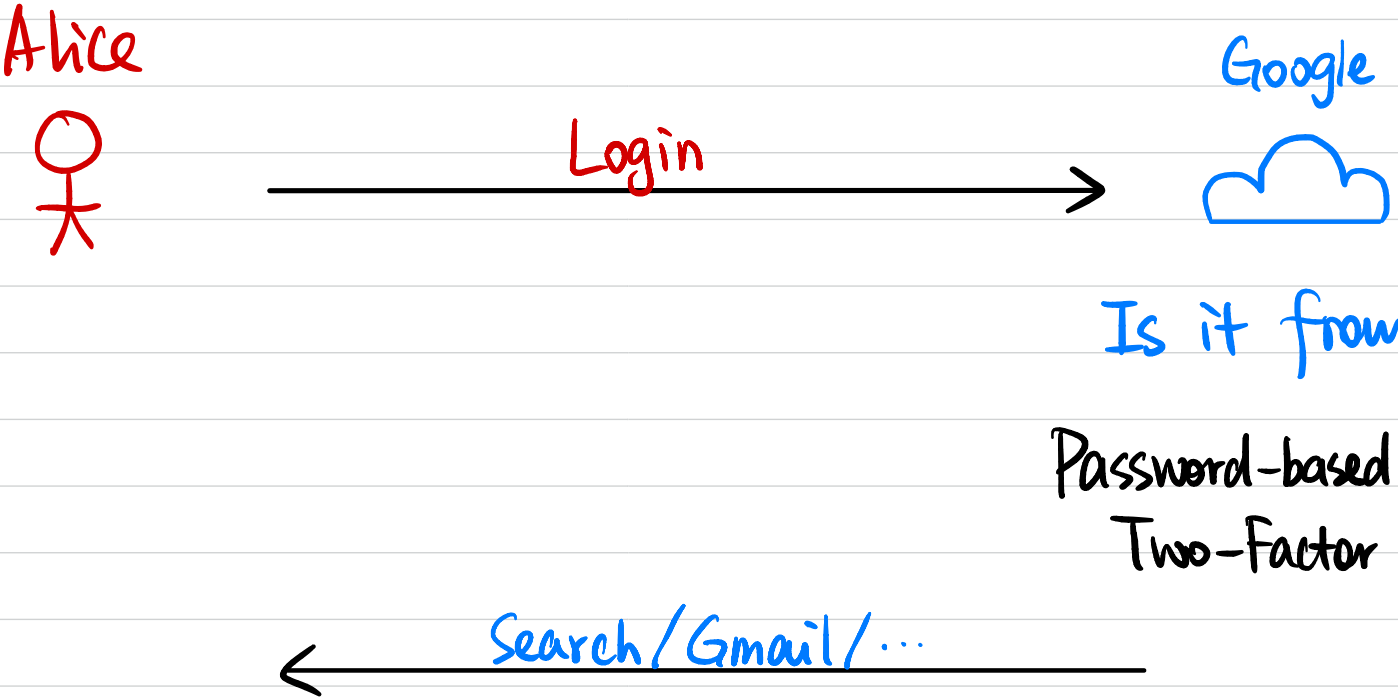
Public-Key Encryption



Message Integrity



Secure Authentication



Is it from Alice?

Password-based Authentication
Two-Factor Authentication

Is it from Google?

http vs. https

Projects Overview

Project 0 (Cipher): Basic Schemes

Project 1 (Signal): Secure Messaging

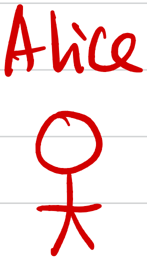
Project 2 (Auth): Secure Authentication

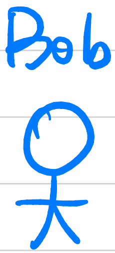
Project 3 (Vote): Zero-Knowledge Proofs

Project 4 (PIR): Fully Homomorphic Encryption (Post-Quantum Crypto)

Project 5 (Yaos): Secure Multi-Party Computation

Project 3: Zero-Knowledge Proofs





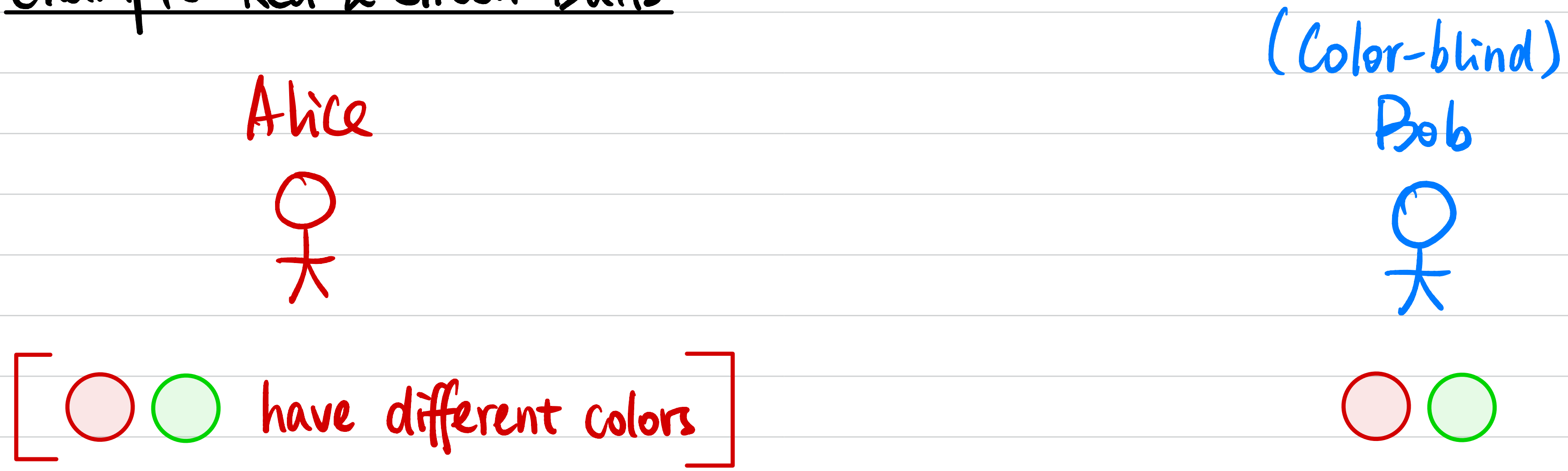
There is a bug in your code

I have the secret key
for this ciphertext

There is enough balance
in my Bitcoin account

🔴 🟢 have different colors

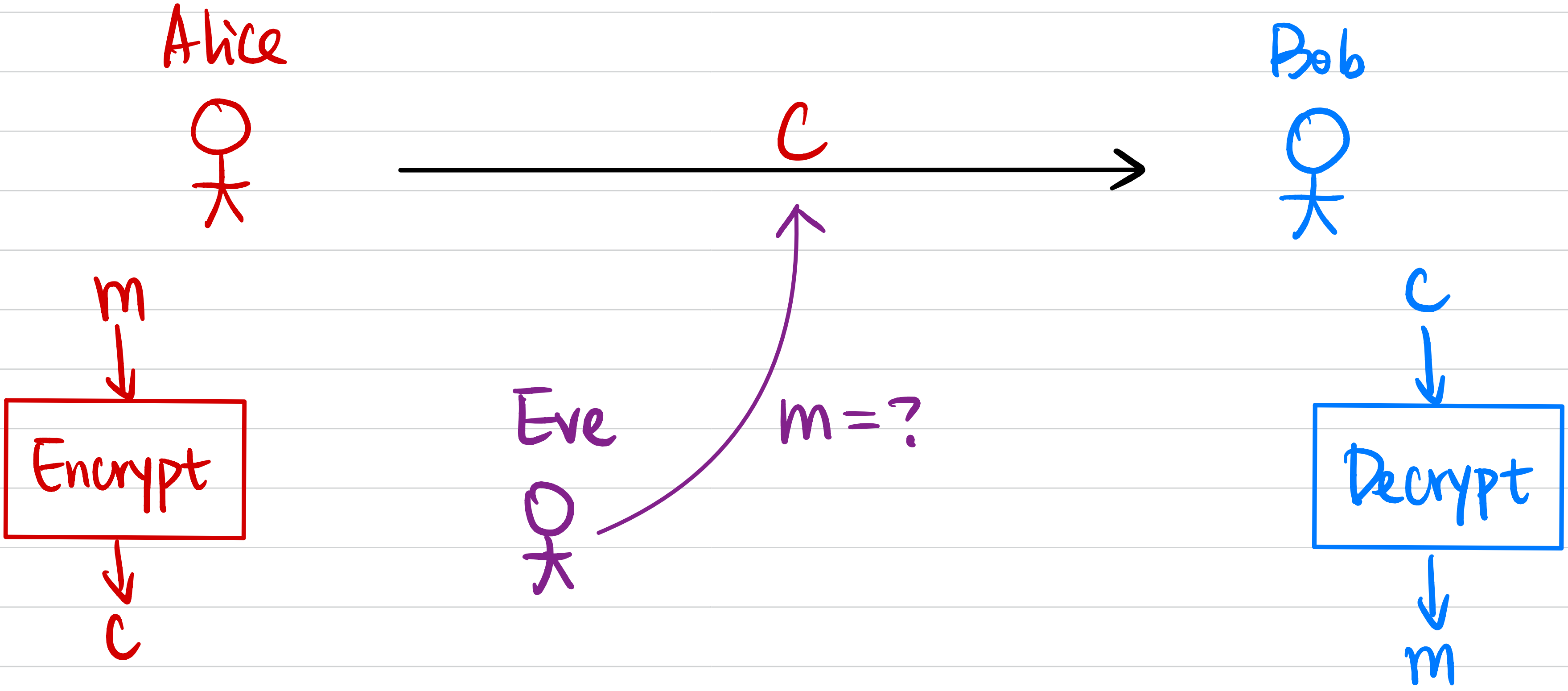
Example: Red & Green Balls



If statement is true:

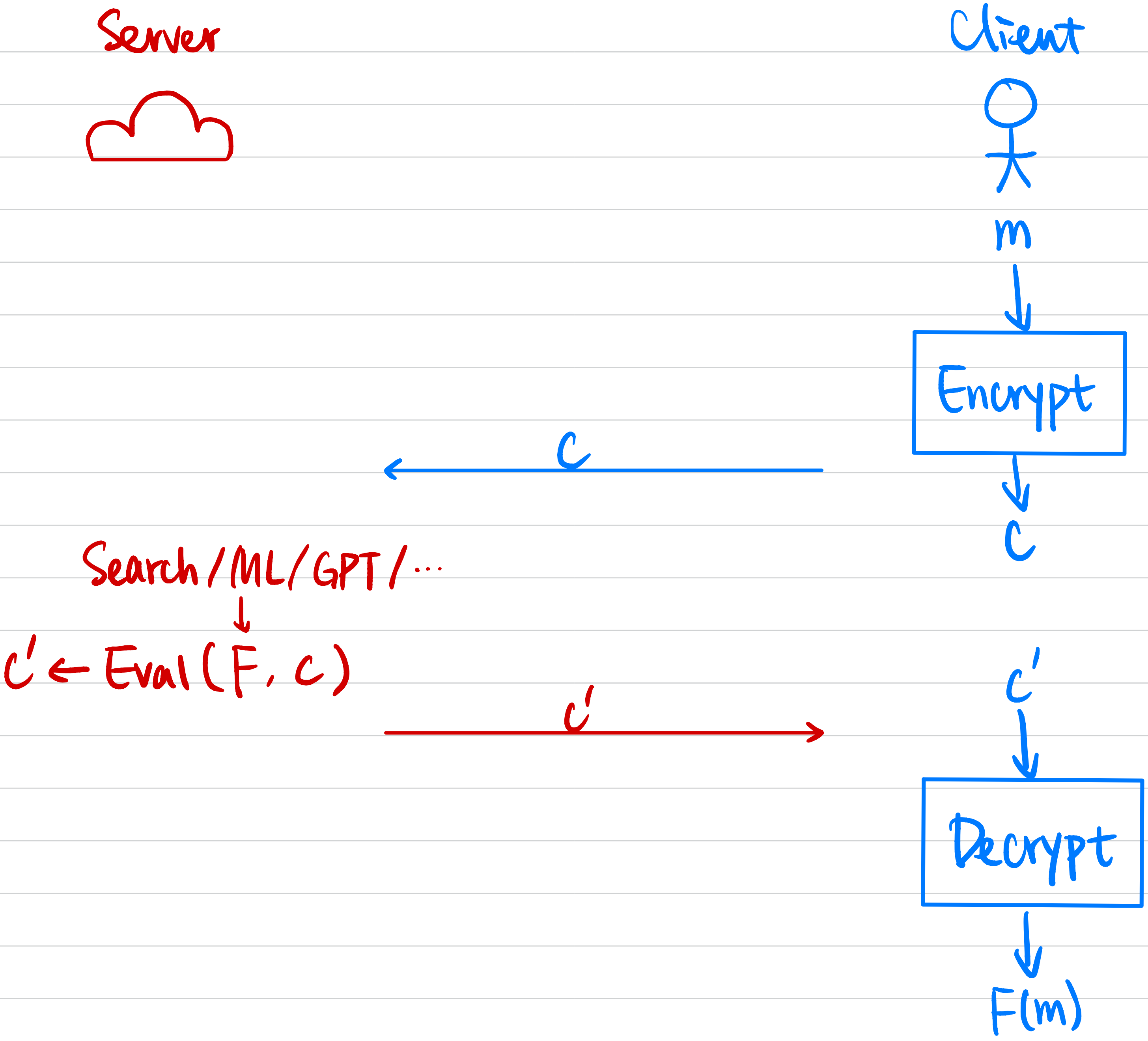
If statement is false:

Project 4: Fully Homomorphic Encryption



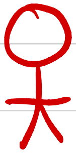
$$\begin{aligned} c_1 &= \mathrm{Enc}(m_1) \\ c_2 &= \mathrm{Enc}(m_2) \end{aligned} \quad \Longrightarrow \quad \begin{aligned} c' &= \mathrm{Enc}(m_1 + m_2) \\ c'' &= \mathrm{Enc}(m_1 \cdot m_2) \end{aligned}$$

Example: Privacy-Preserving Query



Project 5: Secure Multi-Party Computation

Alice



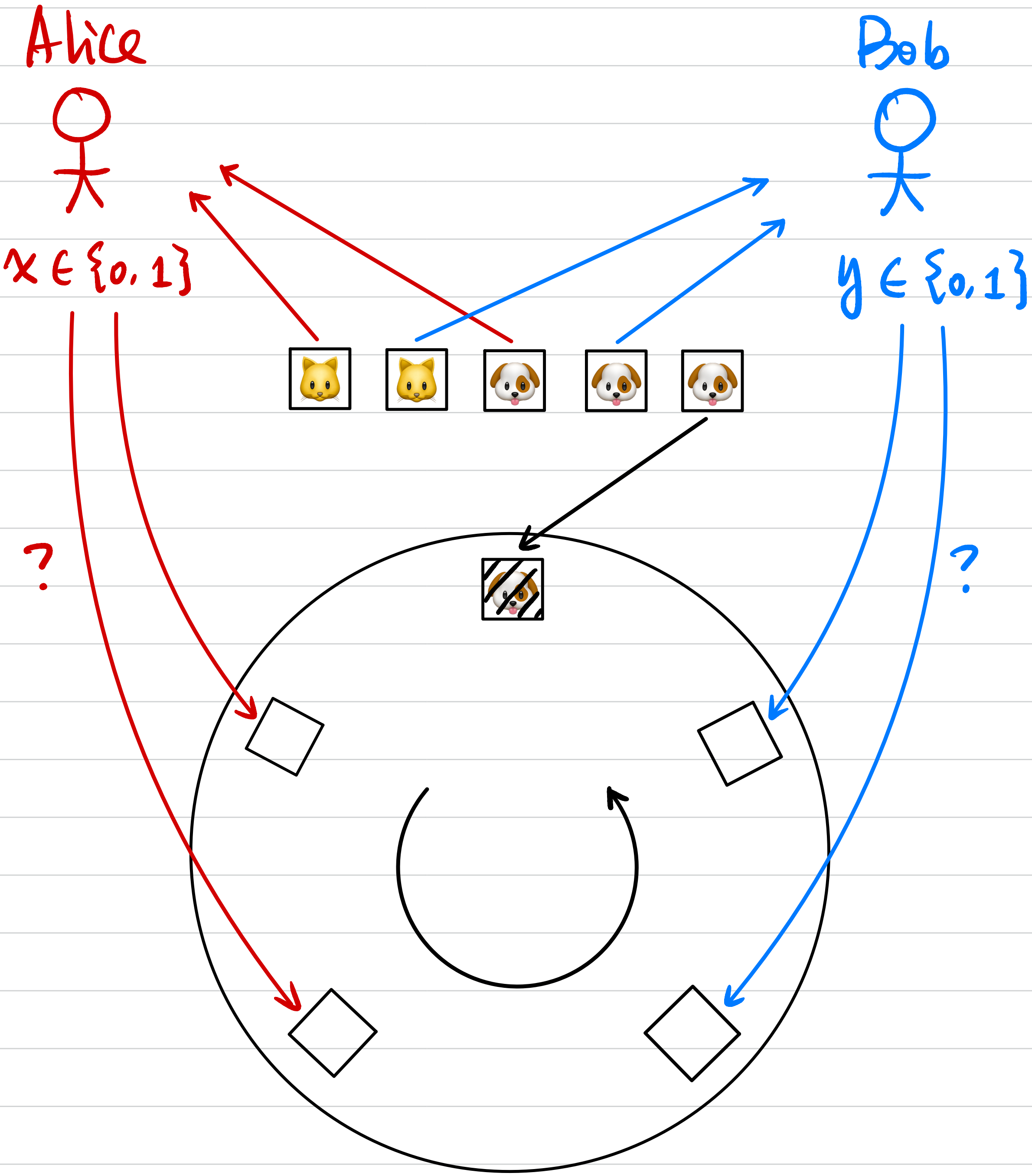
Second date?

Bob

Who is richer?

Mutual friends?

Example: Private Dating



Q & A

- Crypto background?
- Readings before/after lecture?
- Why C++?
- Class Participation
- Remote-Only Students
- Another course with conflicting time?
- CSCI 1040 (The Basics of Cryptographic Systems) "Crypto for poets"

  MATH 1580 (Cryptography) Why is it correct?

  CSCI 1510 (Introduction to Cryptography and Computer Security) Why is it secure?

  CSCI 1515 (Applied Cryptography) How to use it?