CSCI 1515 Applied Cryptography

Course Homepage: https://cs.brown.edu/courses/csci1515/spring-2026

This Lecture:

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

Explore new and existing community resources and mental health support:

BROWN

The Brown community is resilient, caring and strong.

We are ever true.

Logistics

- **Lectures**: Friedman 108 & 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 220/500/1010/1550/1570/APMA 1650/MATH 1530
    (Basic explosure to algorithms & discrete probability)
  - CSCI 300/330 (Programming in C/C++)
- **Textbooks**: See course website

Assignments

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

- **Written Homeworks:** 5

- **Collaboration:**
  - Write up your own solution
  - Acknowledge everyone you've worked with

- **Late Policy:**
  - Projects 0-5: 4 total days, at most 2 days per project
    Beyond that: 40% penalty per day
  - Homeworks: No extension
  - Final Project: No extension

Grading

- 1% Self Introduction
- 4% Project 0 (Cipher)
- 24% Projects 1 (Signal), 2 (Auth), 5 (PIR)
- 24% Projects 3 (Vote), 4 (Yaos)
- 8% Code Review 1 & 2
- 25% Homeworks 1-5
- 14% Final Project

Grade Cutoffs:

A: 90% B: 80% C/S: 70%

AI Policy

- Strongly discouraged !
- Write up your own solution
- Credit AI tools you've used (even for brainstorming)

Generative AI Can Harm Learning

Hamsa Bastani,[1*] Osbert Bastani,[2*] Alp Sungu,[1*†]
Haosen Ge,[3] Özge Kabakcı,[4] Rei Mariman

[1]Operations, Information and Decisions, University of Pennsylvania
[2]Computer and Information Science, University of Pennsylvania
[3]Wharton AI & Analytics, University of Pennsylvania
[4]Budapest British International School

[*]These authors (H.B., O.B., A.S.) contributed equally.
[†]To whom correspondence should be addressed; E-mail: alpsungu@wharton.upenn.edu.

Generative artificial intelligence (AI) is poised to revolutionize how humans work, and has already demonstrated promise in significantly improving human productivity. However, a key remaining question is how generative AI affects *learning*, namely, how humans acquire new skills as they perform tasks.

Your Brain on ChatGPT: Accumulation of Cognitive Debt when Using an AI Assistant for Essay Writing Task△

Nataliya Kosmyna [1]
MIT Media Lab
Cambridge, MA

Eugene Hauptmann
MIT
Cambridge, MA

Ye Tong Yuan
Wellesley College
Wellesley, MA

Jessica Situ
MIT
Cambridge, MA

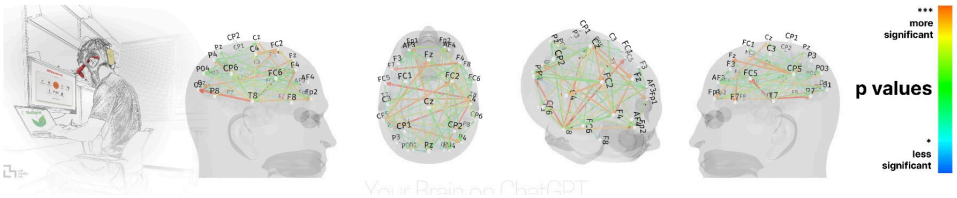
Xian-Hao Liao
Mass. College of Art and Design (MassArt)
Boston, MA

Ashly Vivian Beresnitzky
MIT
Cambridge, MA

Iris Braunstein
MIT
Cambridge, MA

Pattie Maes
MIT Media Lab
Cambridge, MA

United States



In-Class Laptop & Tablet Policy

- No laptop usage in lectures!
- Tablets for note-taking must remain flat on desk

Laptop multitasking hinders classroom learning for both users and nearby peers

Faria Sana [a], Tina Weston [b,c], Nicholas J. Cepeda [b,c,*]

[a] McMaster University, Department of Psychology, Neuroscience, & Behaviour, 1280 Main Street West, Hamilton, ON L8S 4K1, Canada
[b] York University, Department of Psychology, 4700 Keele Street, Toronto, ON M3J 1P3, Canada
[c] York University, LaMarsh Centre for Child and Youth Research, 4700 Keele Street, Toronto, ON M3J 1P3, Canada

ARTICLE INFO

Article history:
Received 11 September 2012
Received in revised form
5 October 2012
Accepted 12 October 2012

Keywords:
Laptops
Multitasking
Attentional control
Pedagogy

ABSTRACT

Laptops are commonplace in university classrooms. In light of cognitive psychology theory on costs associated with multitasking, we examined the effects of in-class laptop use on student learning in a simulated classroom. We found that participants who multitasked on a laptop during a lecture scored lower on a test compared to those who did not multitask, and participants who were in direct view of a multitasking peer scored lower on a test compared to those who were not. The results demonstrate that multitasking on a laptop poses a significant distraction to both users and fellow students and can be detrimental to comprehension of lecture content.

Psychological Science
1–10

DOI: 10.1177/0956797614524581
pss.sagepub.com
SAGE

The Pen Is Mightier Than the Keyboard: Advantages of Longhand Over Laptop Note Taking

Pam A. Mueller[1] and Daniel M. Oppenheimer[2]
[1]Princeton University and [2]University of California, Los Angeles

Abstract
Taking notes on laptops rather than in longhand is increasingly common. Many researchers have suggested that laptop note taking is less effective than longhand note taking for learning. Prior studies have primarily focused on students' capacity for multitasking and distraction when using laptops. The present research suggests that even when laptops are used solely to take notes, they may still be impairing learning because their use results in shallower processing.

What is Cryptography (used for)?

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

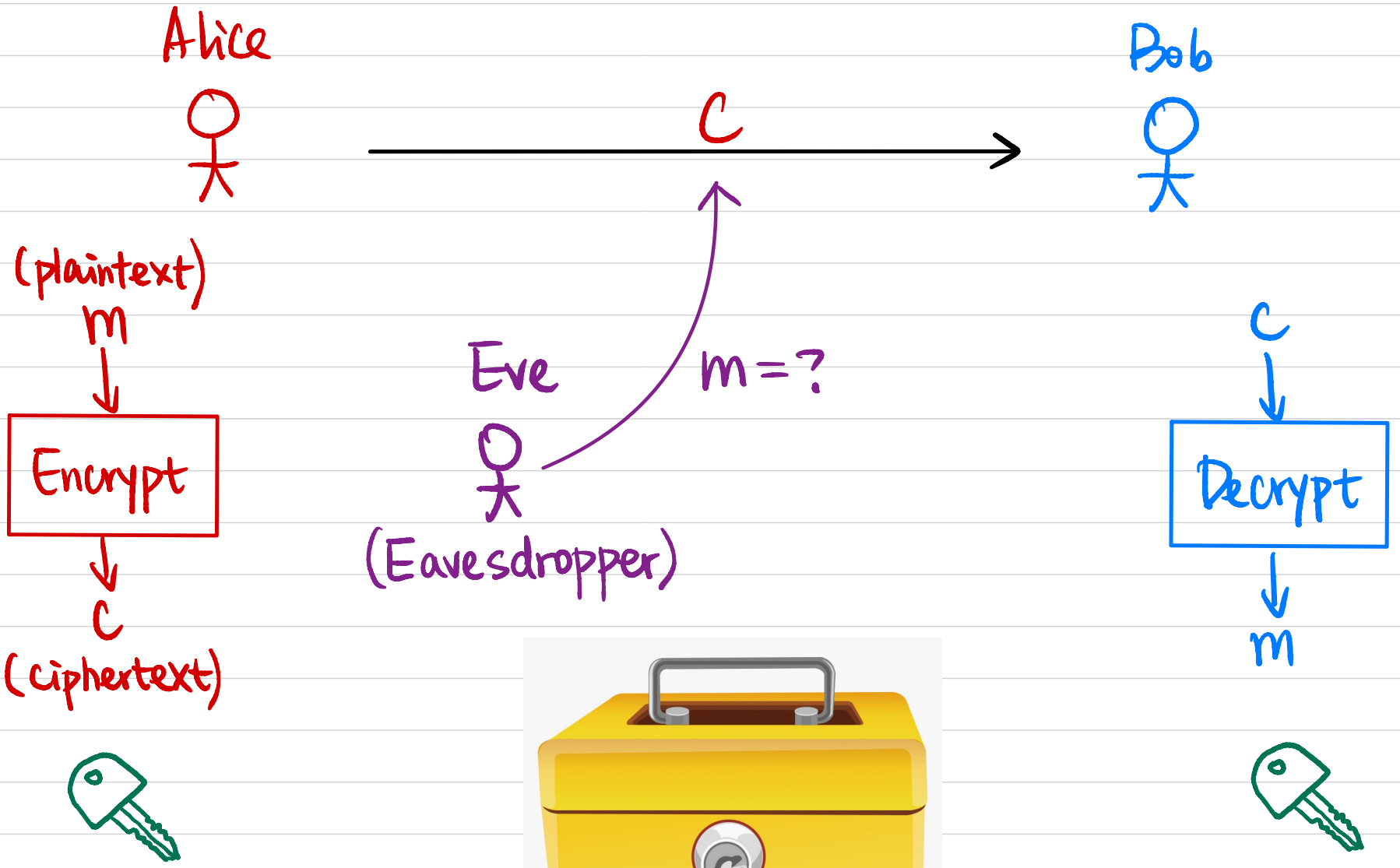
Where is cryptography used in practice?

What guarantees do we want in these scenarios?

Secure Communication

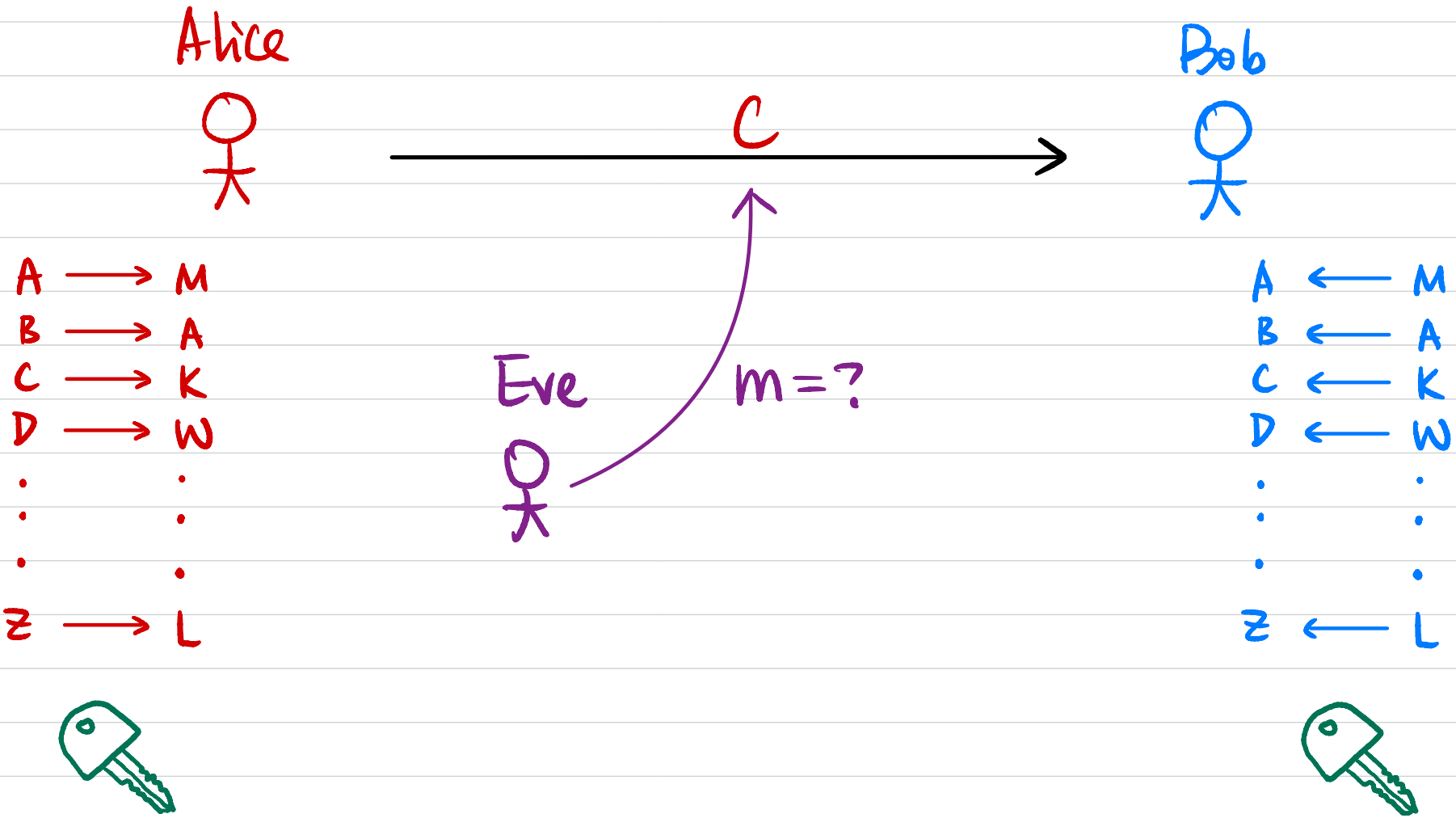
What security guarantee(s) do we want?

Message Secrecy

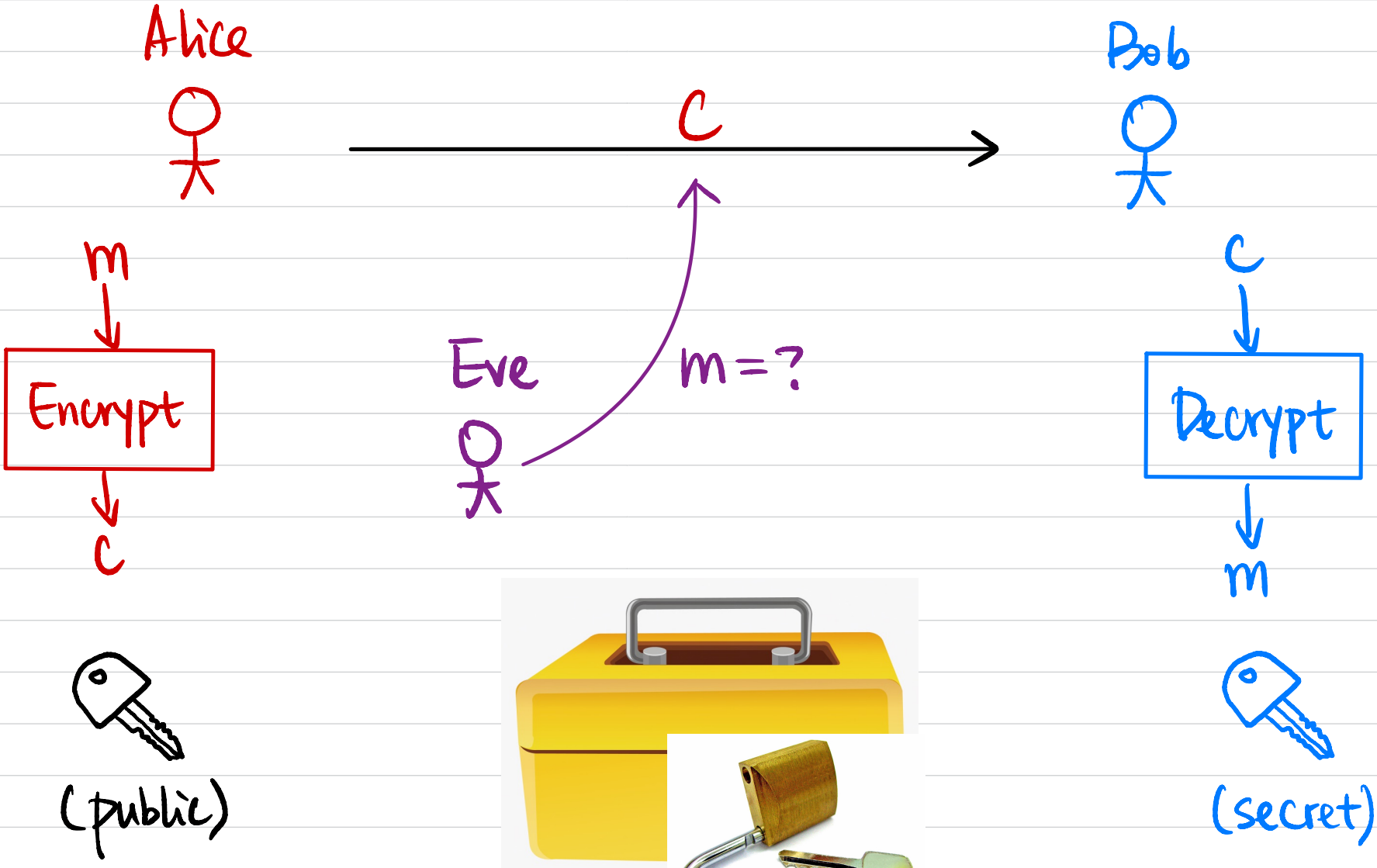


Historical Ciphers

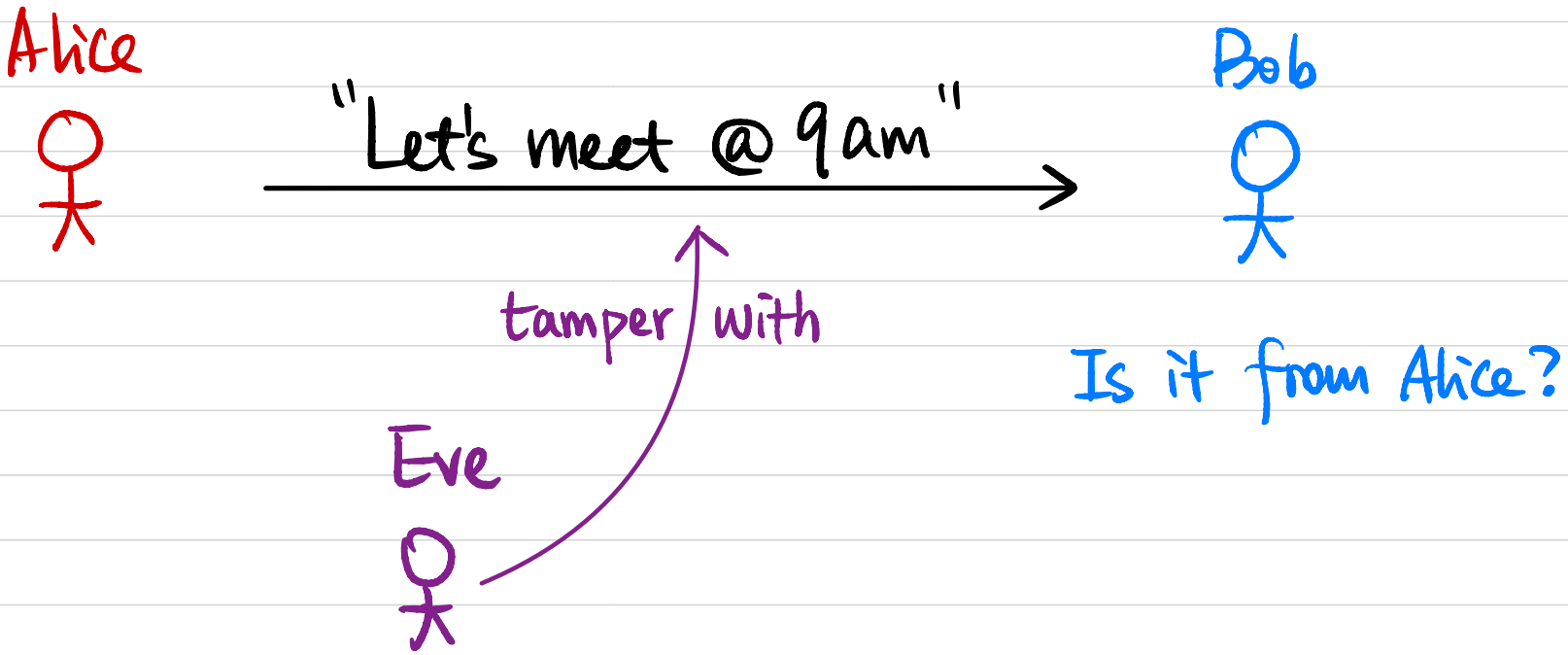
Ex: Substitution Cipher



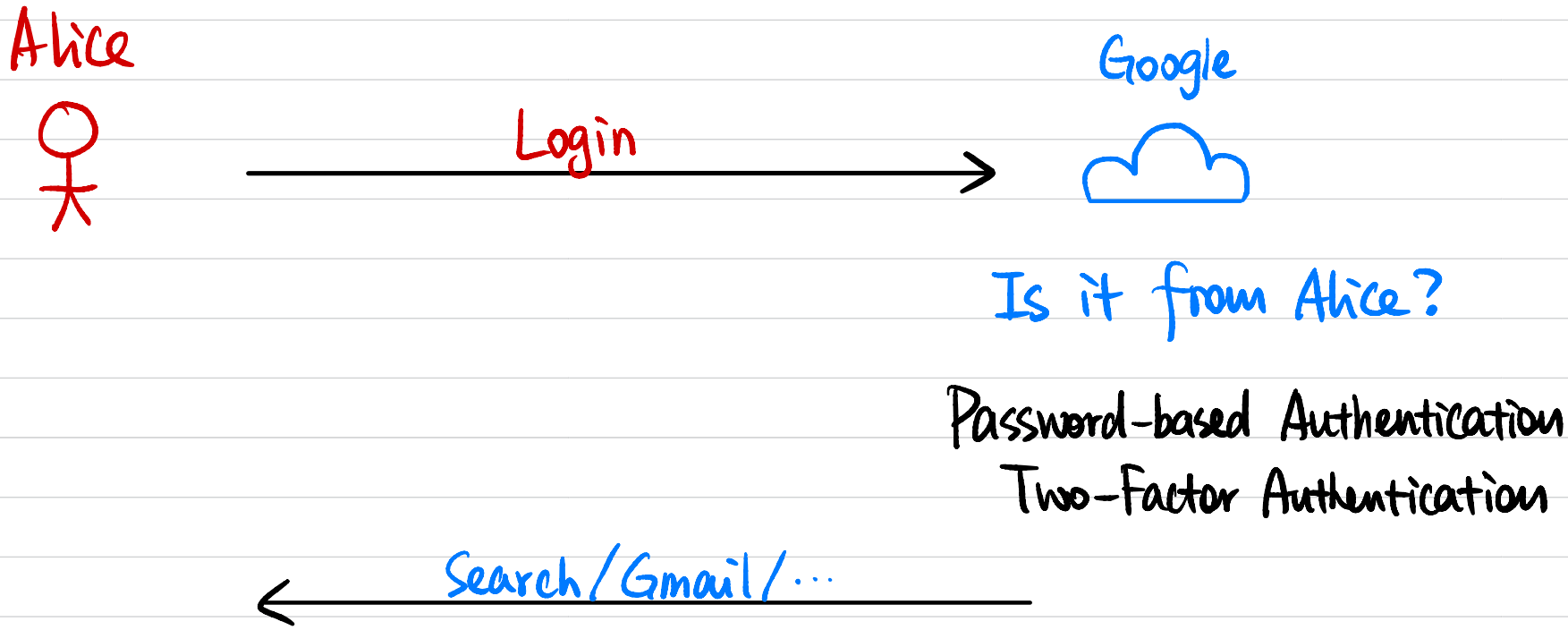
Public-Key Encryption



Message Integrity



Secure Authentication



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 (Yaos): Secure Multi-Party Computation

Project 5 (PIR): Fully Homomorphic Encryption (Post-Quantum Crypto)

Project 3: Zero-Knowledge Proofs

Alice

Bob

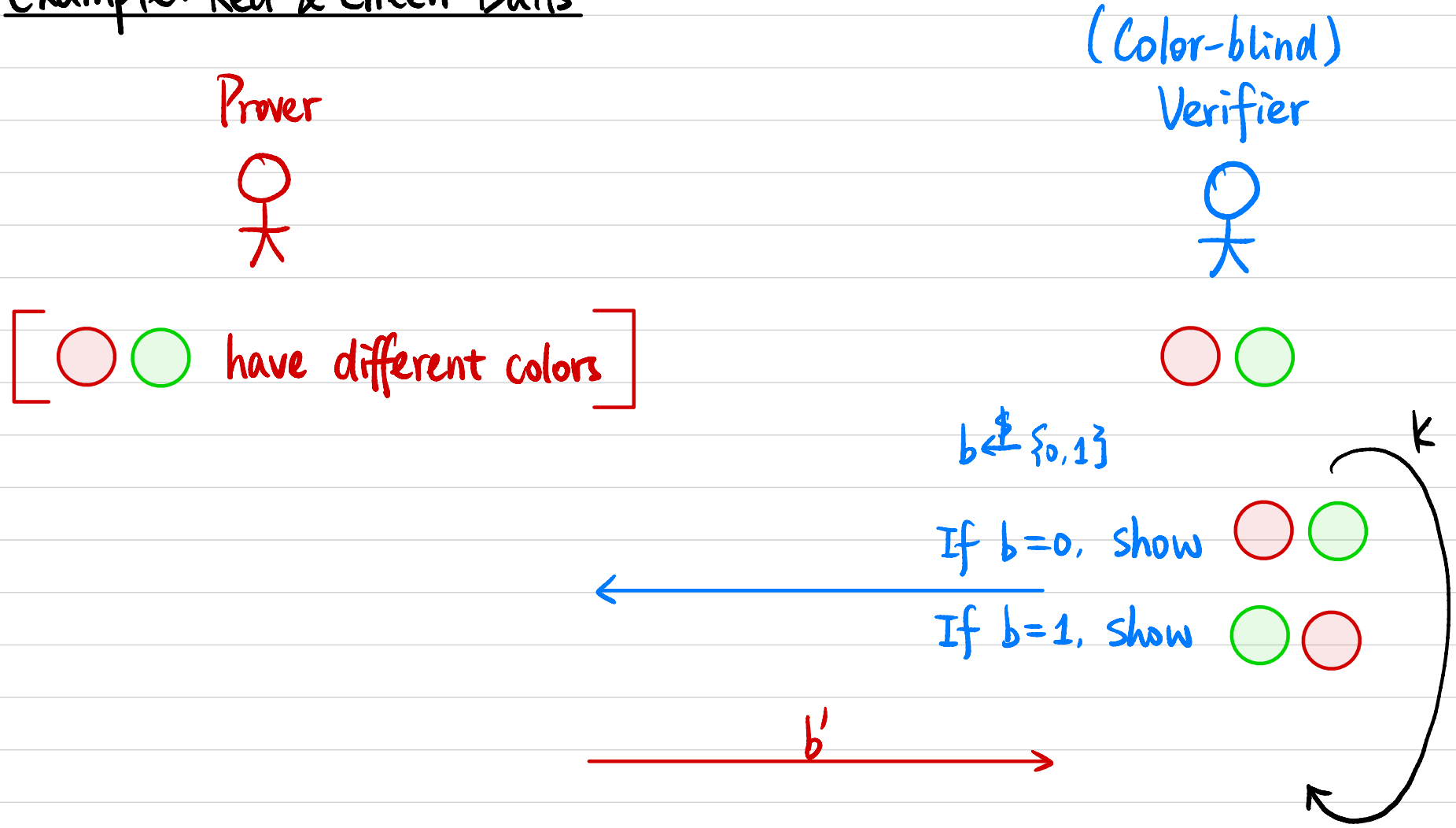
[There is a bug in your code]

[I have the secret key for this ciphertext]

[There is enough balance in my Bitcoin account]

[ have different colors]

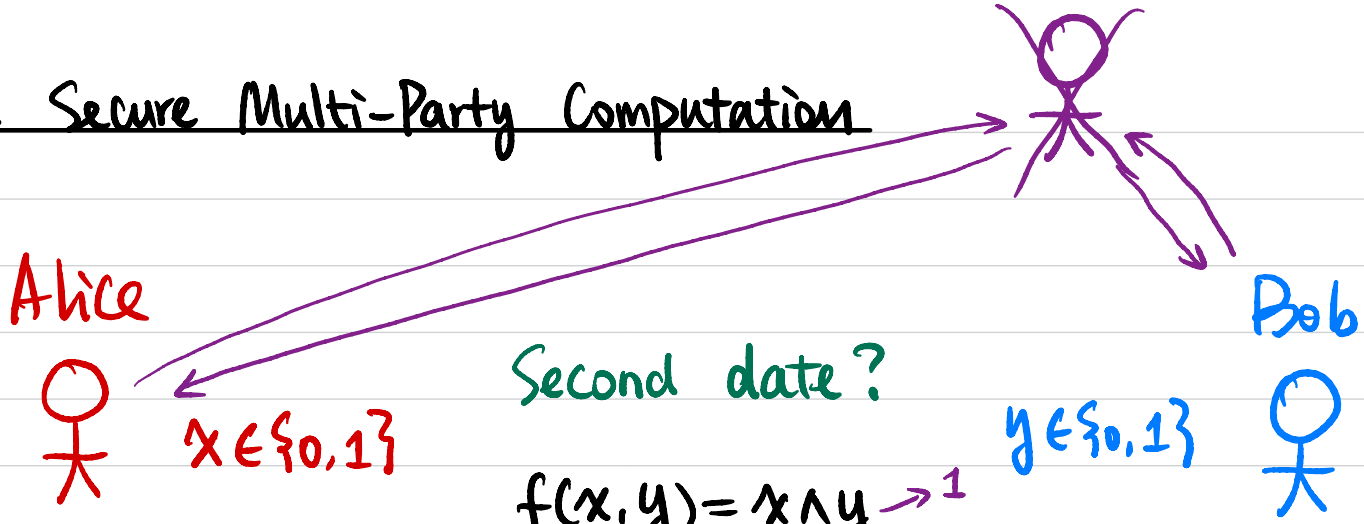
Example: Red & Green Balls



If statement is true: $\Pr[b=b'] = 1$

If statement is false: $\Pr[b=b'] = (1/2)^k$

Project 4: Secure Multi-Party Computation



Second date?

$f(x,y) = x \wedge y \rightarrow 1, 0$

Who is richer?

x y

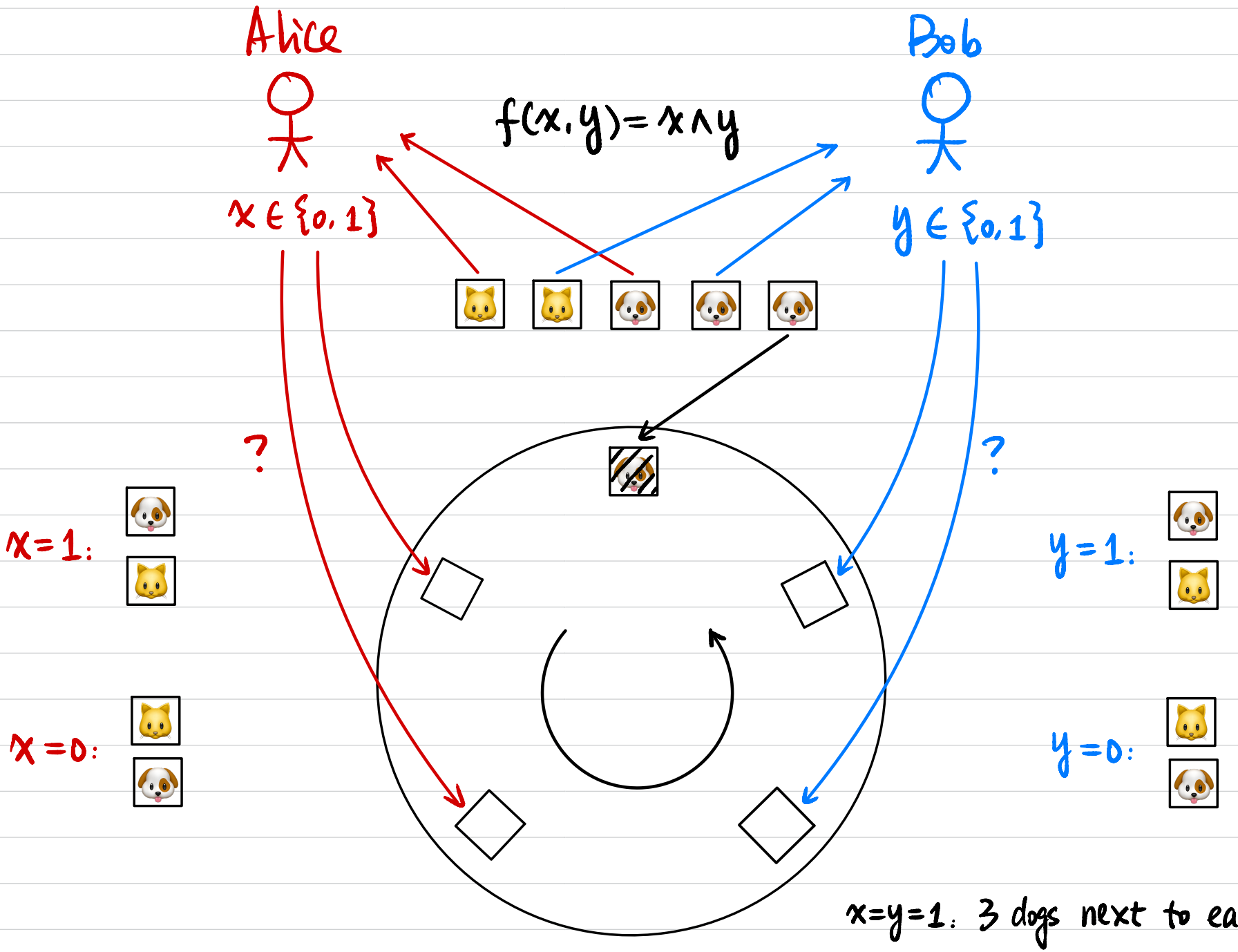
$$f(x,y) = \begin{cases} 0 & \text{if } x < y \\ 1 & \text{Otherwise} \end{cases}$$

Mutual friends?

X Y

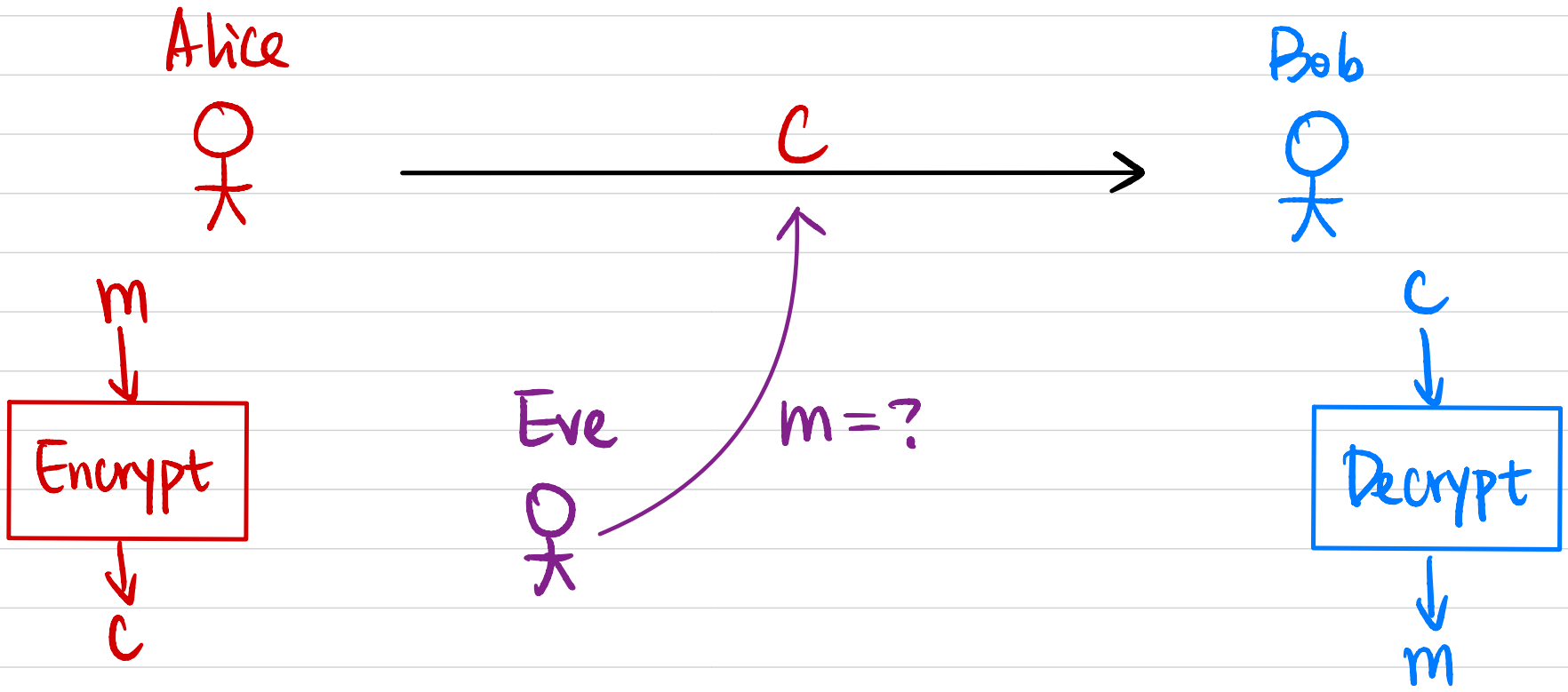
$$f(X,Y) = X \cap Y$$

Example: Private Dating



$x=y=1$: 3 dogs next to each other

Project 5: Fully Homomorphic Encryption



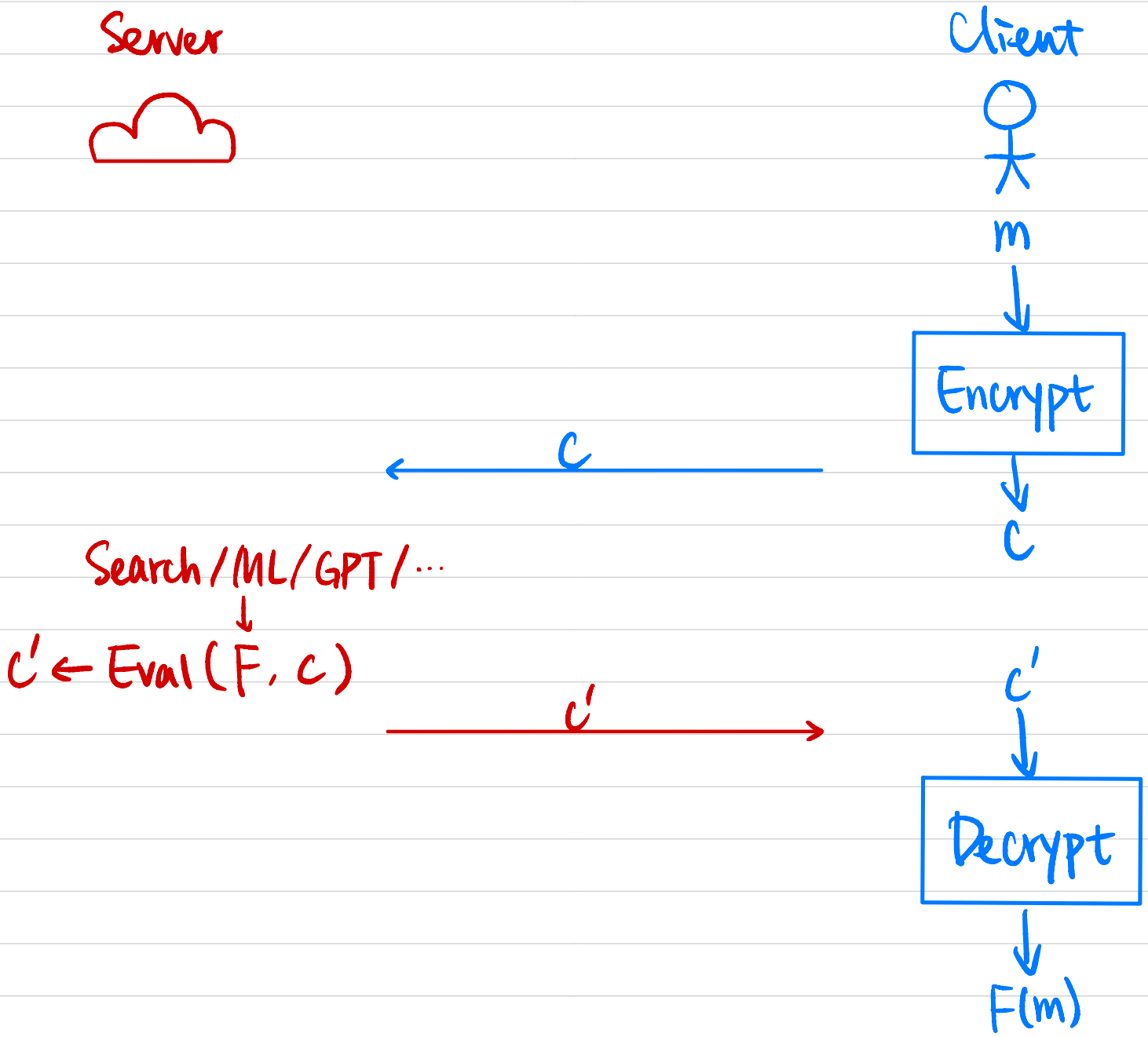
$$c_1 = Enc(m_1)$$

$$c_2 = Enc(m_2)$$

$$\Rightarrow \quad c' = Enc(m_1 + m_2)$$

$$c'' = Enc(m_1 \cdot m_2)$$

Example: Privacy-Preserving Query



Q & A

- Crypto background?
- Readings before/after lecture?
- Why C++?
- Class Participation
- Online session: only available to cybersecurity master's
- 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?
- This course won't be offered in Spring'27