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.

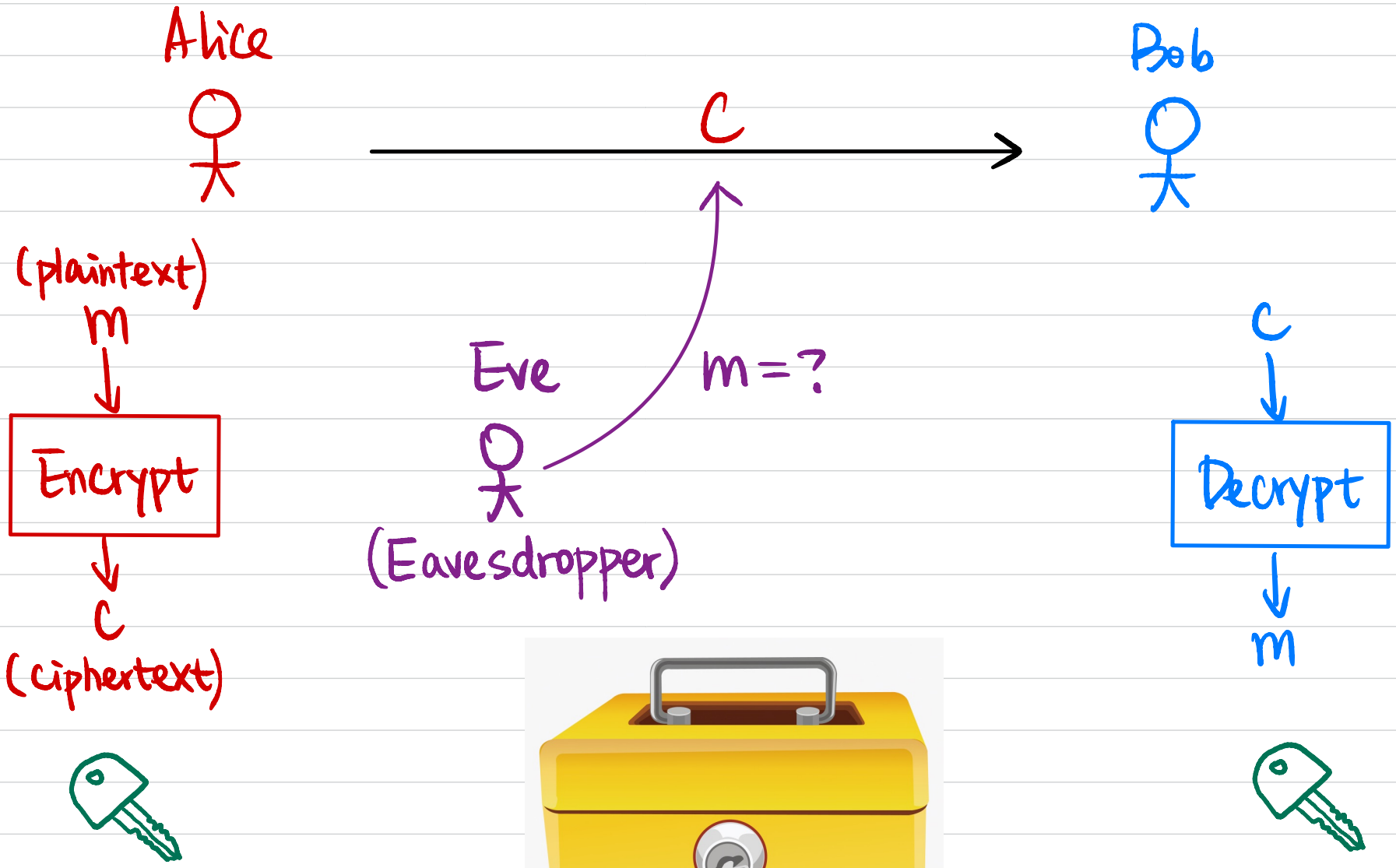
Where is cryptography used in practice?

What guarantees do we want in these scenarios?

Secure Communication

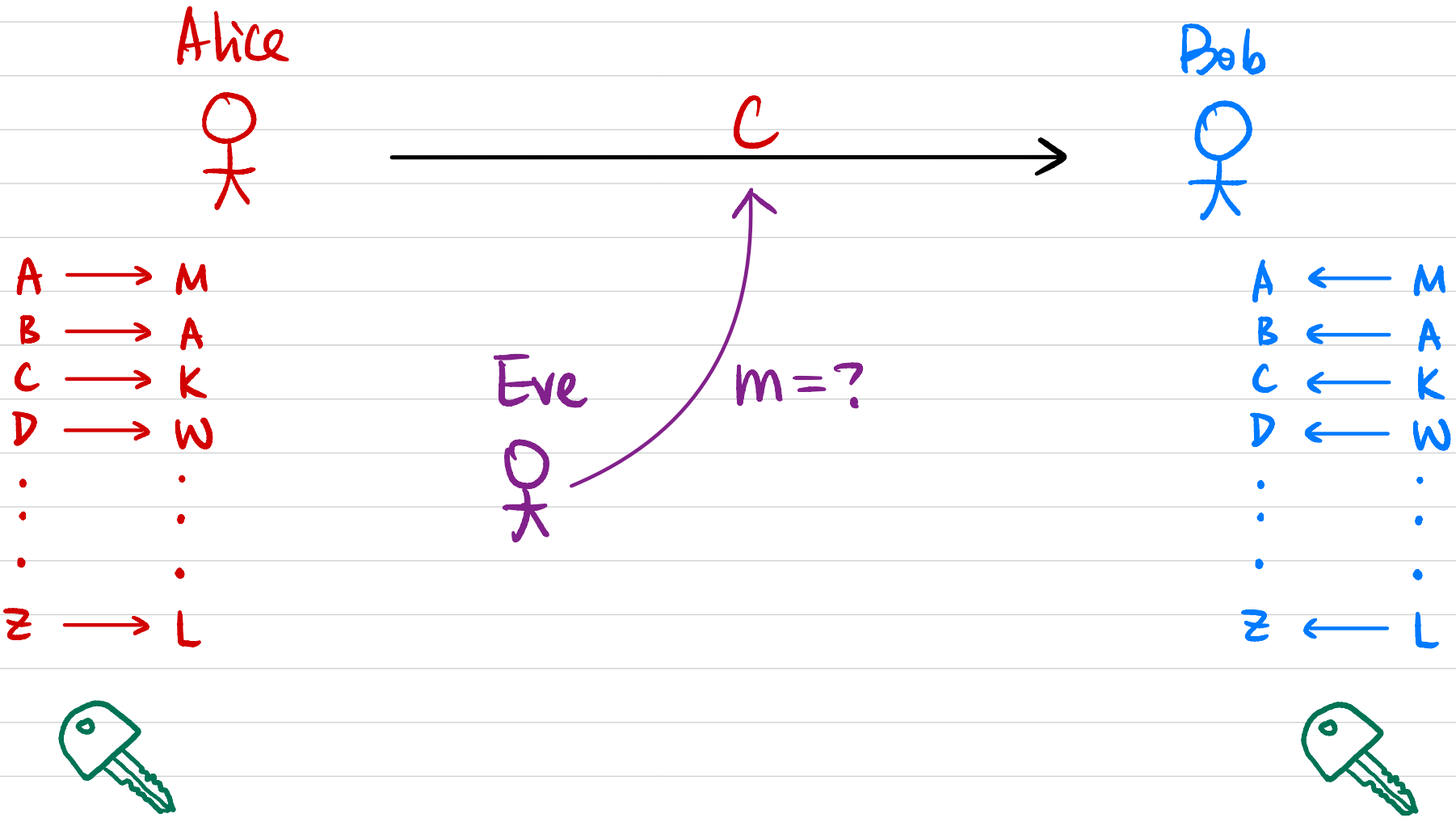
What security guarantee(s) do we want?

Message Secrecy

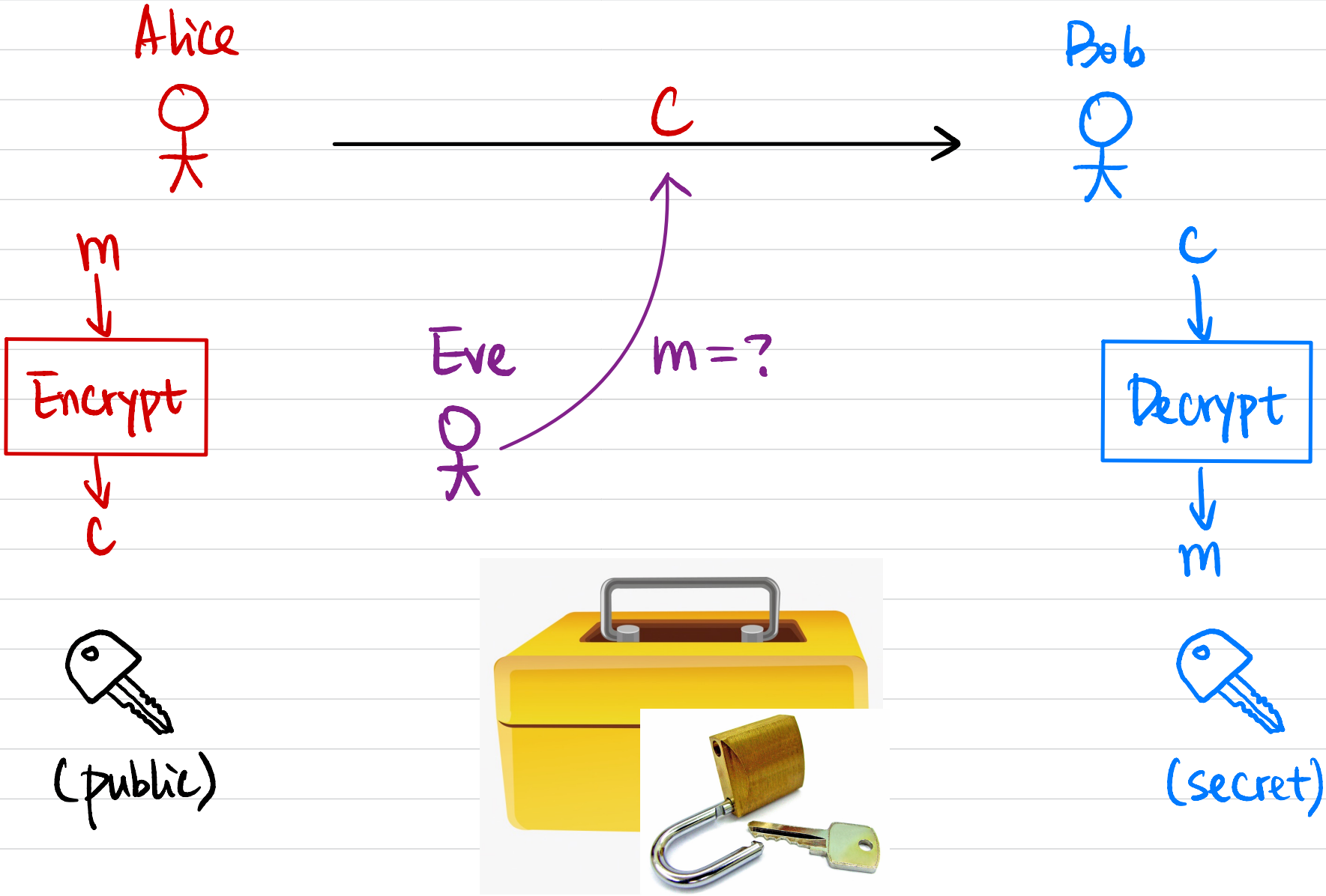


Historical Ciphers

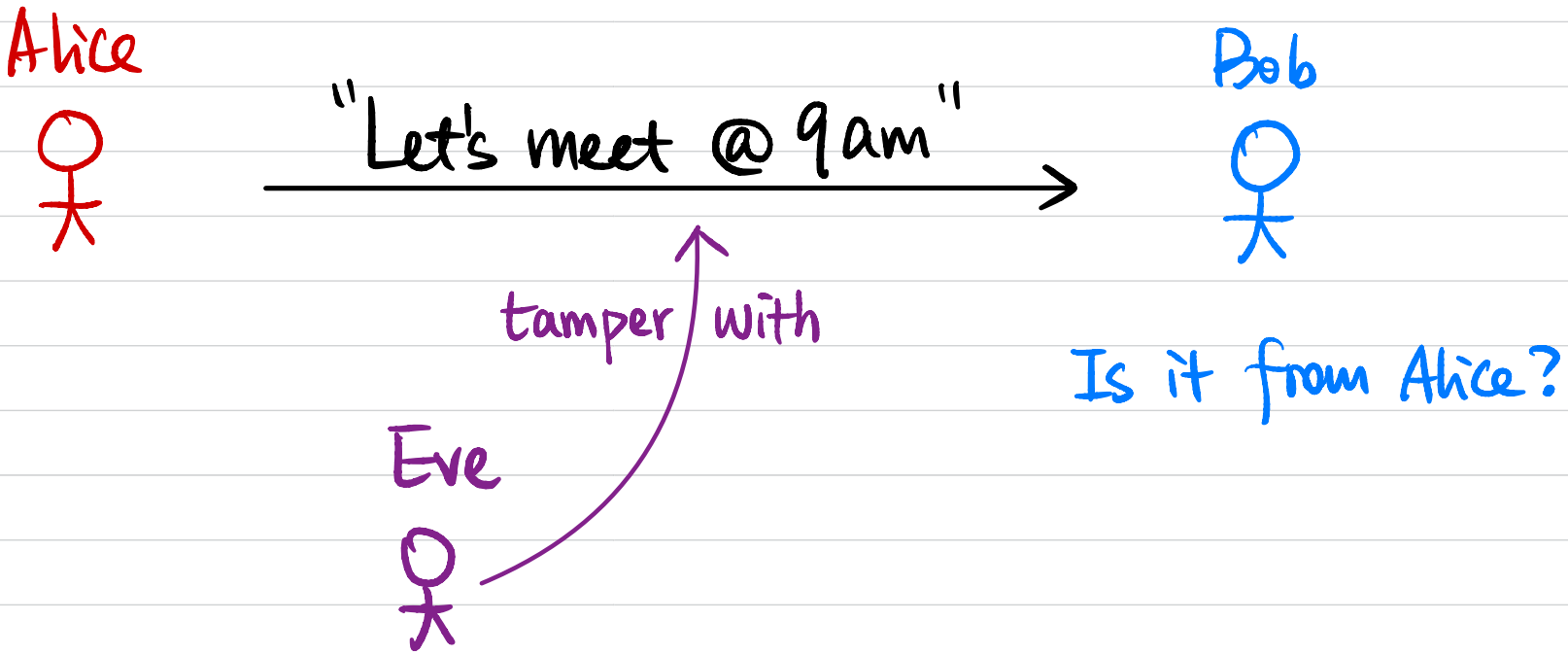
Ex: Substitution Cipher



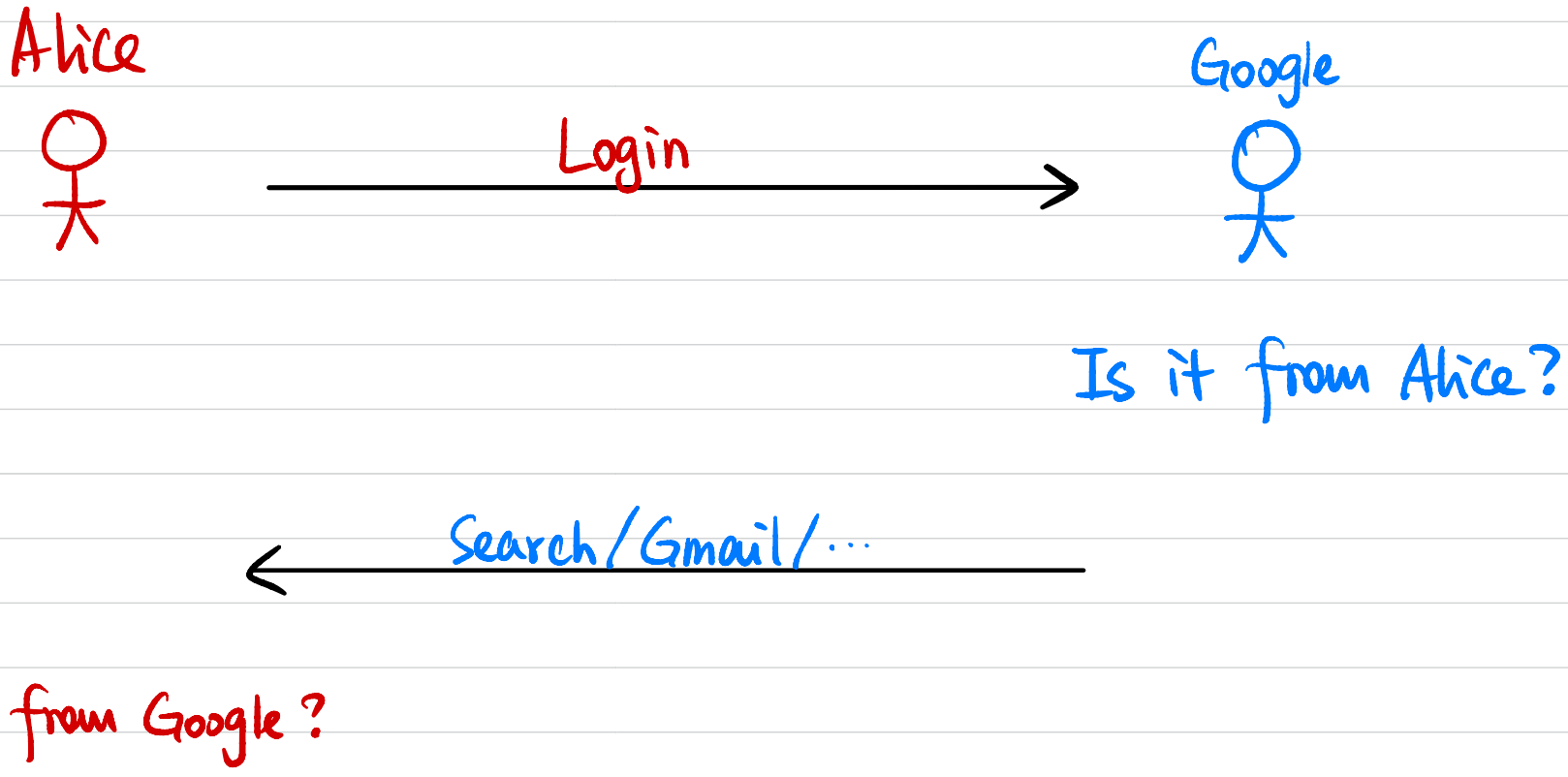
Public-Key Encryption



Message Integrity



Secure Authentication



Projects Overview

Project 0 (warm-up): Basic Schemes

Project 1: Secure Communication

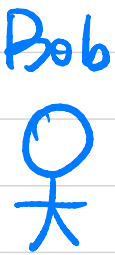
Project 2: Secure Authentication

Project 3: Zero-Knowledge Proofs

Project 4: Secure Multi-Party Computation

Project 5: Fully Homomorphic Encryption
(Post-Quantum Cryptography)

Project 3: Zero-Knowledge Proofs



Coca-Cola & Pepsi taste differently

There is a bug in your code

I have the secret key for this ciphertext

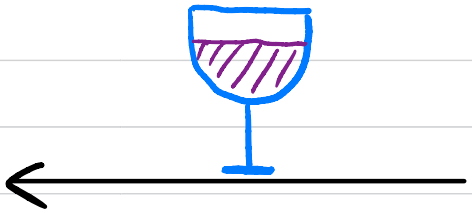
Ex: Coca-Cola & Pepsi

Alice

Bob

[Coca-Cola & Pepsi taste differently]

$b \xleftarrow{\$} \{0,1\}$



$b=0$, Coca-Cola

$b=1$, Pepsi

b'

If statement is true:

If statement is false:

Project 4: Secure Multi-Party Computation

Alice

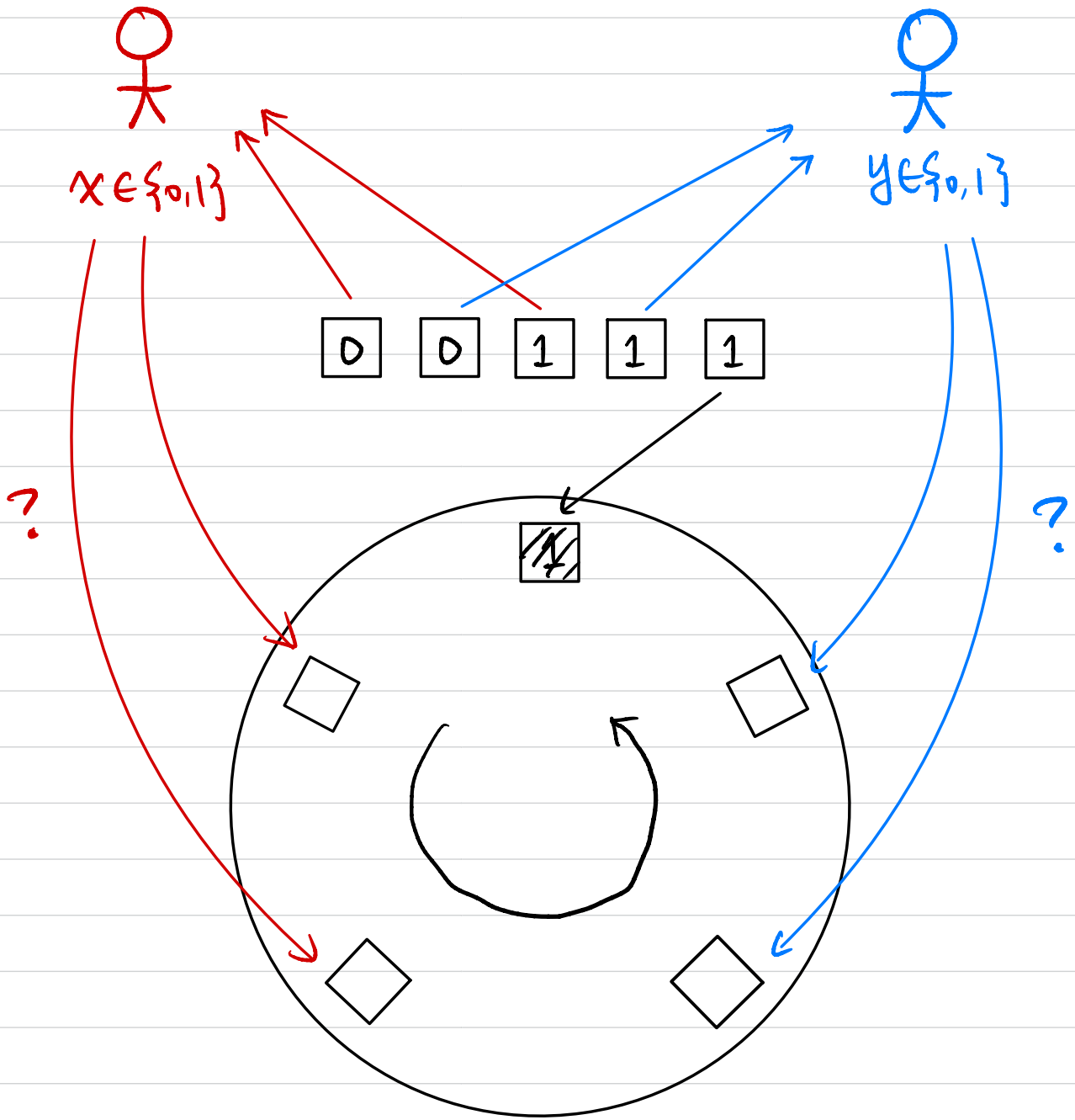
Bob

Second date?

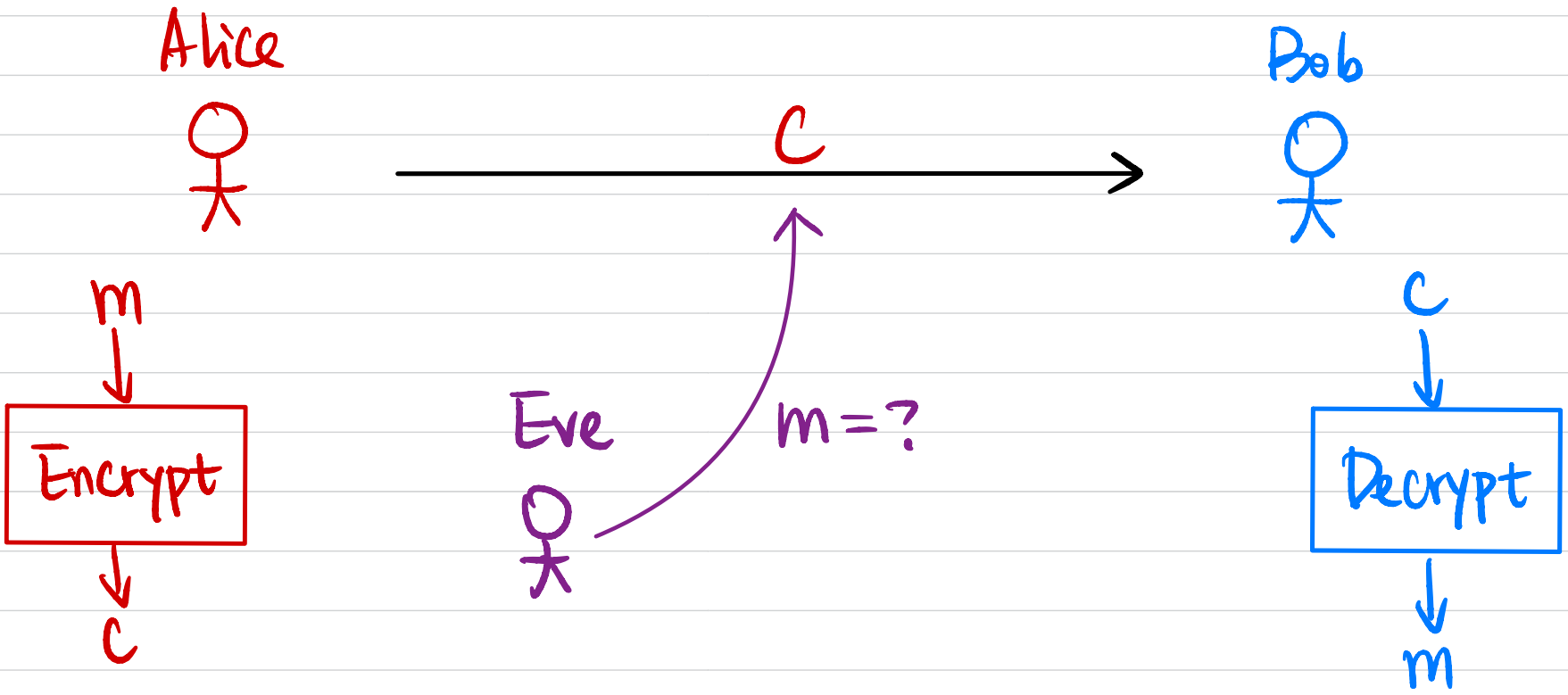
Who is richer?

Common friends?

Ex: Private Dating



Project 5: Fully Homomorphic Encryption

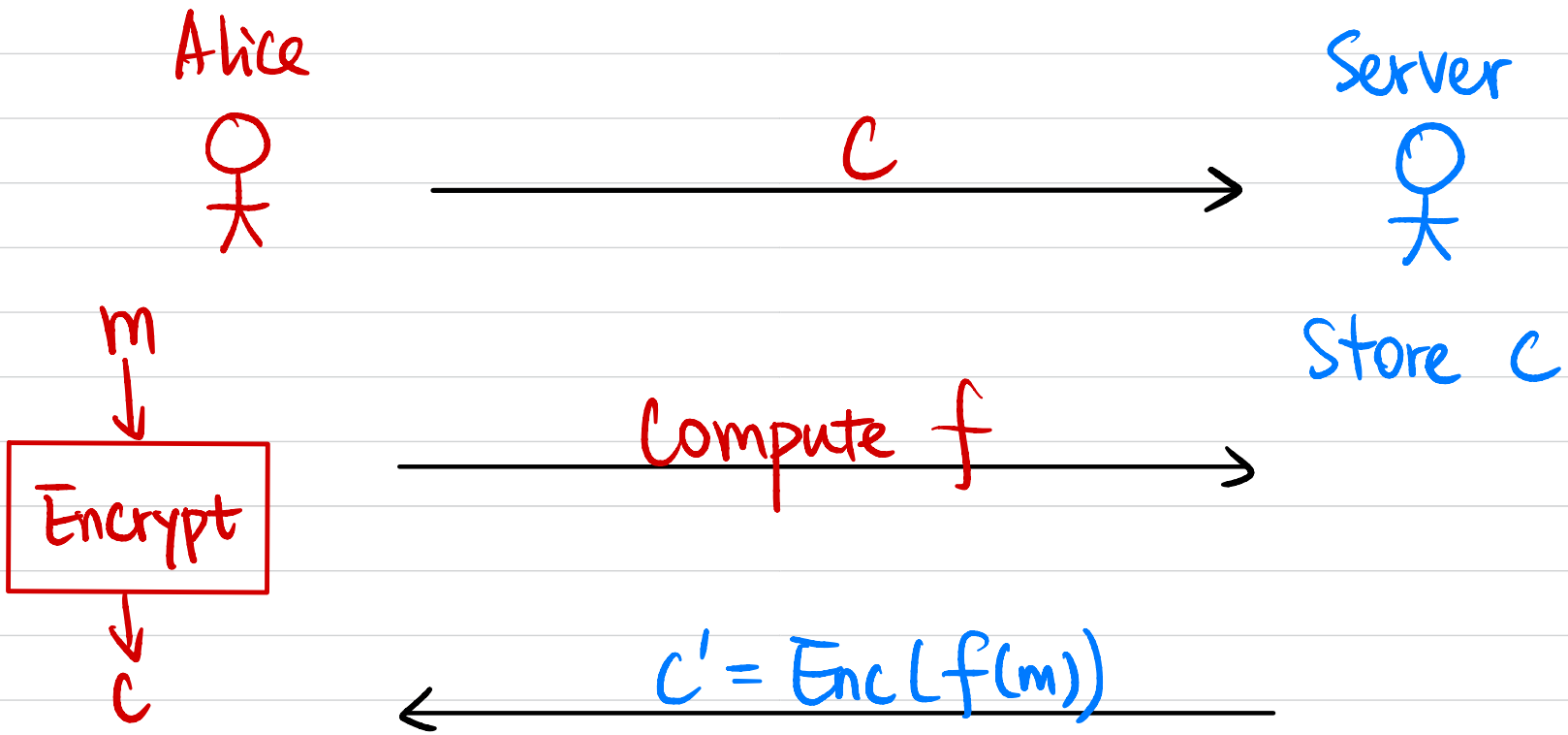


$$c_1 = Enc(m_1)$$

$$c_2 = Enc(m_2)$$

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

Ex: Outsourced Computation



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 gcd(a,b)
- (Extended) Euclidean Algorithm
- Groups
- One-Time Pad
- RSA encryption / signature
- Diffie-Hellman key exchange
- SHA (hash functions)