CSCI 1510

Introduction to Cryptography and Security

Course Homepage: https://cs.brown.edu/courses/csci1510/

- Introduce Staff
- Syllabus
- Introduction & Overview

Logistics

- **Lectures:** CIT 101 & Zoom (recorded)
- **Office Hour:** 12–1pm Thursdays, CIT 511 & Zoom,
  or by appointment
- **TA OH:** See course website (calendar)
- **EdStem** / **Gradescope** / **Course Website**
- **Prerequisites / Override:**
  CSCI 0220 & 1010
  Basic algorithms, number theory, discrete probability, complexity theory.

Textbooks

- "Introduction to Modern Cryptography" by Katz & Lindell
- "A Graduate Course in Applied Cryptography" by Boneh & Shoup

Class Participation

- Ask / Answer ≥ 5 technical questions throughout the semester, from 5 different lectures.

- Bonus Points: (cap 5 points)

  If you ask a "good" question or give a "good" answer.

- Keep track of all the questions you've asked / answered & bonus points you've earned (see template)

  Submit at the end of the semester.

Homeworks

- Homework 0 + 10
- Due on Fridays, 2 late days for free
- No further extension
- Lowest HW grade will be dropped.

- Collaboration / Google / ChatGPT:
  - Write up your own solution
  - Acknowledge everyone you've worked with
  - Credit all resources you've looked at

Exams

- **Midterm:** Tue 10/24 (in-class)

  You may consult 6 single-sided sheets of notes.

- **Final:** 2-5pm, Wed 12/13

  You may consult 12 single-sided sheets of notes.

- In each HW, there will be a question for you to synthesize course materials from that week into a one-page summary.

Grading

- 10% Class Participation
- 2% HW 0
- 54% HW 1-10 (best 9 out of 10)
- 14% Midterm
- 20% Final

What is Cryptography?

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

Where is cryptography used in practice?

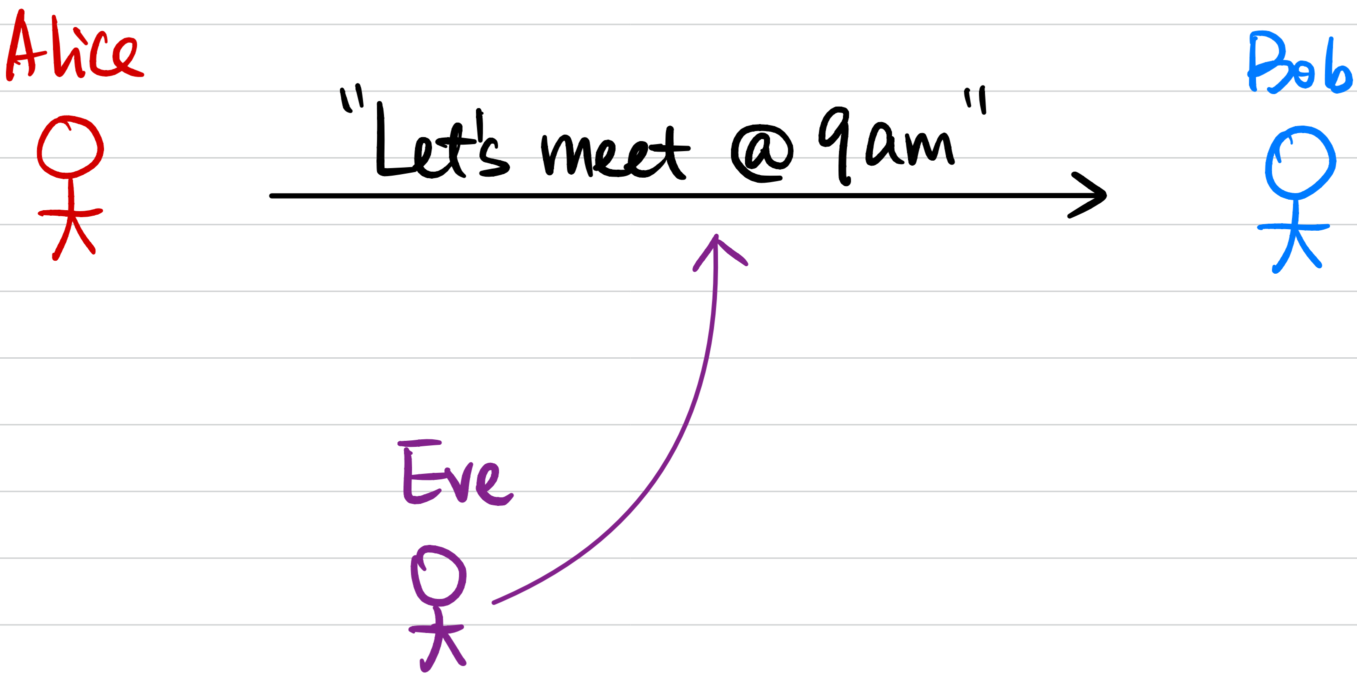
What guarantees do we want in these scenarios?

About the Course

Goal: Learn the theoretical basis of the cryptography in the real world.

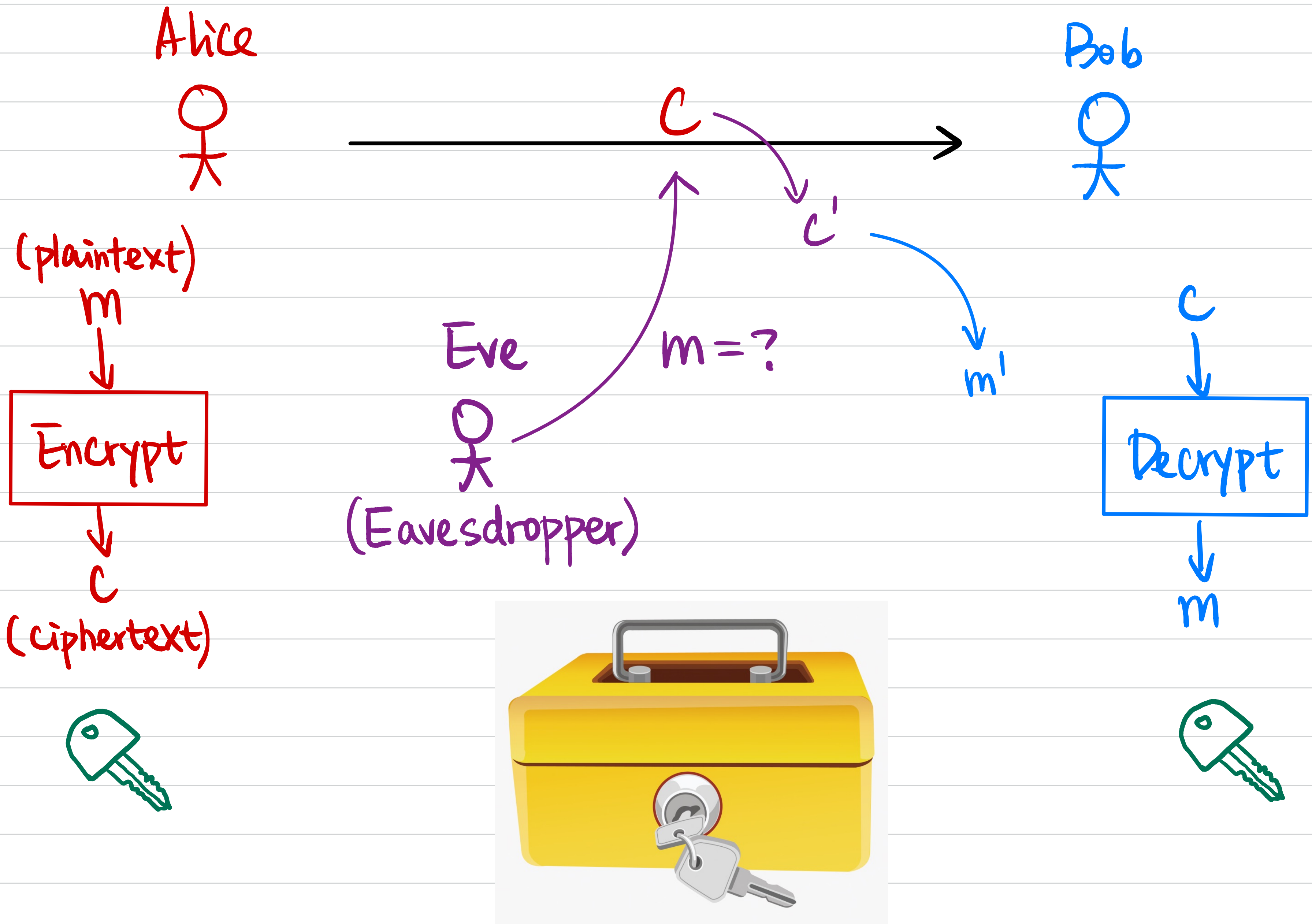
- Learn about key primitives
- Understand what security guarantees they provide
- Learn how to construct and how to prove
- Build up a "crypto mindset"

Secure Communication



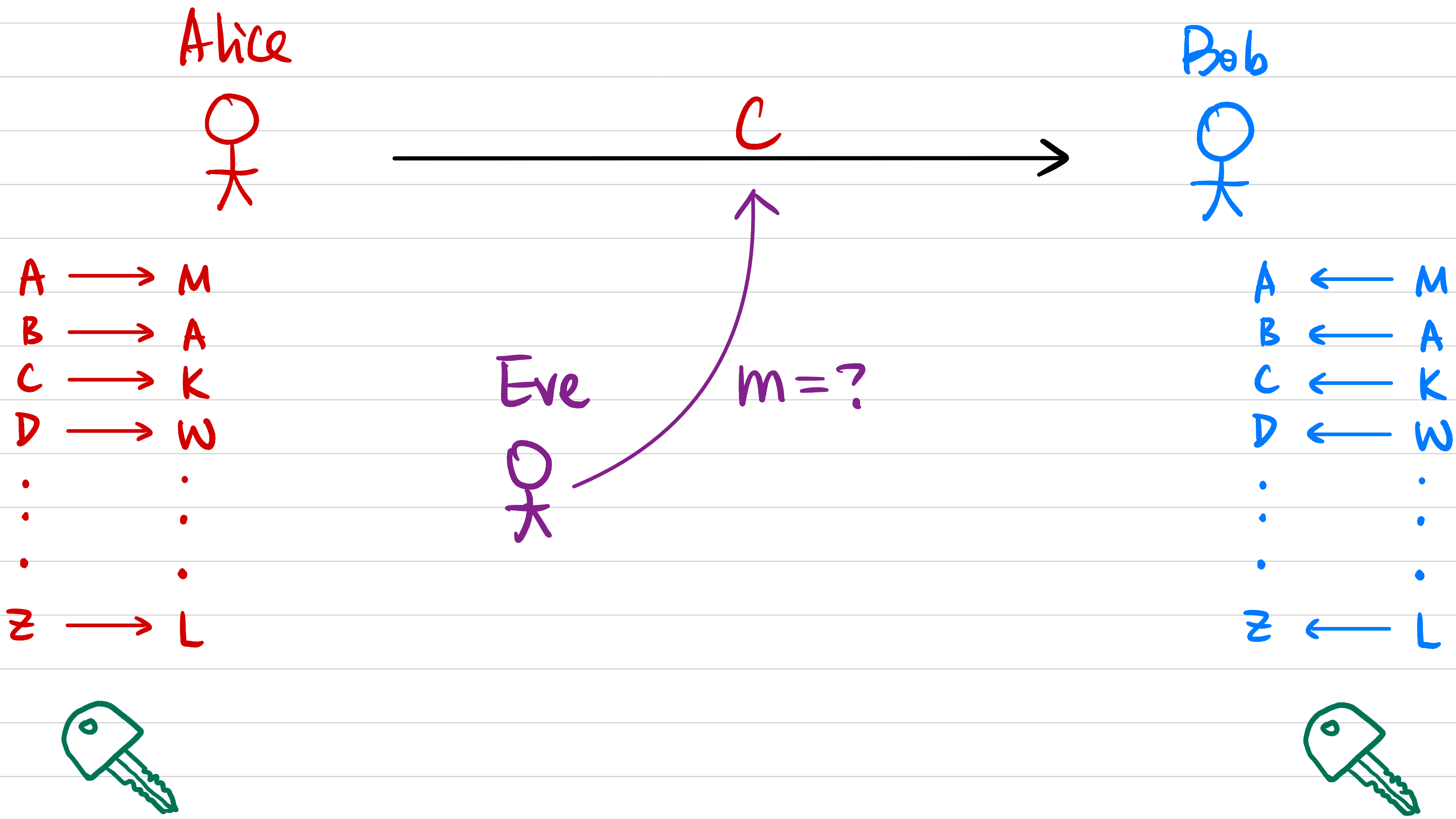
What security guarantee(s) do we want?

Message Secrecy

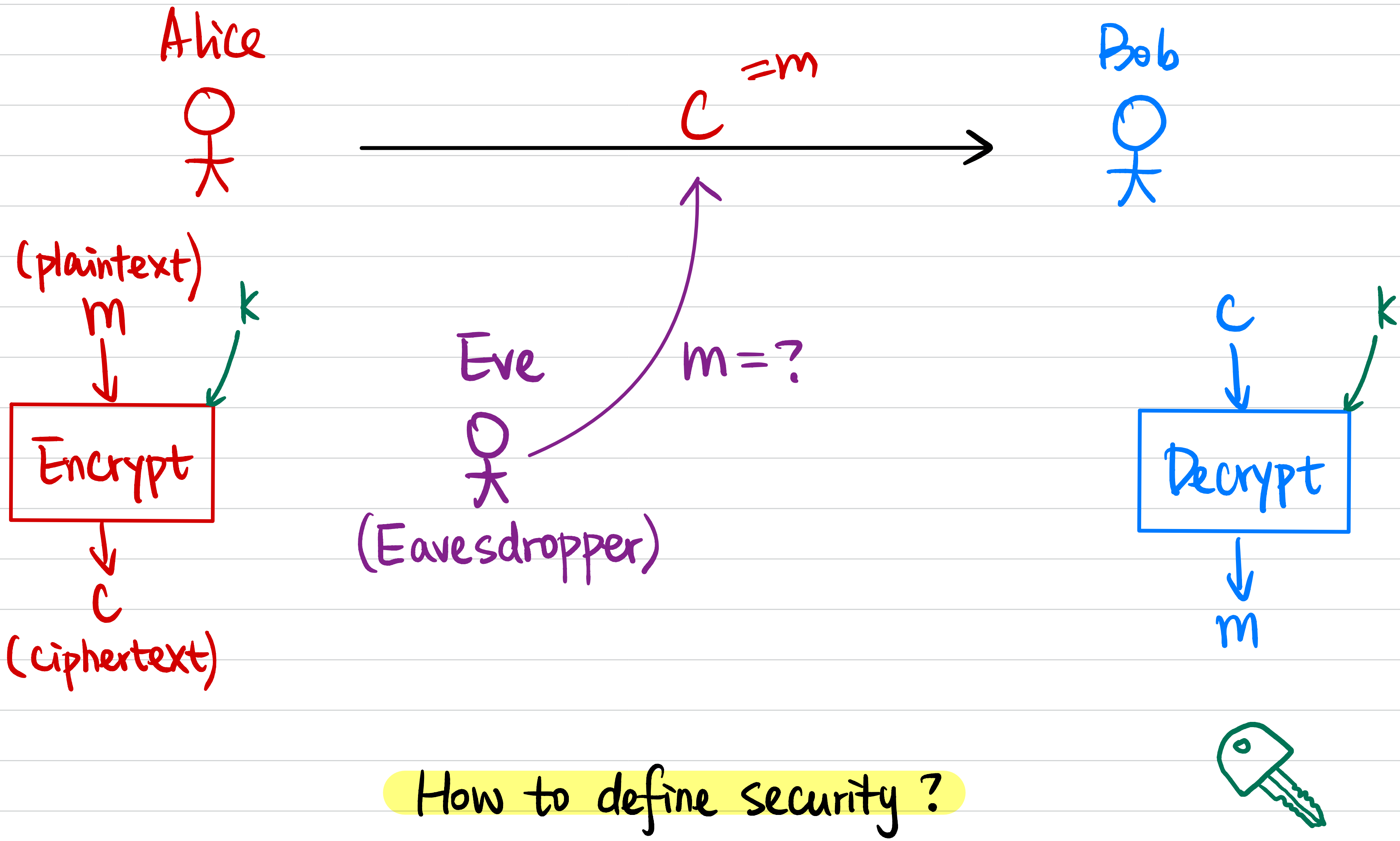


Historical Ciphers

Ex: Substitution Cipher



Modern Cryptography



How to define security ?

How to define security?

- It's impossible for Eve to recover k from c.

$$Enc_k(m) = m$$
$$\uparrow$$
$$c = m$$

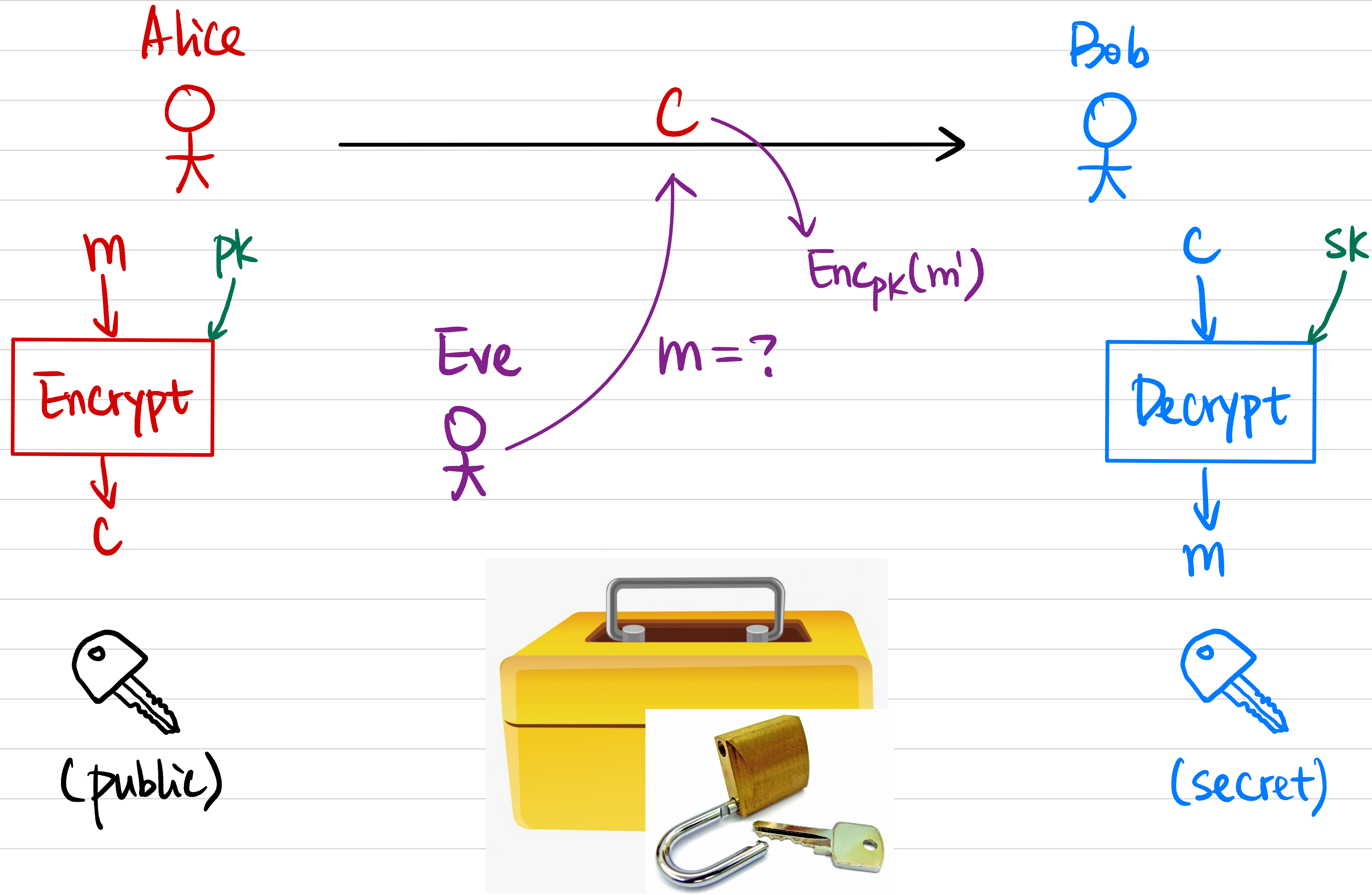
- It's impossible for Eve to recover m from c.

90% of m?

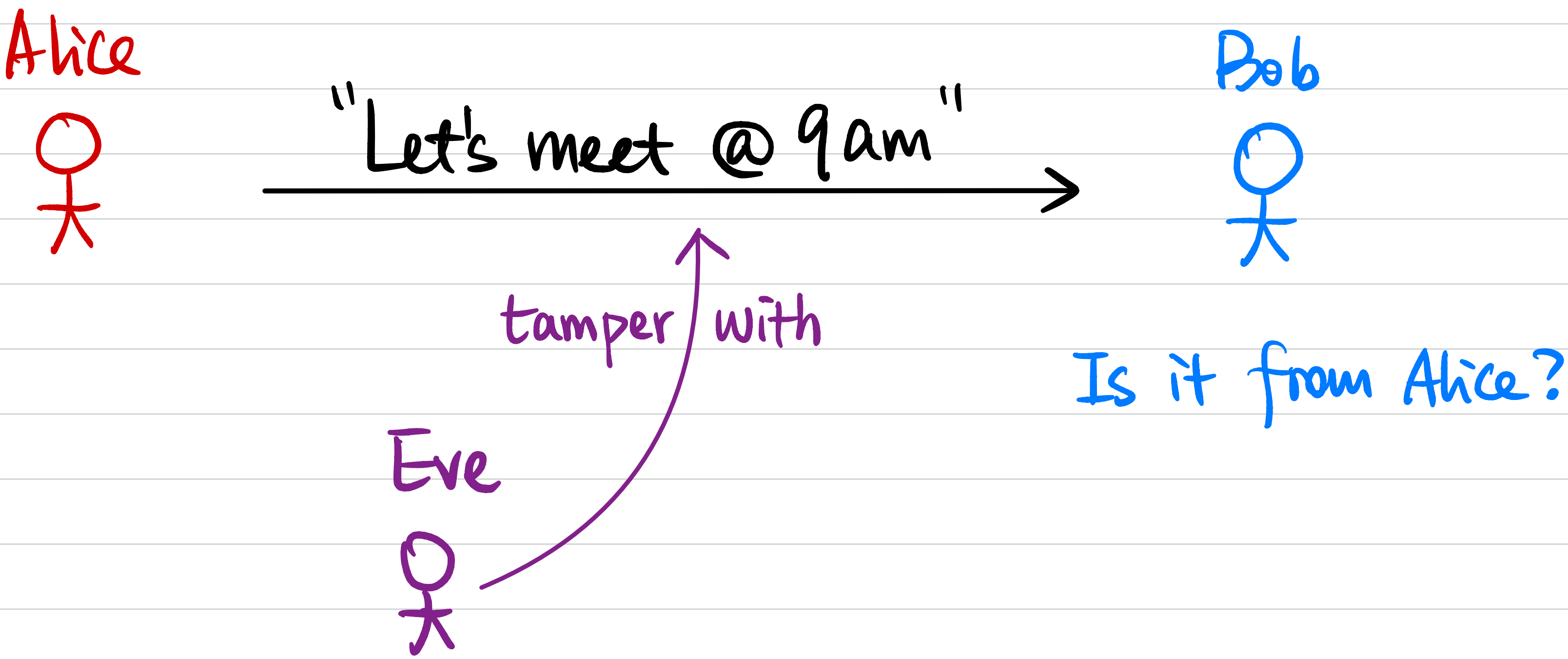
- It's impossible for Eve to recover any character of m from c.

distribution of m?

Public-Key Encryption



Message Integrity



Message Integrity

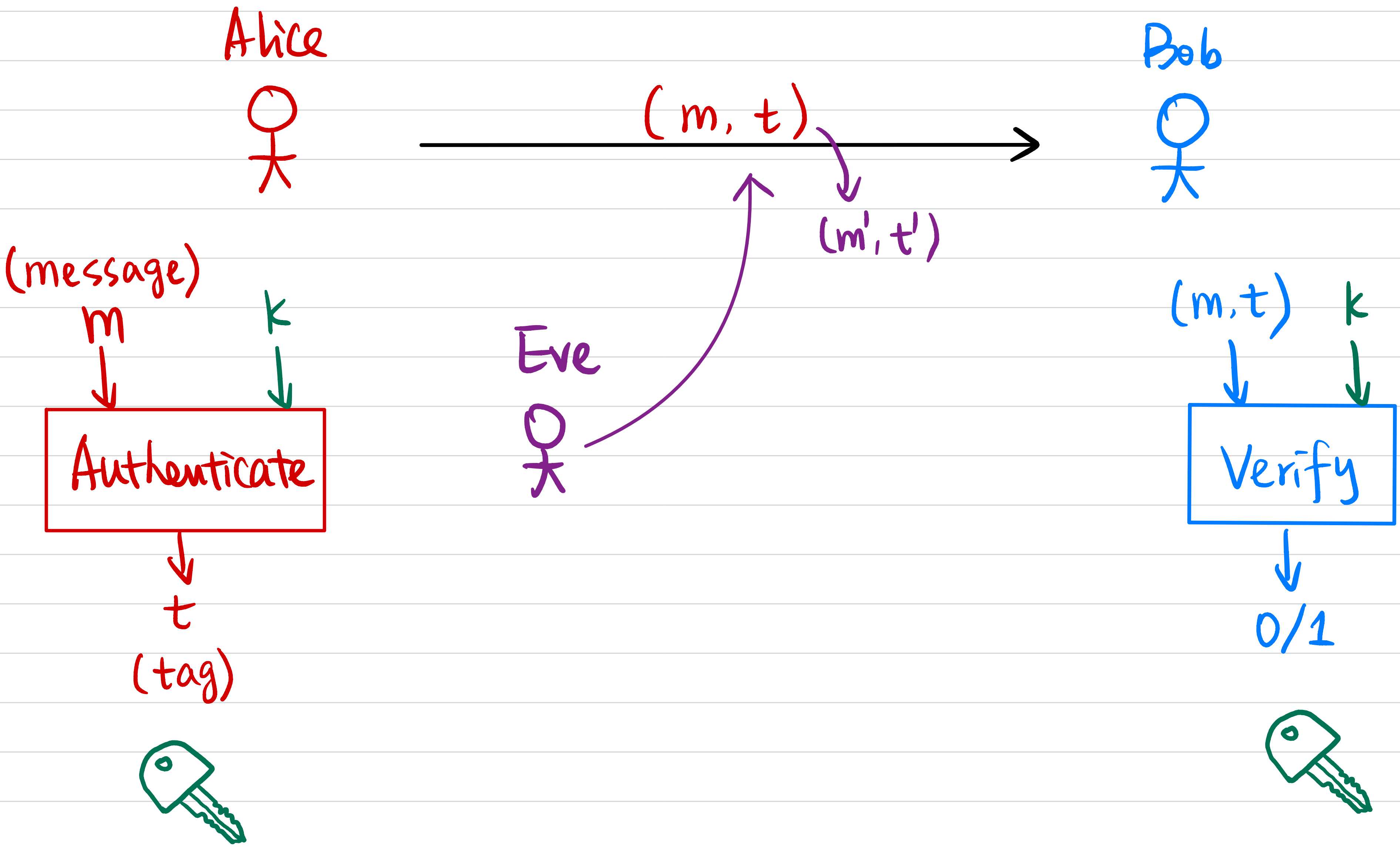
Is it from Google?

http vs. https

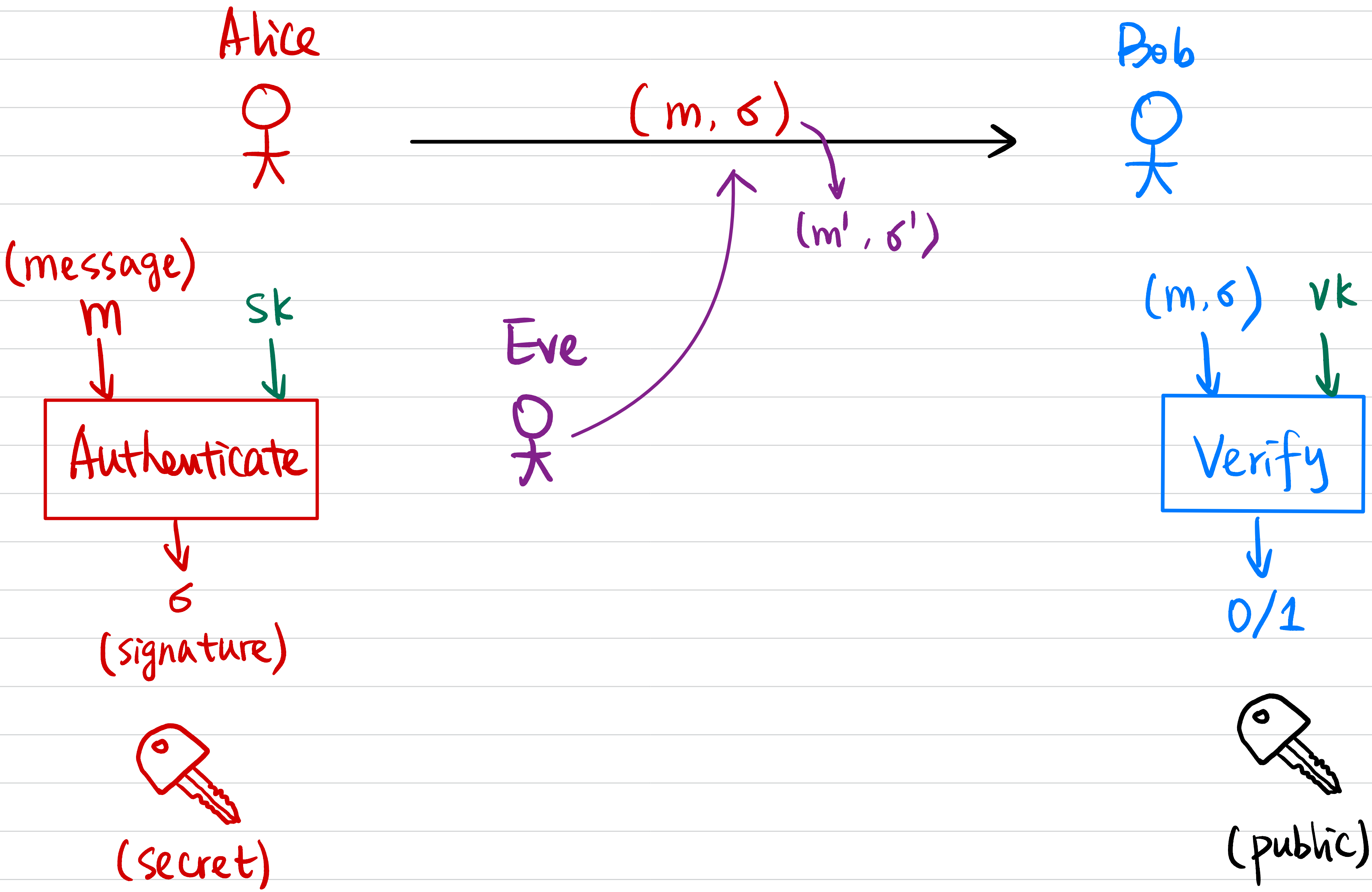
How to achieve message integrity?

Does encryption suffice?

Message Authentication Code (MAC)



Digital Signature



Pseudorandom Number Generator

Sample $r \leftarrow \{0, 1, 2, \cdots, 9\}$

$r := \text{rand}(\text{seed})$

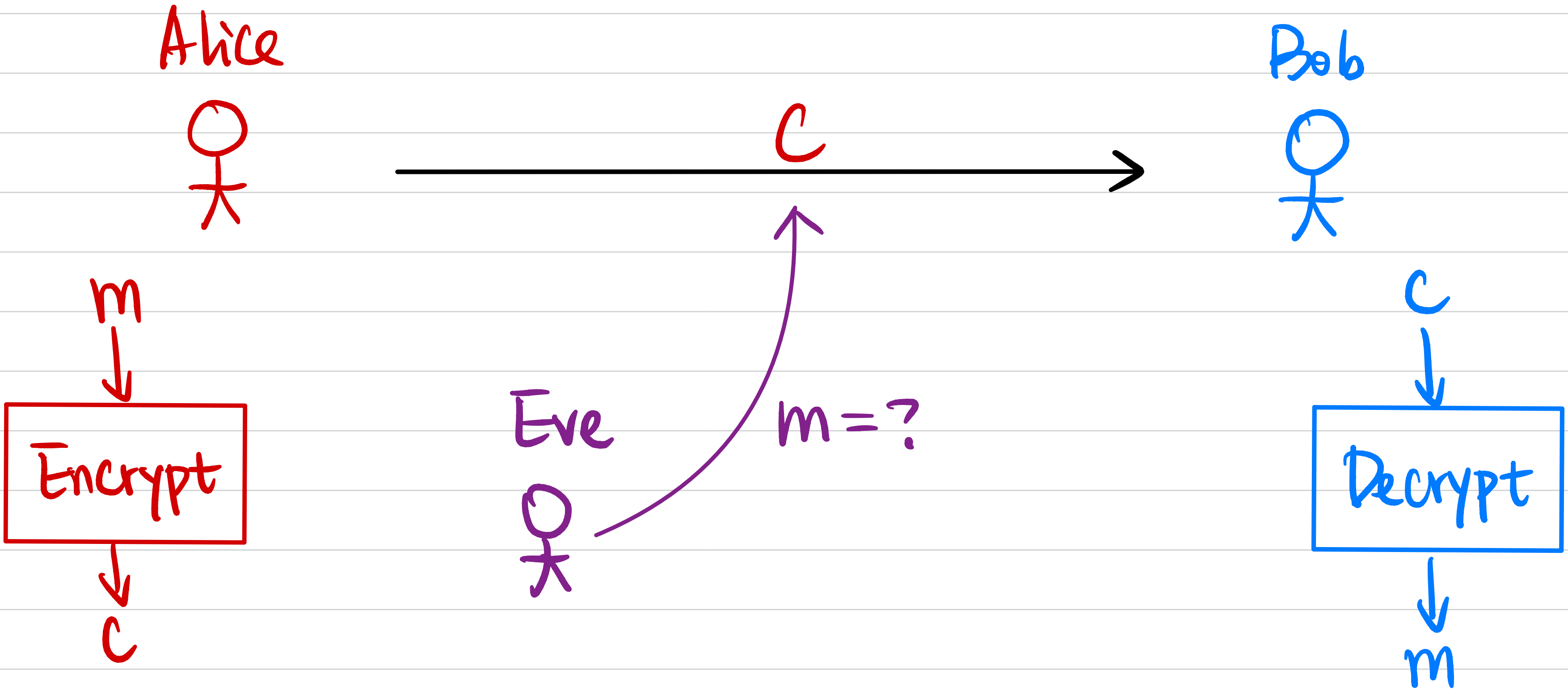
deterministic (→ rand)   timestamp (→ seed)

How to define "pseudorandomness"?

Overview

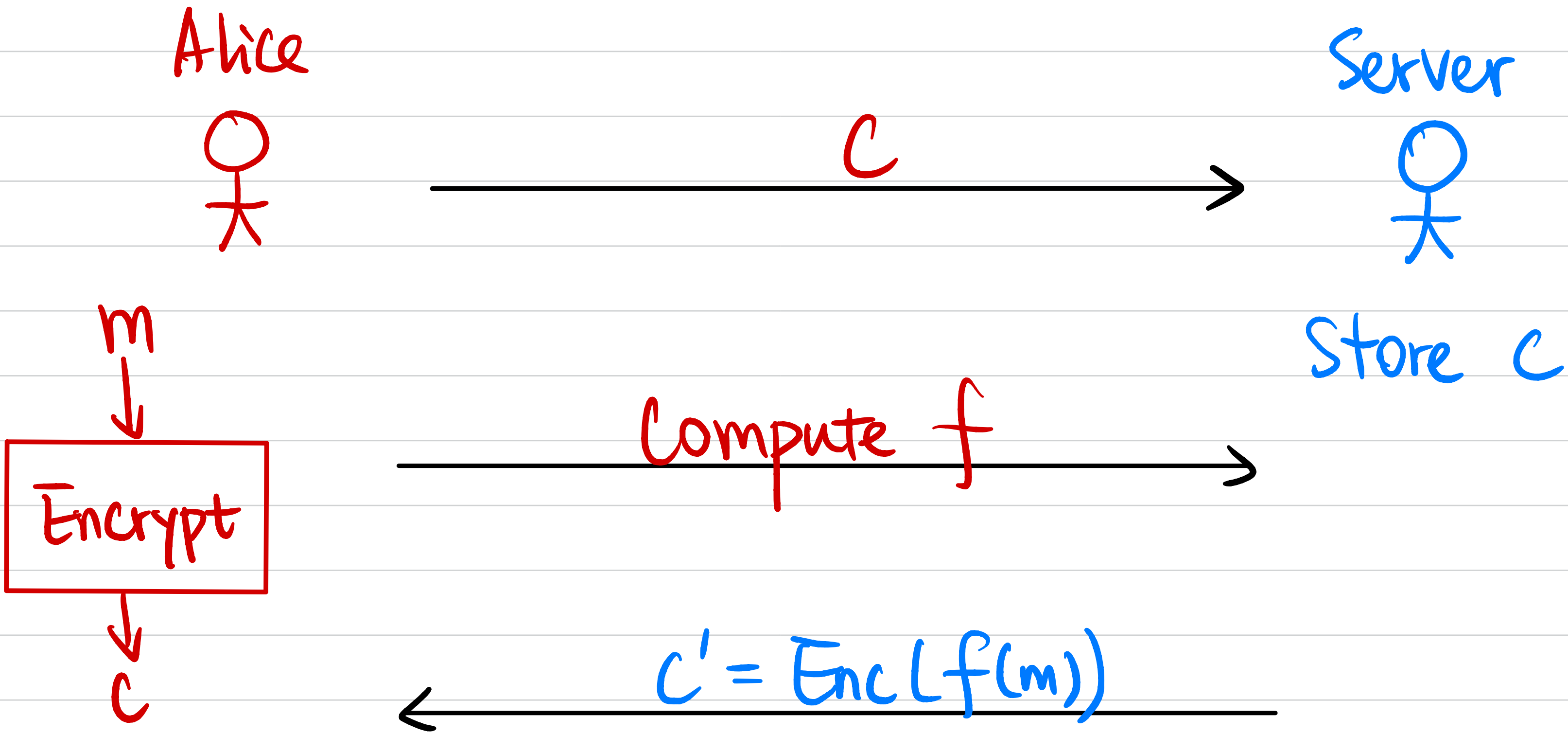
- Message Secrecy: symmetric-/public-key encryption
- Message Integrity:
  - Message Authentication Codes
  - Digital Signatures
- Key Primitives:
  - Pseudorandom Generator / Pseudorandom Function / Hash Function
  - Computational Assumptions: RSA / DLOG / Diffie-Hellman
- Encryption with Advanced Properties:
  - Fully Homomorphic Encryption (post-quantum security)
  - Identity-Based Encryption
- Secure Protocols:
  - Zero-Knowledge Proofs
  - Secure Multi-Party Computation
- Program Obfuscation

Fully Homomorphic Encryption (FHE)

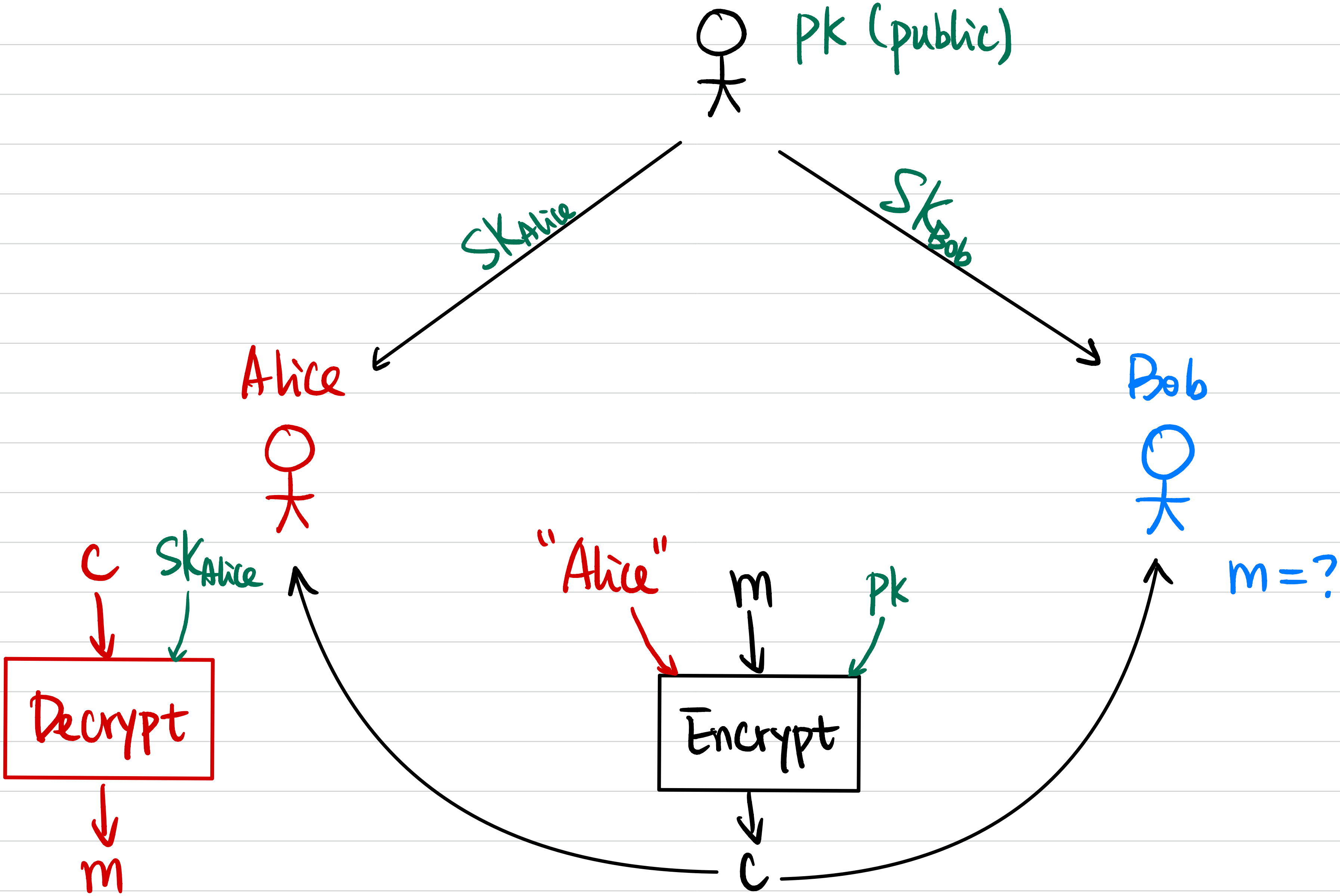


$$c_1 = \mathrm{Enc}(m_1)$$
$$c_2 = \mathrm{Enc}(m_2)$$
$$\Rightarrow \quad c' = \mathrm{Enc}(m_1 + m_2)$$
$$c'' = \mathrm{Enc}(m_1 \cdot m_2)$$

Ex: Outsourced Computation



Identity-Based Encryption (IBE)



Zero-Knowledge Proof (ZKP)

Alice

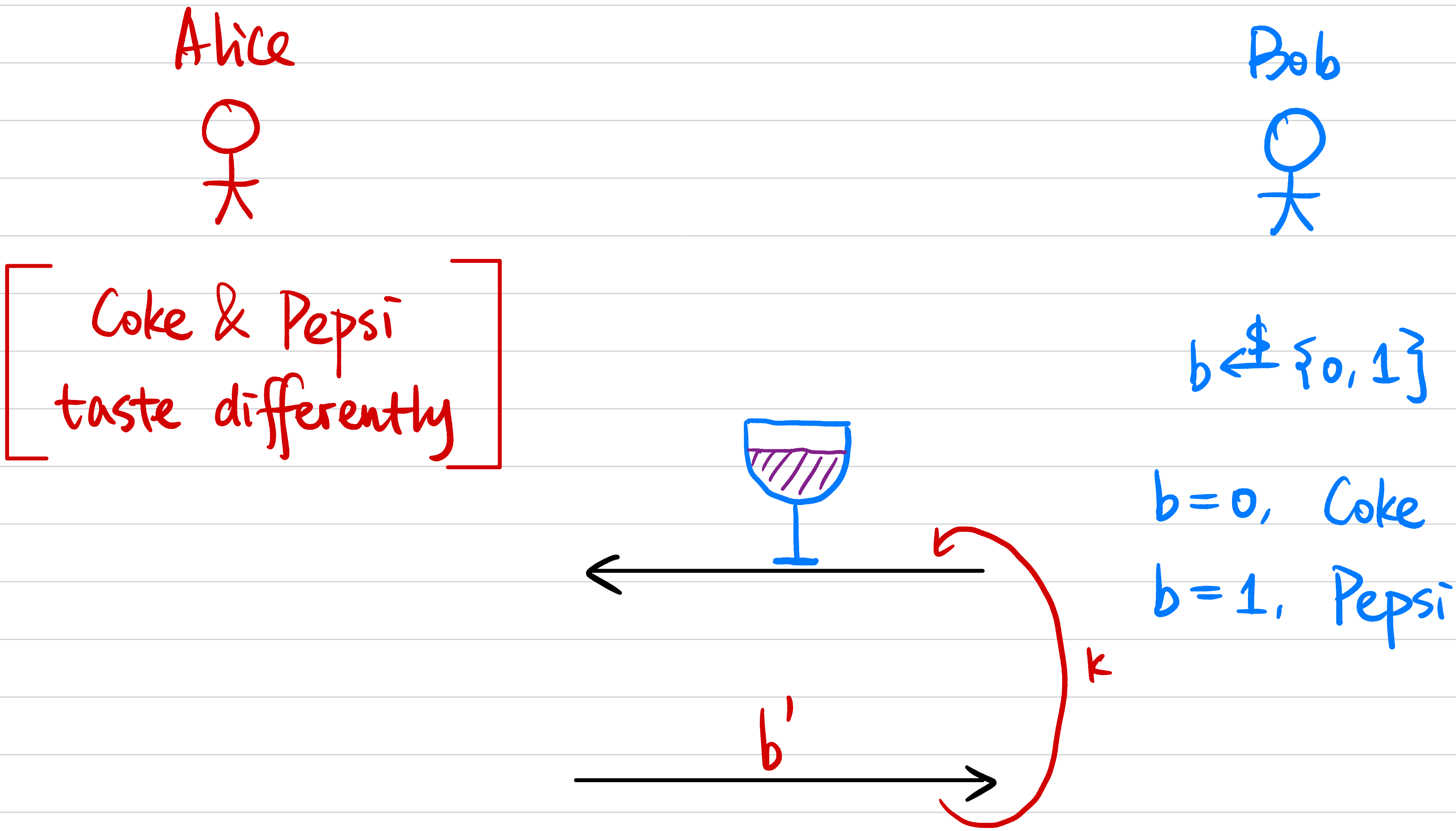
Bob

[Coke & Pepsi taste differently]

[There is a bug in your code]

[I have the secret key for this ciphertext]

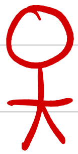
Ex: Coke & Pepsi

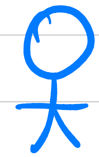


If statement is true: $\Pr[b=b'] = 1$

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

Secure Multi-Party Computation (MPC)

Alice 

Bob 

Second date?

$x \in \{0,1\}$ $x \wedge y$ $y \in \{0,1\}$

Who is richer?

$x \in \mathbb{Z}$ $x > y$? $y \in \mathbb{Z}$

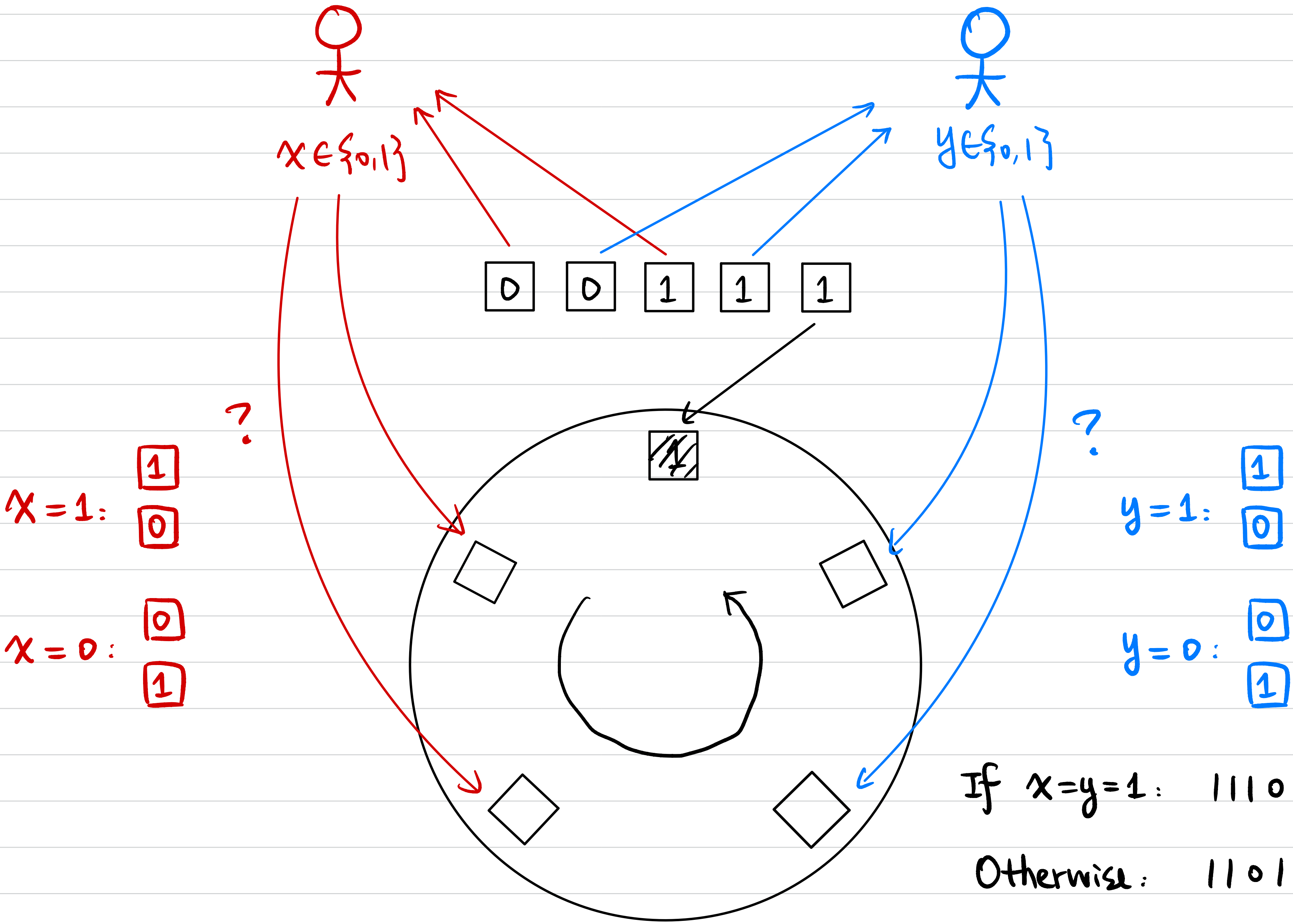
Common friends?

X $X \cap Y$? Y

Input: x Input: y

$f(x, y)$?

Ex: Private Dating



If $x=y=1$: 11100

Otherwise: 11010

Program Obfuscation