(Advanced) Computer Security!

Cryptography

Intro to Cryptography

(part I)

Prof. Travis Peters

Montana State University

CS 476/594 – Computer Security

Spring 2021

https://www.traviswpeters.com/cs476

Today

Reminder!
Please update your Slack, GitHub, Zoom
(first/last name, professional photo/background)

- Announcements
  - Lab 05 due today
- Learning Objectives
  - Basics around crypto

Intro & Overview

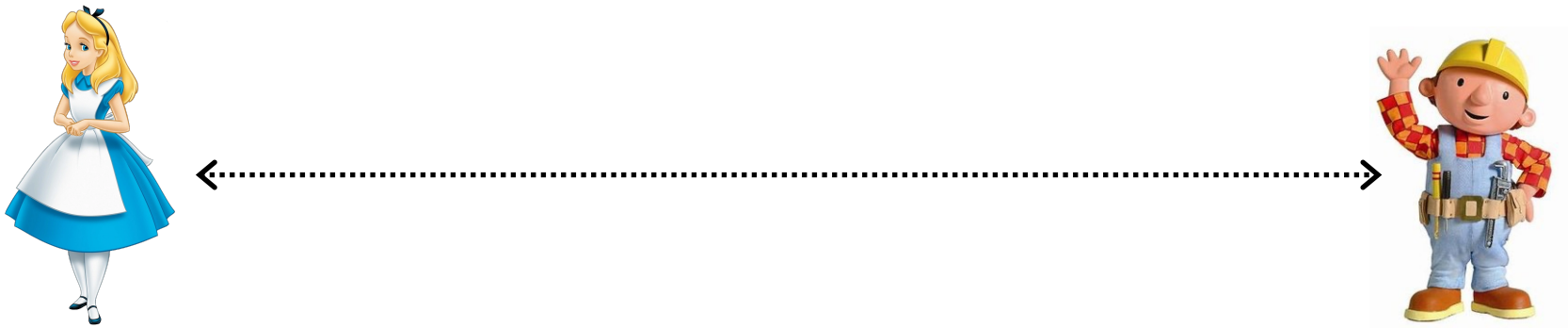
- **Information Security**
  - The protection of information and information systems (a.k.a. cybersecurity)
  - What security technologies to use? Procedures? Controls?

- **Cryptography**
  - Provides the mathematical techniques that underpins most information security tech

- **CAUTION!**
  - We study this topic for completeness…
  - NEVER ROLL YOUR OWN CRYPTO!

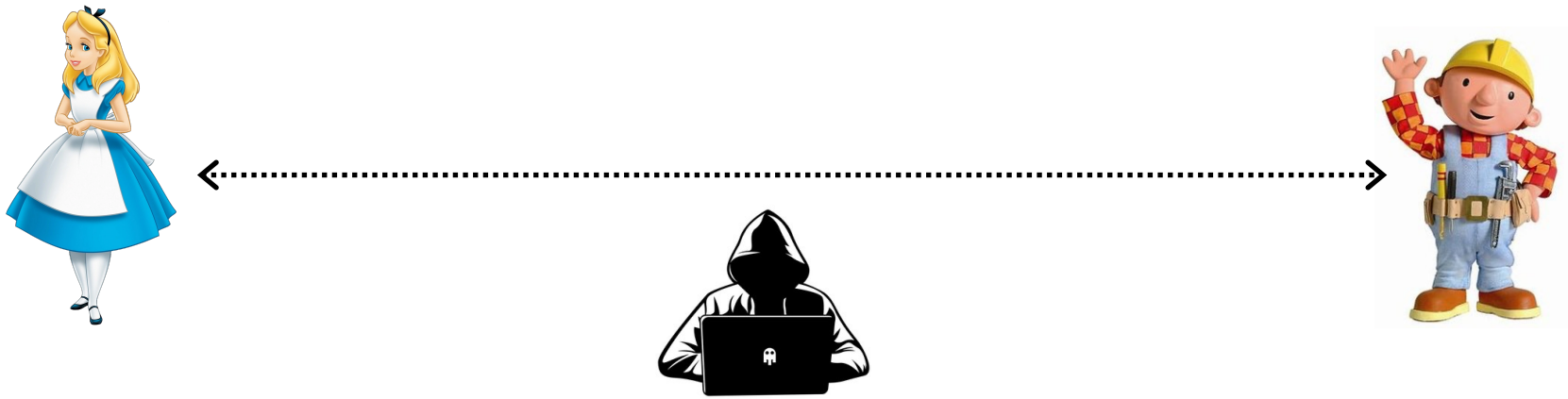
What is Cryptography?

Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries.



What is Cryptography?

Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries.



What is Cryptography?

Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries.

Goals: Confidentiality / Integrity / Authenticity

"Can only Bob see my message?"

"Is this message really from Alice?"

"How can I make sure my message will reach Bob without being changed?"

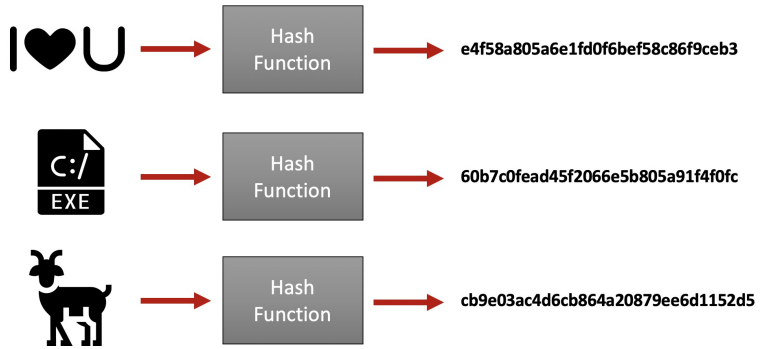
"Is this the message Alice intended to send?"

"Is it possible that Alice can deny ever sending me this message in the future?"

Roadmap

- Secret-Key Encryption (a.k.a. Symmetric Key Encryption)

- Cryptographic Hash Functions (e.g., MD5, SHA-*)



- Public-Key Encryption (a.k.a. Asymmetric Key Encryption)