Modern Cryptography

Introduction to Basic Cryptography

Dr. Ryan Riley

جامعة قطر
QATAR UNIVERSITY

Modern Cryptography

- Modern cryptography is based heavily on mathematics
- The math is hard
- We won't cover the details in this class
  - If you want the details, *Wikipedia* is an excellent resource

- Today we'll just do a brief overview of the three main types

Three Types of Crypto

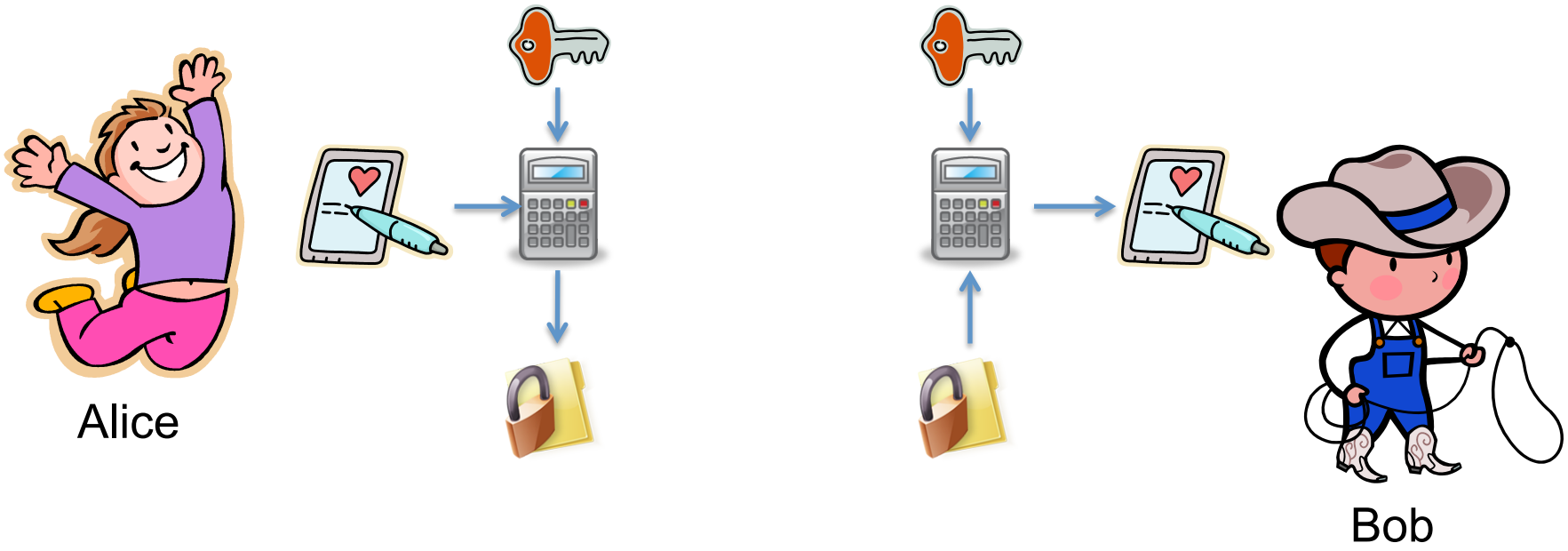
1. Secret Key Cryptography (Symmetric)
2. Public Key Cryptography (Asymmetric)
3. Message Digest (Hashing)

Remember…

- Most of our encryption techniques have:
  - An algorithm (What you do to the message)
  - A key (The secret that you need in order to encrypt/decrypt properly)

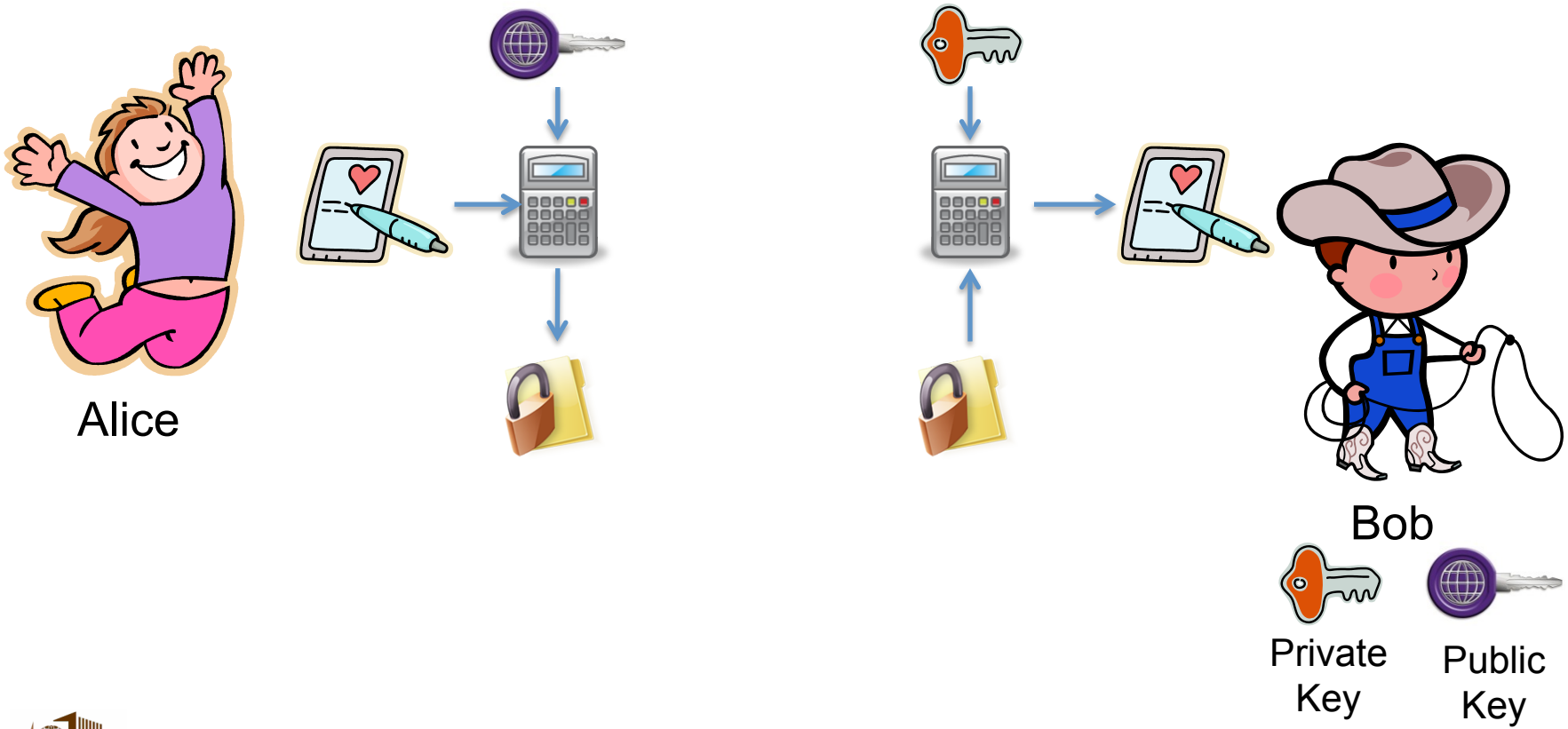
Secret Key / Symmetric Crypto

- A cryptographic technique where both parties in the communication share the same key



Public Key / Asymmetric Crypto

- A cryptographic technique where both parties in the communication use *different* keys



Message Digest / Hashing

- Transform any arbitrary message into a fixed length number
- Should be one-way
  - Message -> Hash is easy
  - Hash -> Message is hard
- Widely used in a lot of computing

Types of Cryptanalysis

- Ciphertext Only
  - Attacker only has ciphertext, needs to decrypt it
- Known Plaintext
  - Attacker knows some ciphertext and its corresponding plaintext, needs to decrypt some other ciphertext
- Chosen Plaintext
  - Attacker can get any plaintext he wants encrypted, needs to decrypt some specific ciphertext

Summing Up

- Three types of cryptography
  - Symmetric (Secret key)
  - Asymmetric (Public key)
  - Hashing (Digest)

- Three types of cryptanalysis
  - Ciphertext only
  - Known plaintext
  - Chosen plaintext