(Advanced) Computer Security!

Cryptography

Asymmetric Key Cryptography

Prof. Travis Peters

Montana State University

Computer Security

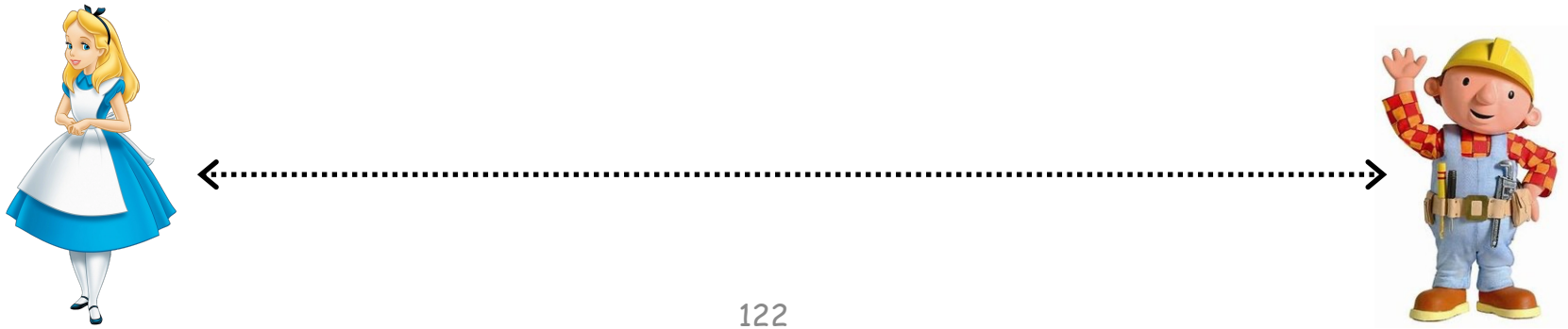
https://www.traviswpeters.com/cs476

Introduction to Asymmetric Key Cryptography

- Overview of Asymmetric Key (aka Public-Key) Cryptography
- Roadmap

Intro to Asymmetric Key Crypto

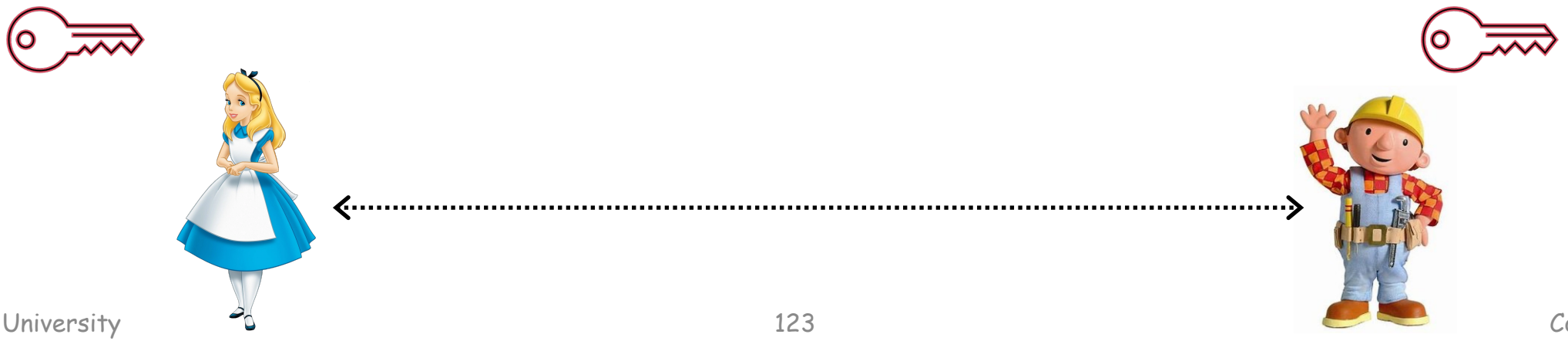
Asymmetric Key Cryptography is at the foundation of today's secure communication, which allows communicating parties to obtain a **shared secret key**



Intro to Asymmetric Key Crypto

In **symmetric key crypto**, the **same key** was used for both encryption and decryption

Q: How do parties get the key?

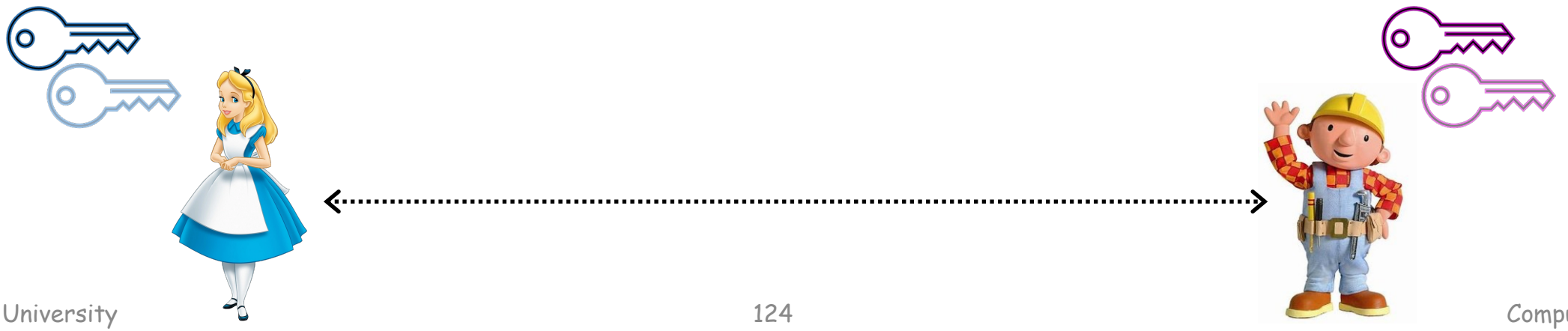


Intro to Asymmetric Key Crypto

In **public key crypto**, **different keys** are used for encryption and decryption

Public key (for **encryption**) and Private key (for **decryption**)

Private key (to create **digital signature**) and Public key (to **verify signature**)



A Brief History Lesson

- Historically same key was used for encryption and decryption
- **Challenge:** exchanging the secret key (e.g., face-to-face meeting)

- 1976: Whitfield Diffie and Martin Hellman
  - DH key exchange protocol
  - Proposed a new public-key cryptosystem

- 1978: Ron Rivest, Adi Shamir, and Leonard Adleman (all from MIT)
  - Attempted to develop a public-key cryptosystem
  - Created RSA algorithm

Roadmap -> Where do we go next?

- Public-key algorithms
  - Diffie-Hellman key exchange
  - RSA algorithm
  - Digital signatures
- Public-key crypto & Python
- Applications
  - Authentication
  - HTTPS and TLS/SSL
  - Chip Technology Used in Credit Cards