# Cryptography

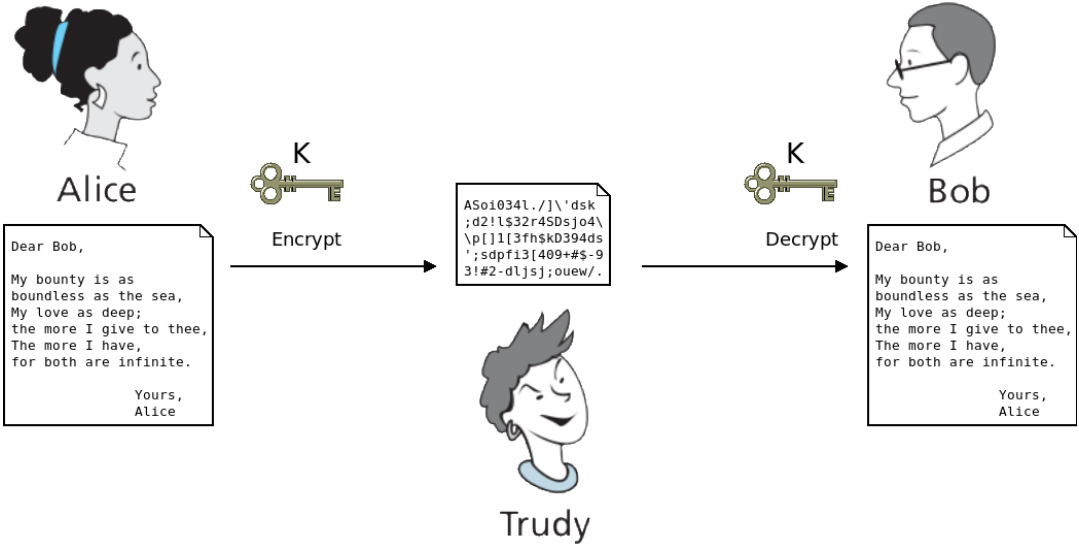
## Asymmetric Key Cryptography

Irfan Kanat

Department of Digitization
Copenhagen Business School

February 21, 2022

# Recap: Symmetric Key Cryptography



# The Problem with Symmetric Key Cryptography

For two thousand years cryptography required a shared key.

This is ok if you can meet and exchange keys.

Did you exchange keys with your bank?

# Big Idea: Securing Data in Transit

Alice and Bob want to communicate securely

- Confidentiality
- Integrity
- Authentication

# Asymmetric Key Cryptography

We shared keys for 2000 years

# Asymmetric Key Cryptography

We shared keys for 2000 years

Then we found a better way!

# Asymmetric Key Cryptography

We shared keys for 2000 years

Then we found a better way!

RADICALLY DIFFERENT!

MARVELOUSLY ELEGANT!

# Asymmetric Key Cryptography

# Keys Galore!

Everyone gets two keys!

- Public Key
- Private Key

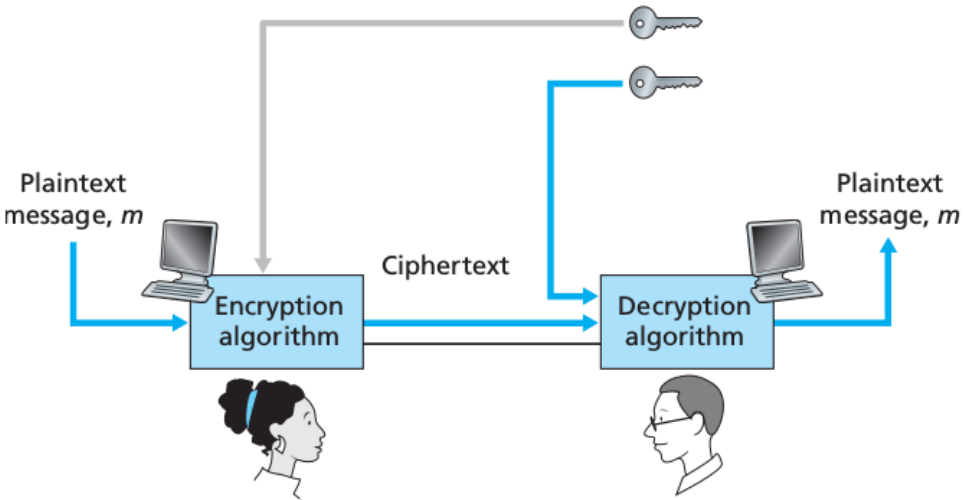
# PKE and Secure Communications

Let's remember:

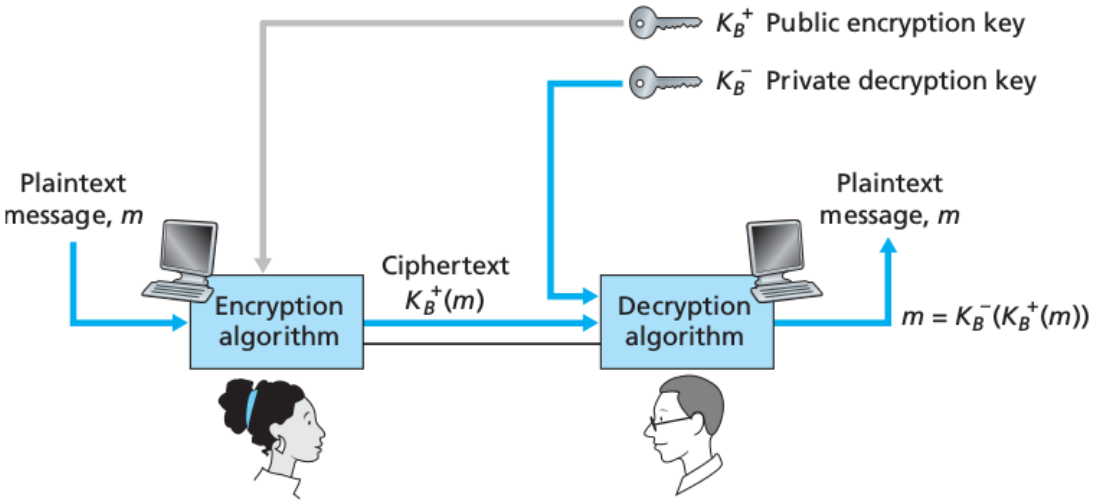
- Confidentiality
- Authentication
- Integrity

How can we achieve these with PKE?

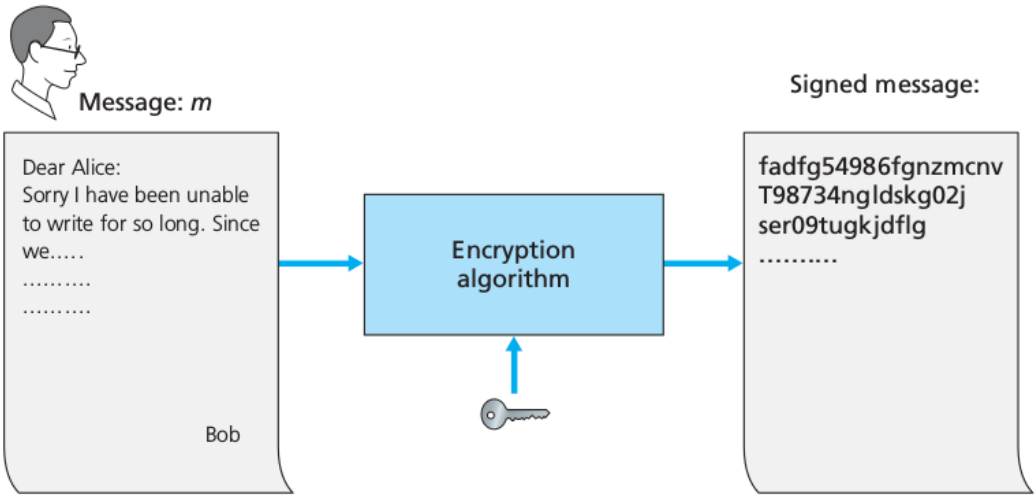
# Confidentiality



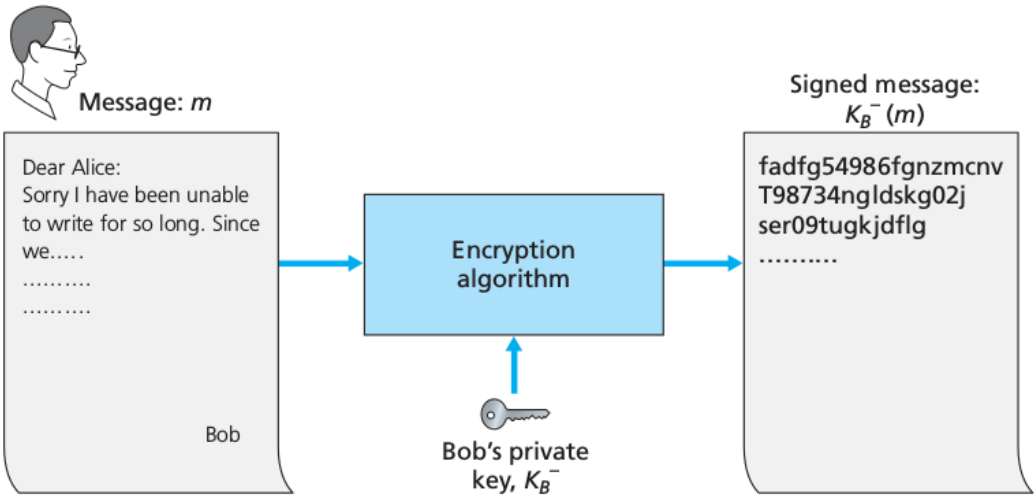
# Confidentiality



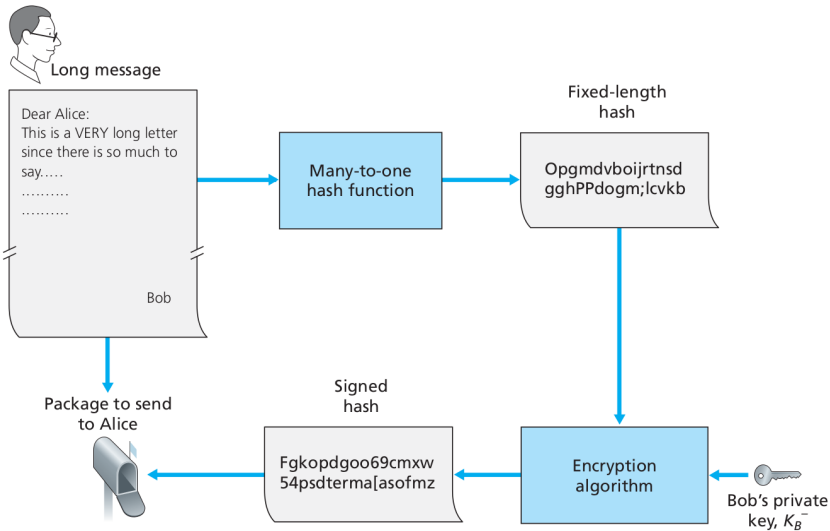
# Authentication



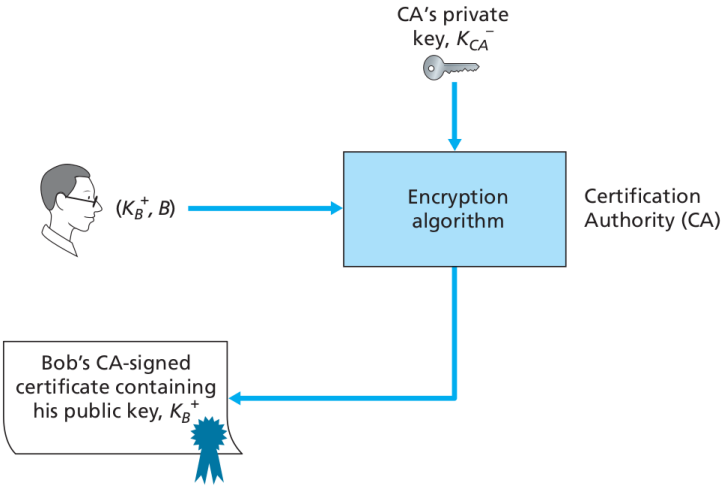
# Authentication



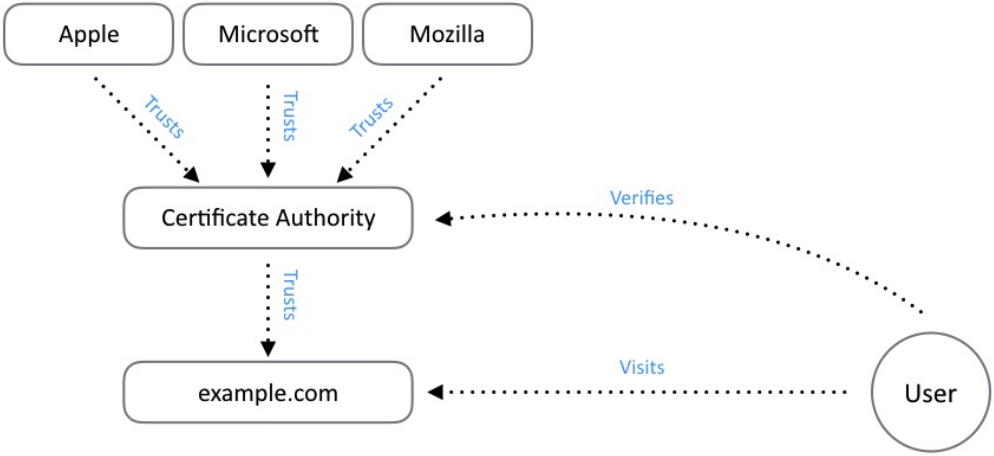
# Integrity and Digital Signatures



# Certificates and Certificate Authorities



# Certificates and Certificate Authorities



Certificate Authorities, what could go wrong?


https://
Chinese CA 'mistakenly' gave out SSL Certs for GitHub Domains

# Asymmetric Key Cryptography and Data in Transit

Ideal for communication

Overhead is a problem

In combination with Symmetric key encryption.

# Recap

- The Need for Multiple Keys
- Asymmetric Key Cryptography
- Confidentiality, Integrity, and Authentication (the other A)