Web 3.0

Cryptography

Karim Stekelenburg

What are we going to discuss

Index

- History of cryptography
- Polymorphism
- Hashing
- Symmetric cryptography
- Asymmetic cryptography
- Exchanging keys

History of cryptography

First occurrences of cryptography

Ancient cryptography

- Egypt — Khnumhotep II — 1900 BC — Symbol replacement
  - Used to ‘enhance it linguistic appeal’, not to conceal.
- West Asia — Mesopotamia — 1500 BC — Symbol replacement
  - Used to conceal a pottery glaze formula
- Greece — Sparta — 900 BC - 192 BC — Cylinder folding
  - Used to conceal military messages
  - Strokes with text were wrapped around a cylinder with a specific diameter

Cesar cypher

Roman empier

A B C D E F G H I J K L M N O P Q R S T U V W X Y

Left shift of 3 characters

D E F G H I J K L M N O P Q R S T U V W X Y A B C

Cesar cipher

Roman empier

A B C D E F G H I J K L M N O P Q R S T U V W X Y

Left shift of 3 characters

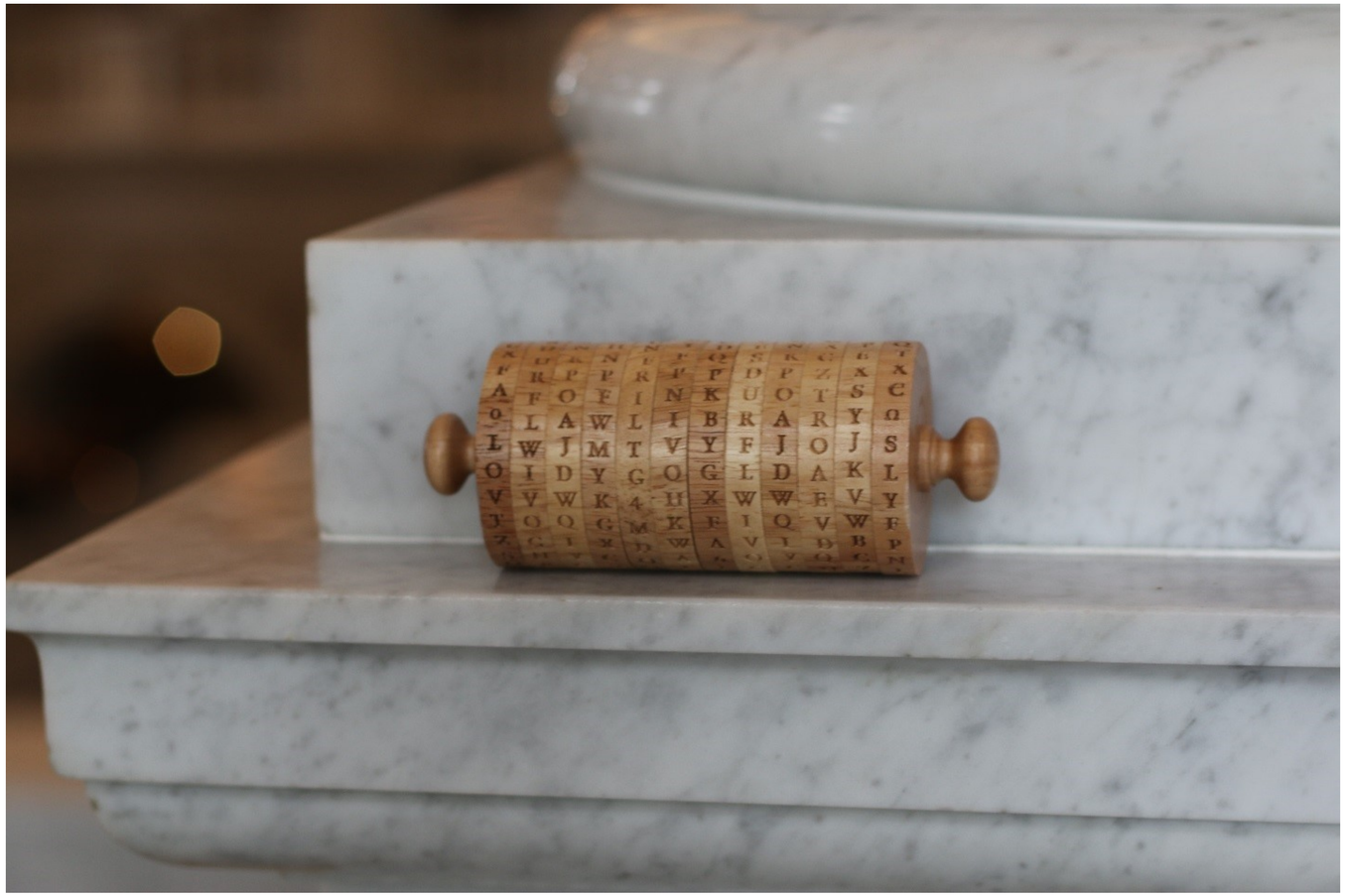
D E F G H I J K L M N O P Q R S T U V W X Y A B C

yilzhzexfk jfklo

blockchain minor

The cipher wheel

AKA Jefferson disk —1795



The enigma machine

WWII

The ‘big’ problem with these techniques?

Once you know the algorithm, you can crack the code

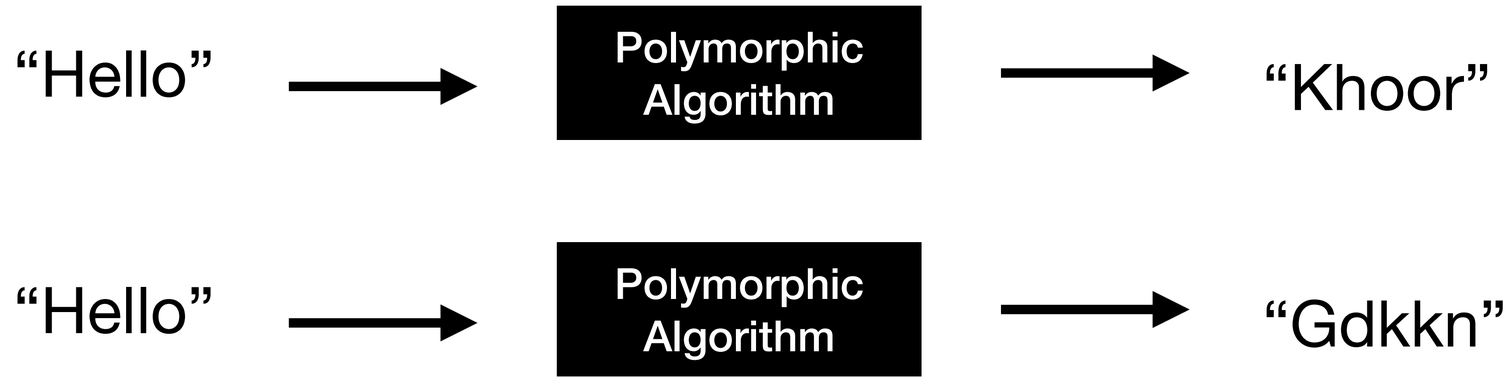
Examples

- Spartan cylinder
  - If I know the cylinder’s diameter, I can crack the code
- Cesar cipher
  - If I know the shift, I can crack the code
- Enigma machine
  - If I know the configuration, I can crack the code

Modern cryptography

Polymorphism

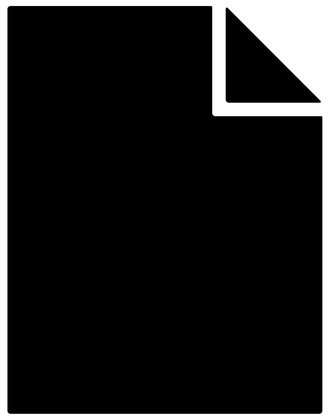
- A very mathematical and complex subject.
  - Far beyond the scope of this course.
- In essence: the cipher changes itself with each use.



Almost <u>all</u> modern cryptography is based on polymorphic cryptography

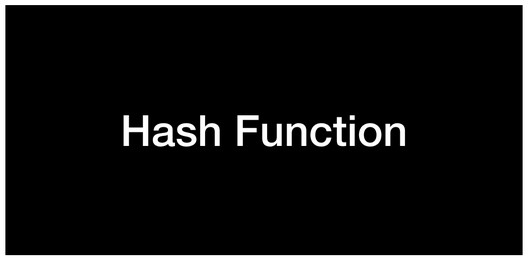
Hashing

A ‘one way function’



01011010001
10010010011
11100111000

(Input)



MDEwMTEwMTA
wMDEKMTAwMT
AwMTAwMTEKM
TExMDAxMTEw
MD

(Hash value)

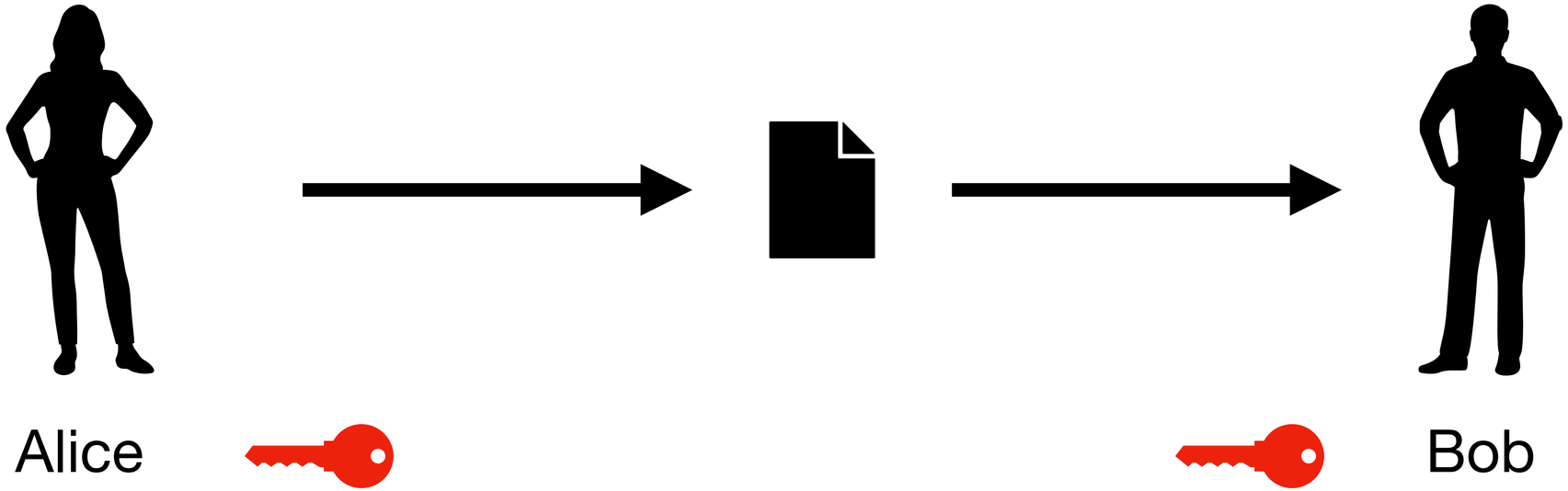
Hashing

Properties

- The same input can produce different outputs (polymorphic)
- Different inputs should **never** produce the same output
- The hash of an input is **quick** to calculate
- The input of a hash value is **slow** to calculate
- Hashing is **NOT** the same as encryption

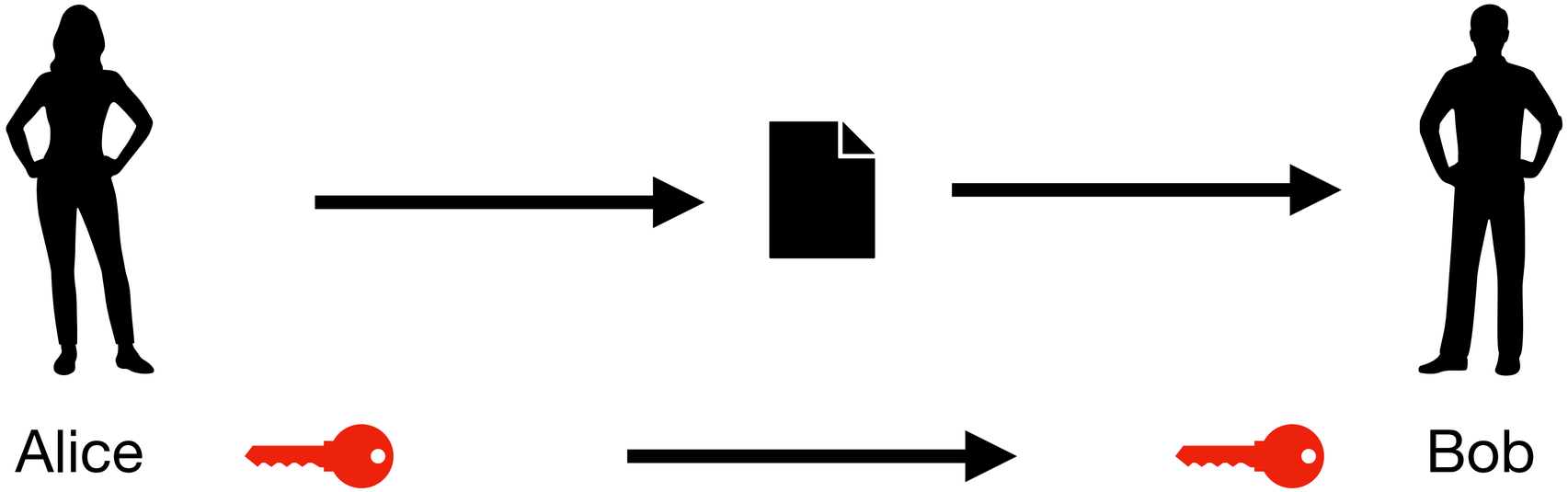
Symmetric cryptography

Single key encryption



Symmetric cryptography

The problem



Symmetric cryptography

Applications

- Banking — Encrypting credit card data or other personally identifiable information
- Data storage — Encrypting data on a device (when it’s not being transferred)

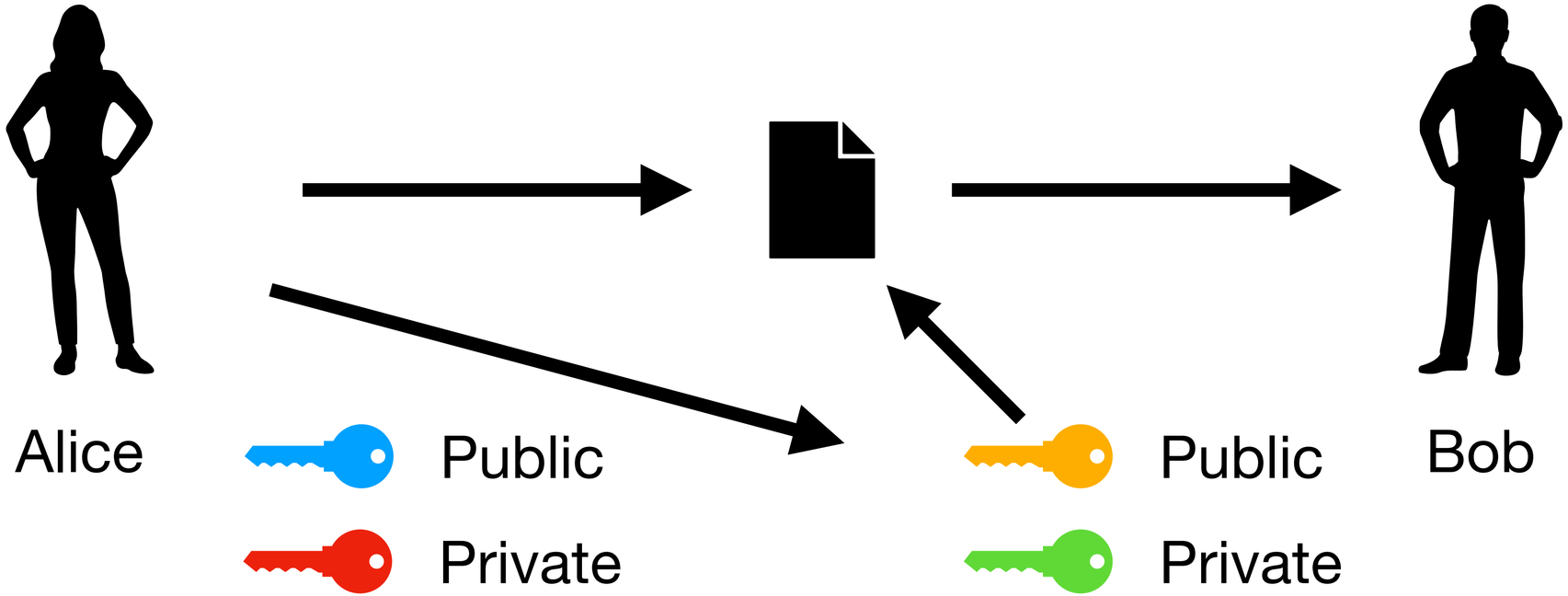
Symmetric cryptography

Properties

- The same key is used to encrypt and decrypt messages
- In order for someone to decrypt a message, they need to know the key
- Transmitting the key is dangerous, because eves-droppers might catch it
- Relatively fast

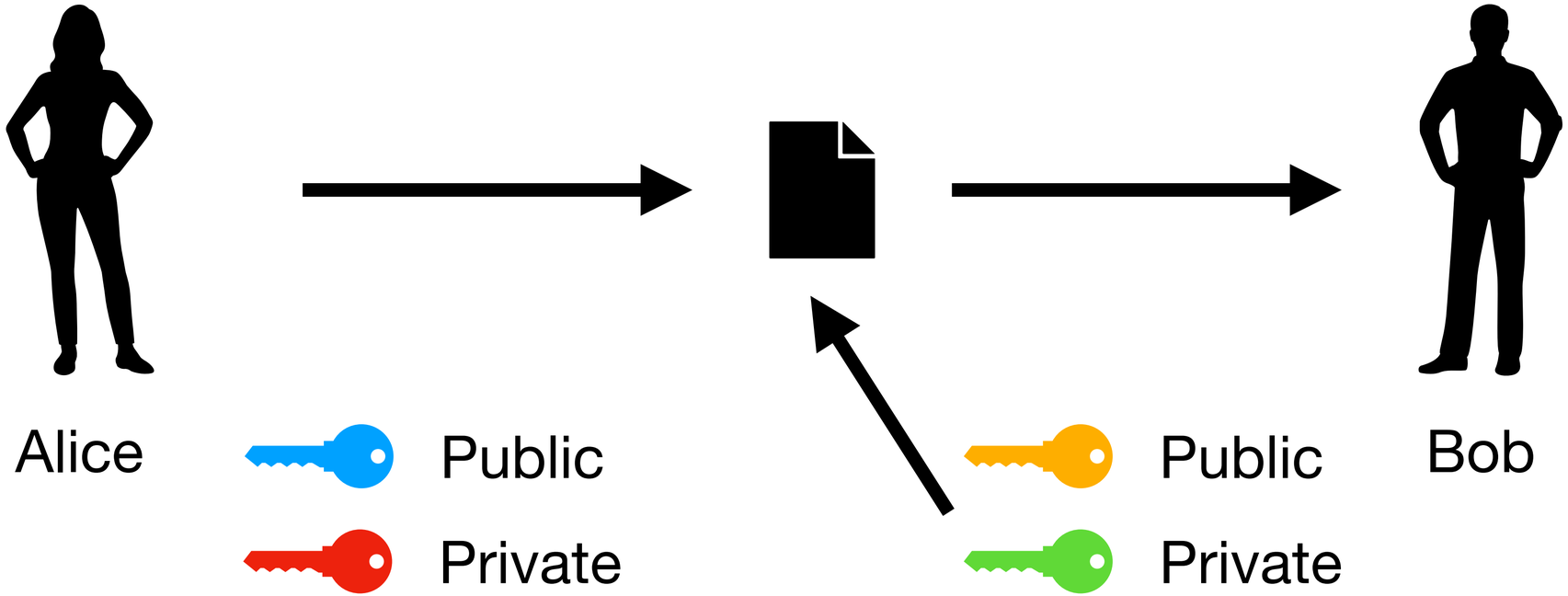
Asymmetric encryption

AKA public key cryptography



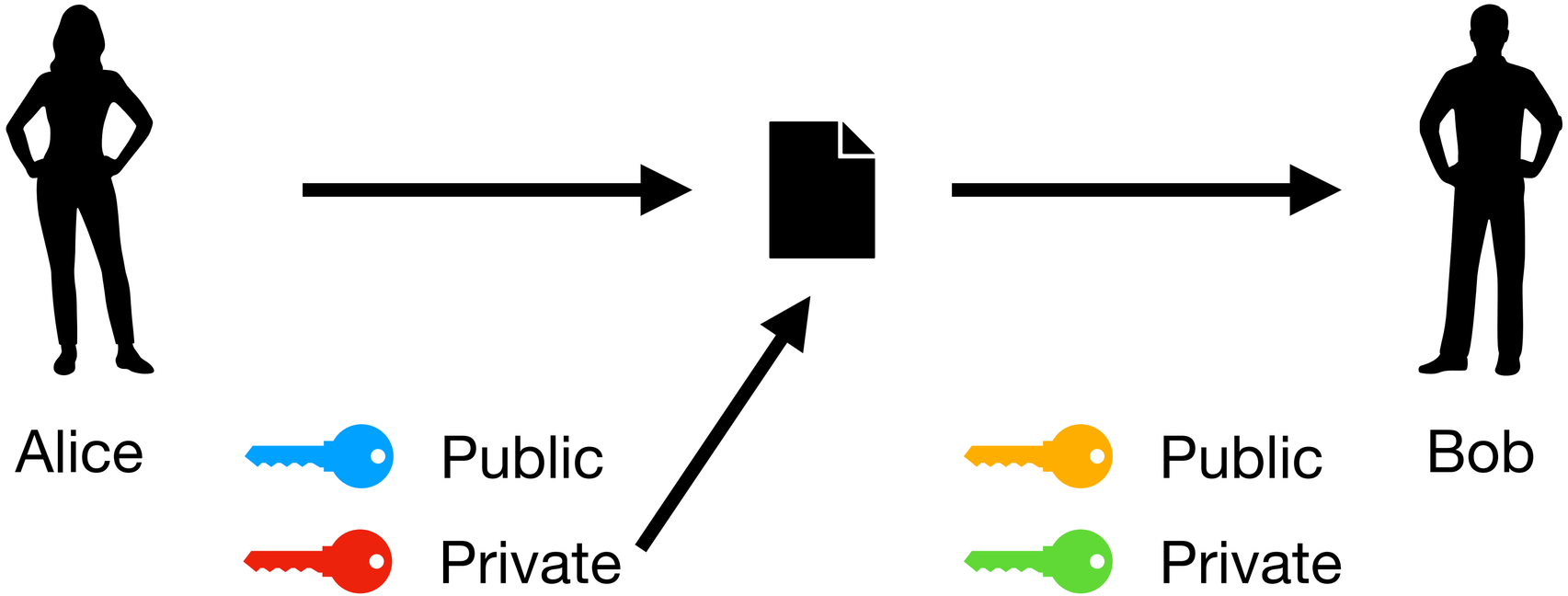
Asymmetric decryption

AKA public key cryptography



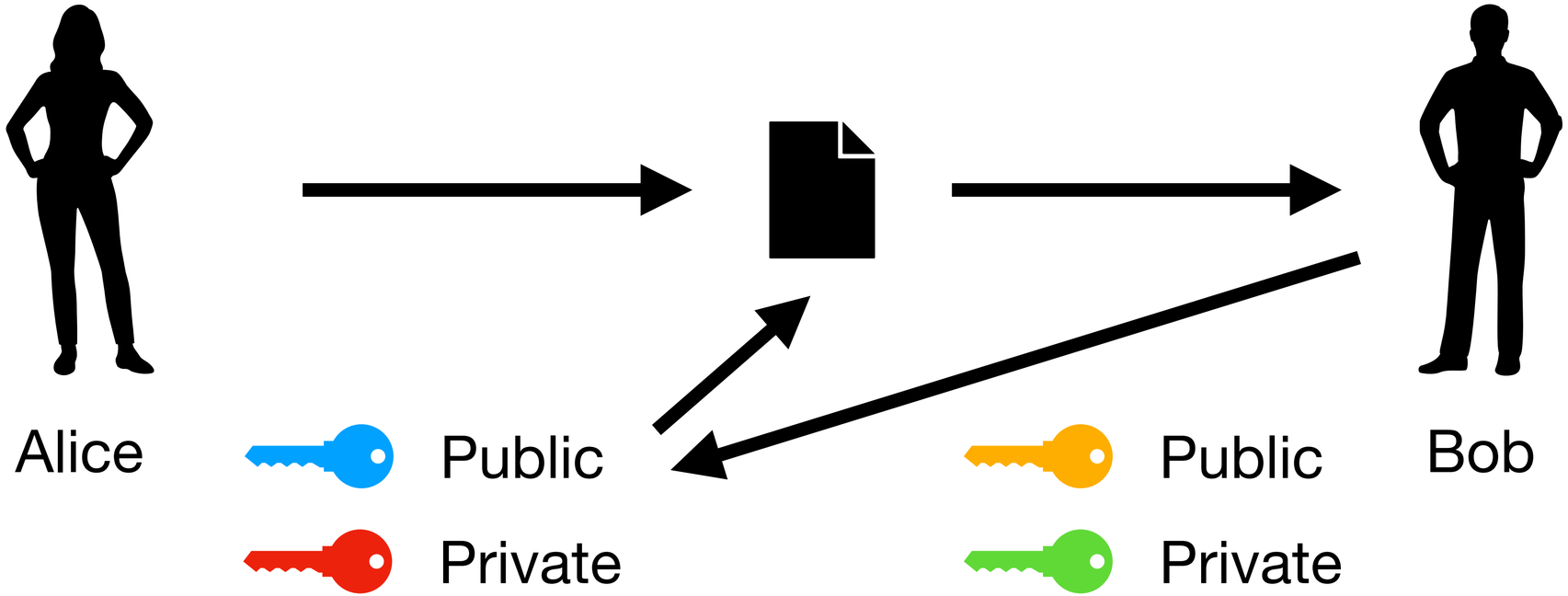
Asymmetric cryptography

Creating signatures



Asymmetric cryptography

Verifying signatures



Asymmetric cryptography

Applications

- Digital signatures
- Blockchain (confirming the identity to authorize transactions)
- Public key infrastructure (PKI) (signed certificates)

Asymmetric cryptography

Properties

- Multiple keys are used to encrypt and decrypt messages
- In order for someone to decrypt a message meant for Bob (encrypted using his public key), key need to know his private key.
- No key or ‘shared secret’ needs to transmitted, only variables.
- Relatively slow compared to symmetric cryptography

A solution to the performance issues of asymmetric encryption

Diffie-Hellman Key Exchange

Diffie-Hellman key exchange

- Solves the problem of exchanging the **symmetric key**
- It does so by creating a exchanging mathematical variables, but the the key itself.
- These variables are then used to create the **same key** by both parties
- The result is that:
  - We have the **security** of **asymmetric encryption**.
  - We have the **speed** of **symmetric encryption**.

Diffie Hellman key exchange

Relevant questions

For the final presentation

- Does the technology use hashing? If so, why?
- Does the technology use encryption?
  - If so:
    - Why?
    - Is it symmetric or asymmetric, or maybe a combination?
    - Why that particular encryption choise?
  - If not:
  - Are there any gains to using encryption? Is there some potential?