

Public Key Cryptography

Simon Pohmann

University of Oxford

October 28, 2021

Remember Patrick's talk...

Medical



Legal

Military

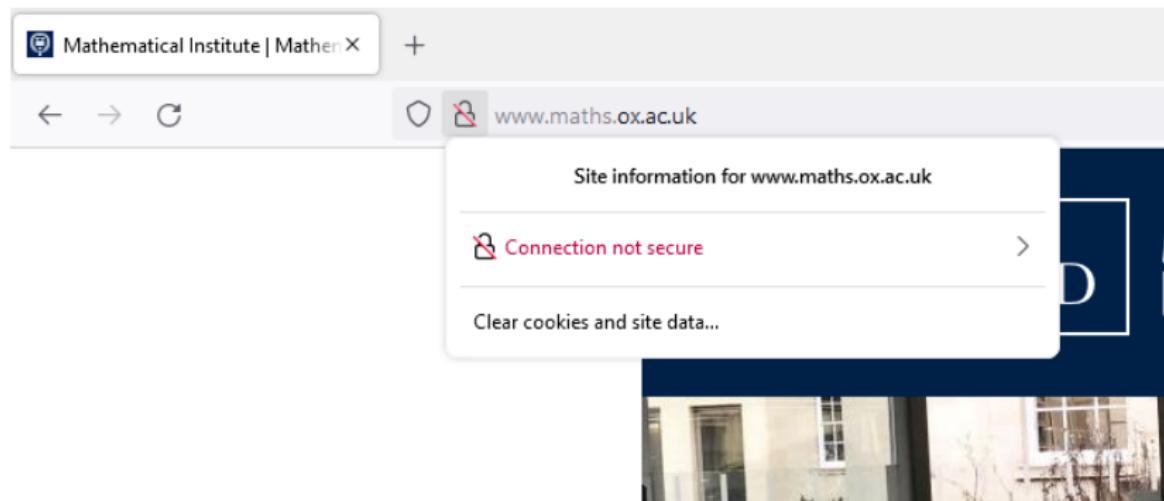
Finance

Critical Infrastructure

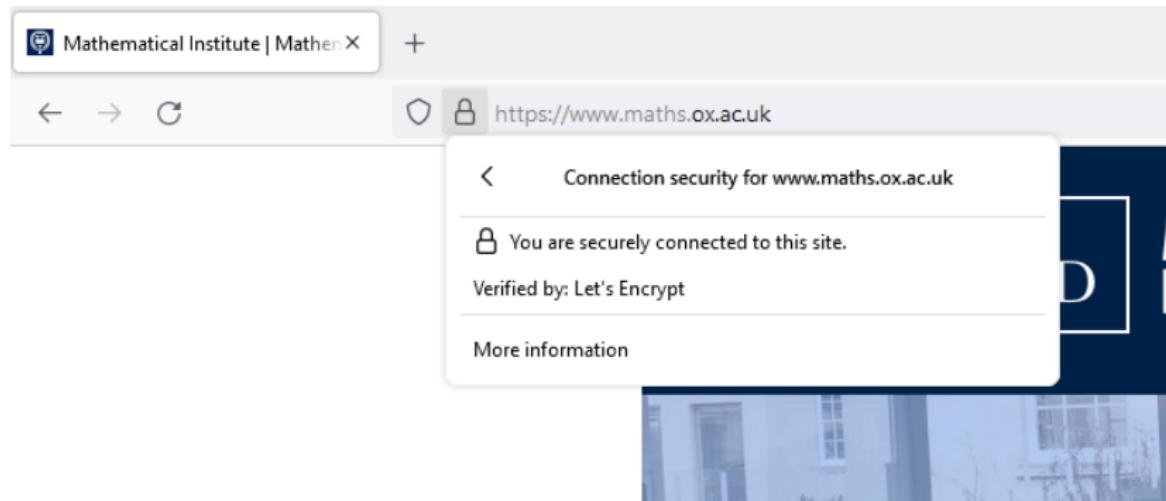
Social Media

e-Commerce

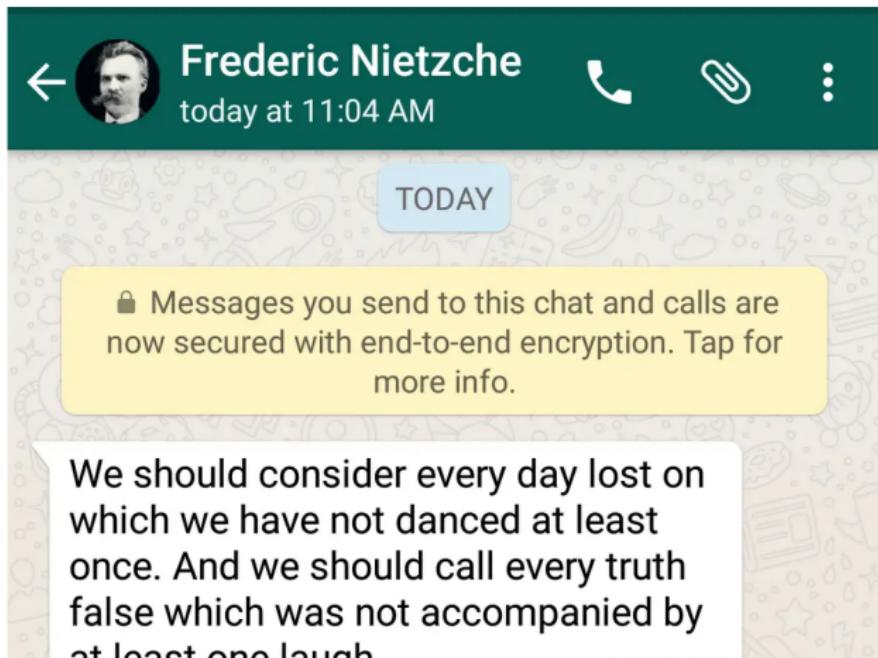
Where do we encounter cryptography?



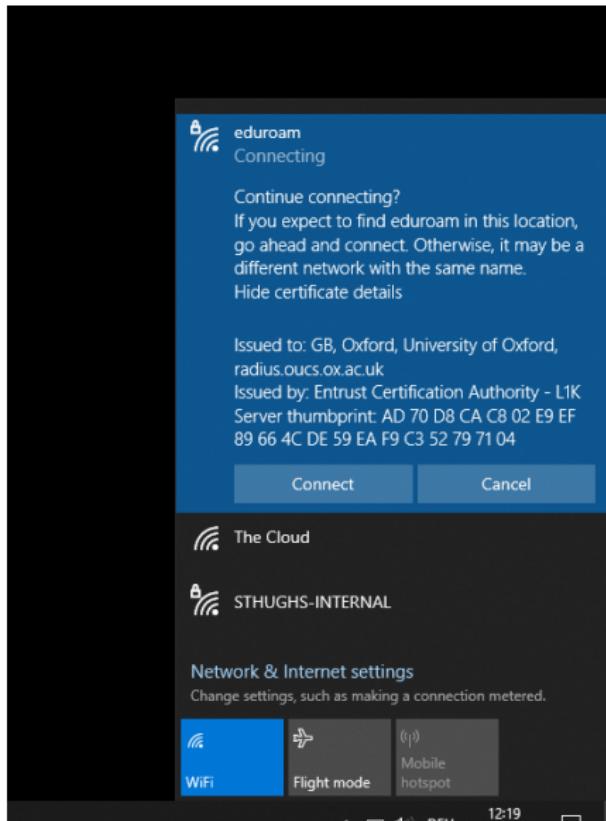
Where do we encounter cryptography?



Where do we encounter cryptography?



Where do we encounter cryptography?



Beginnings of cryptography

Caesar's cipher

H E L L O
↓ +3
K H O O R

Beginnings of cryptography

Caesar's cipher

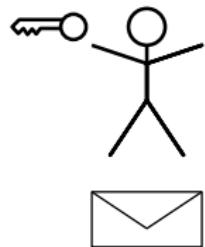
The diagram shows the encryption of the word "HELLO" using a Caesar cipher with a shift of 3. The letters are arranged in two rows: "H E L L O" on top and "K H O O R" on the bottom. A vertical arrow between the two rows is labeled "+3", indicating the shift.

H	E	L	L	O
↓ +3				
K	H	O	O	R

- Very insecure (even if shift is unknown)
- Symmetric cipher

Symmetric cryptography

Alice



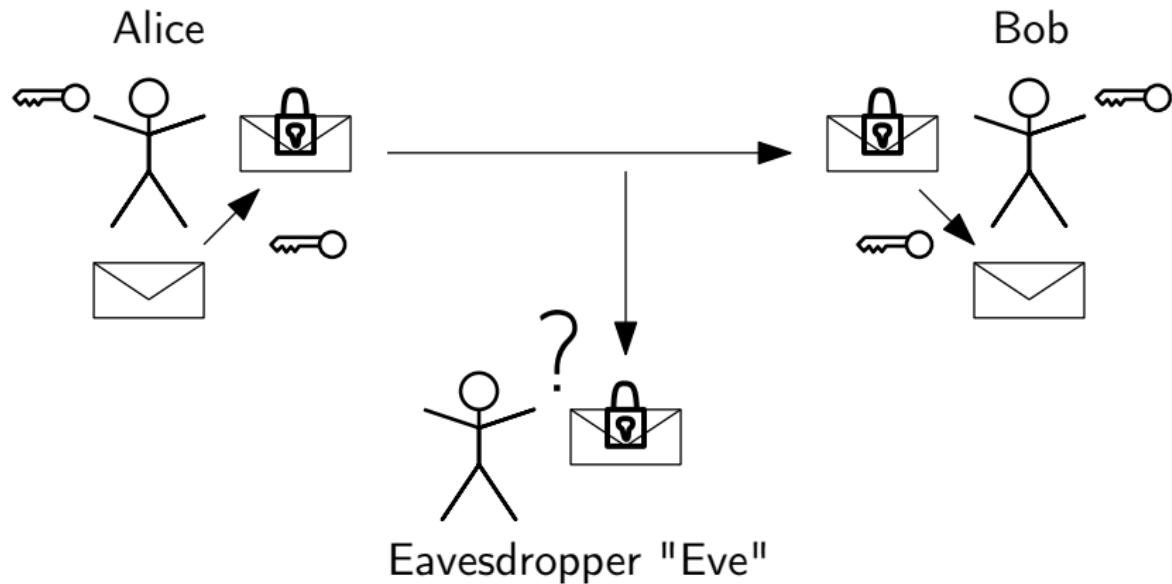
Bob



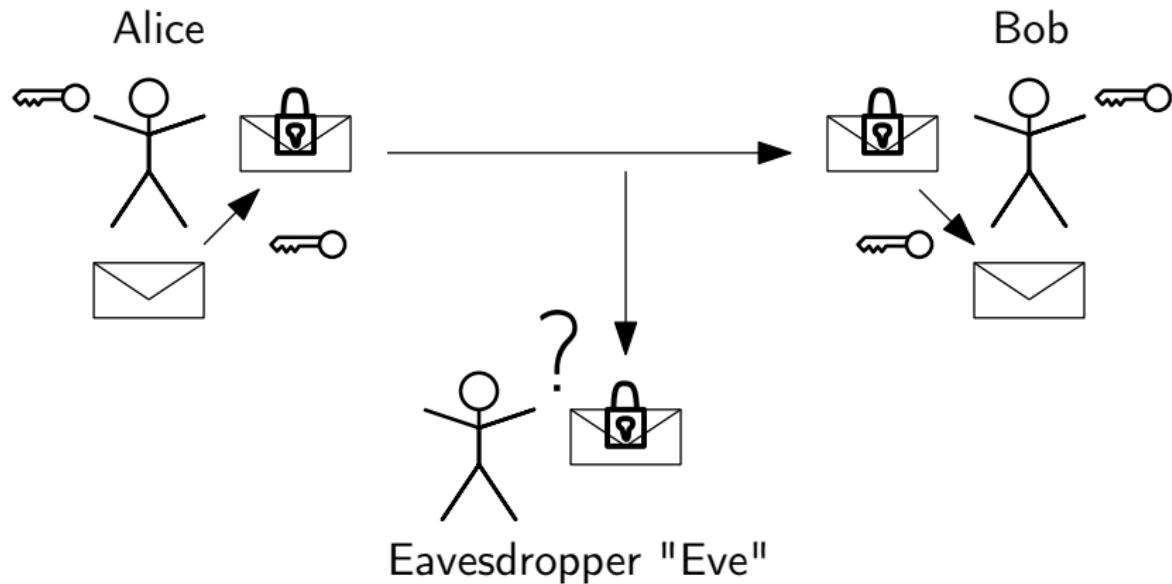
Symmetric cryptography



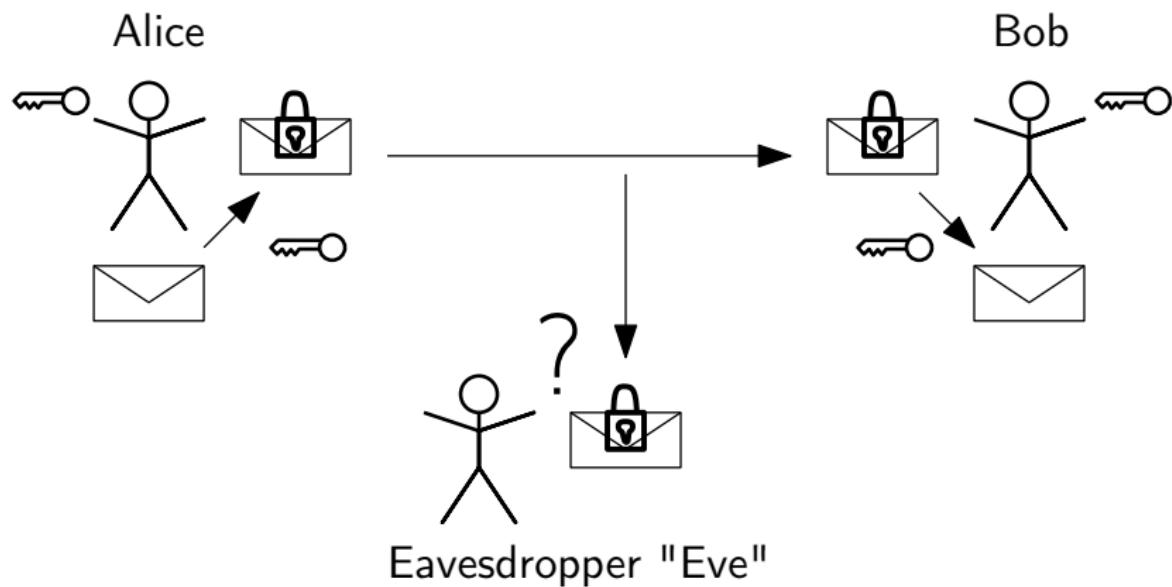
Symmetric cryptography



Symmetric cryptography

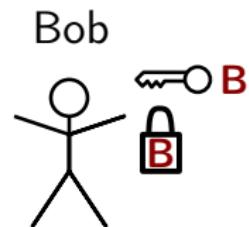
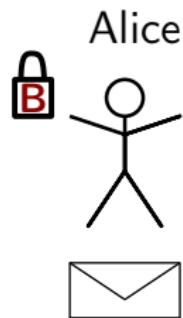


Symmetric cryptography



Problem: Key Exchange!

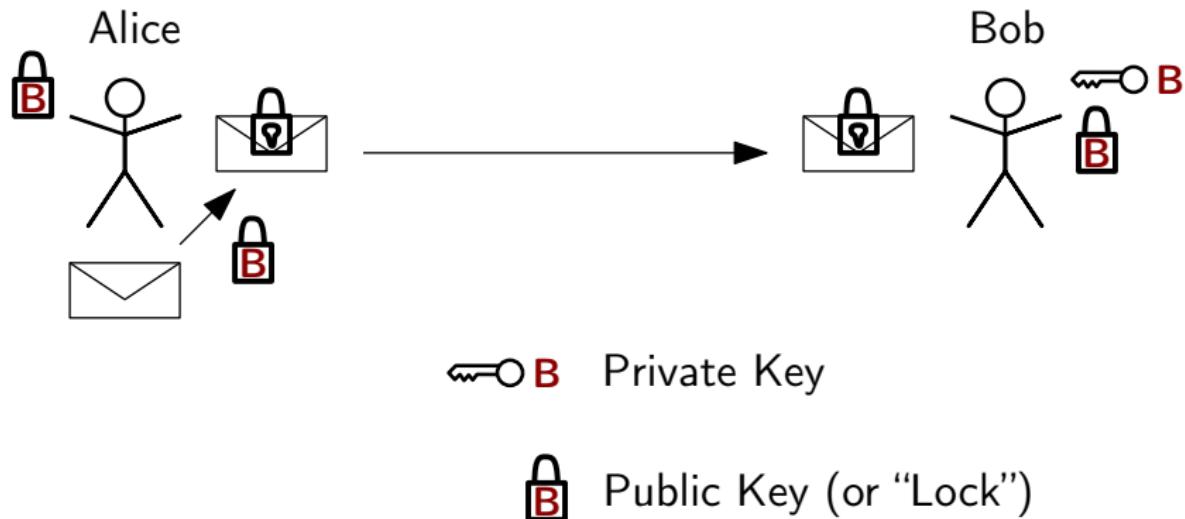
Asymmetric cryptography



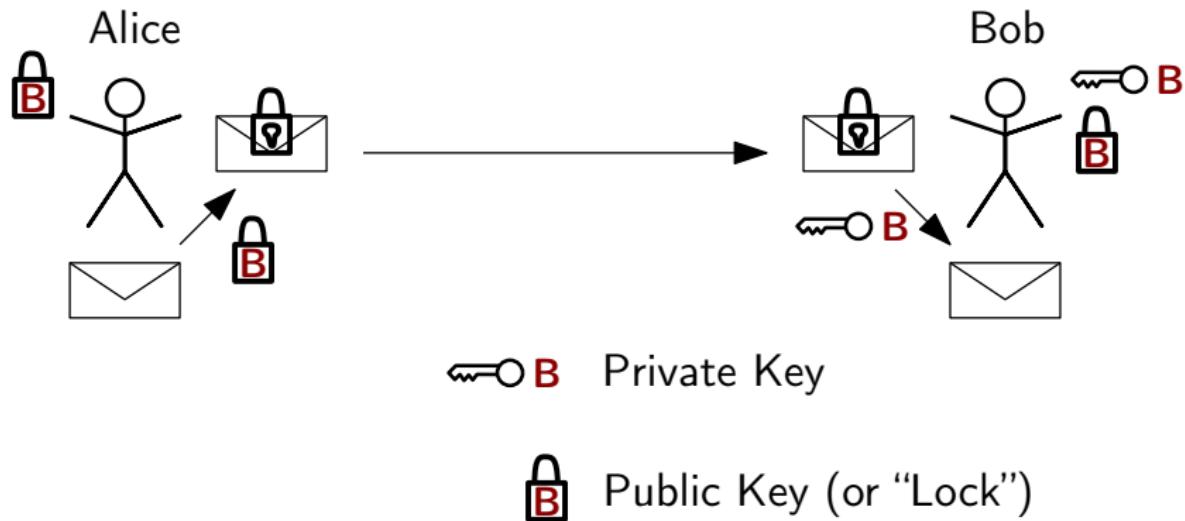
🔑 B Private Key

🔒 B Public Key (or “Lock”)

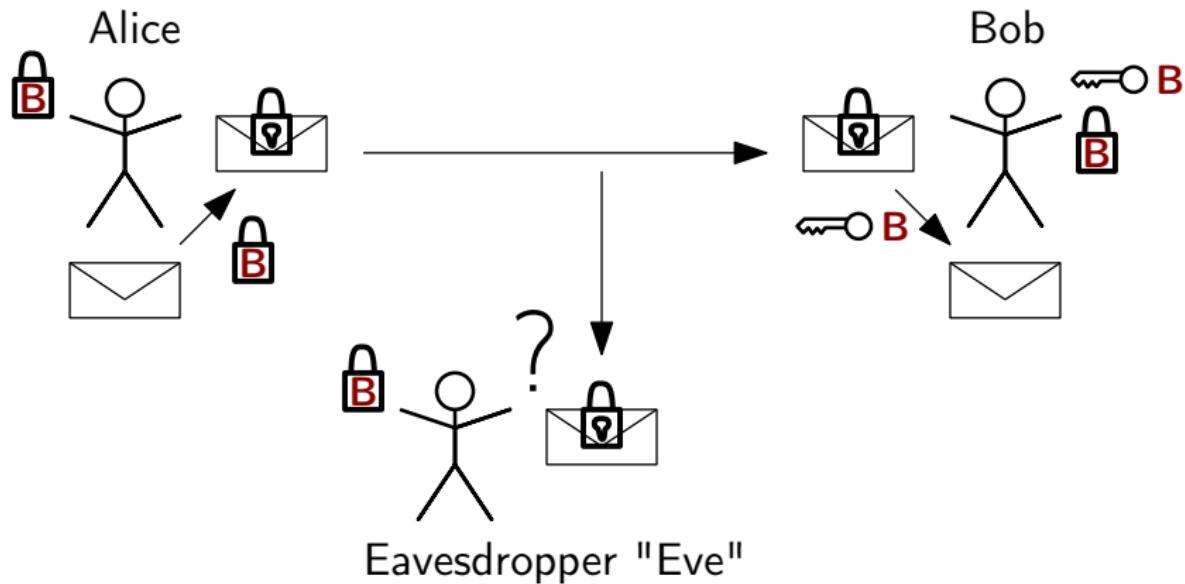
Asymmetric cryptography



Asymmetric cryptography



Asymmetric cryptography



An issue in Public Key Crypto

- Symmetric cryptography can (in principle) be “perfectly secure”
- Asymmetric cryptography cannot

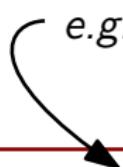
For all possible messages do

- Encrypt the message using the public key
- If the result matches the cipher, we are done

An issue in Public Key Crypto

- Symmetric cryptography can (in principle) be “perfectly secure”
- Asymmetric cryptography cannot

e.g. *all 1000-character sequences*



For all possible messages do

- Encrypt the message using the public key
- If the result matches the cipher, we are done

An issue in Public Key Crypto

- Symmetric cryptography can (in principle) be “perfectly secure”
- Asymmetric cryptography cannot

e.g. *all 1000-character sequences*
there are $9.4 \cdot 10^{1414}$ of them

For all possible messages do

- Encrypt the message using the public key
- If the result matches the cipher, we are done

Public Key Crypto

Asymmetric cryptography relies on problems, that cannot be solved
efficiently or within reasonable time

Public Key Crypto

Asymmetric cryptography relies on problems, that cannot be solved
efficiently or within **reasonable time**

- Usually problems with mathematical structure

Public Key Crypto

Asymmetric cryptography relies on problems, that cannot be solved
efficiently or within **reasonable time**

- Usually problems with mathematical structure
- Currently: Prime factorization and discrete logarithm

Public Key Crypto

Asymmetric cryptography relies on problems, that cannot be solved
efficiently or within **reasonable time**

- Usually problems with mathematical structure
- Currently: Prime factorization and discrete logarithm
- In the future: Quantum-computer safe problems