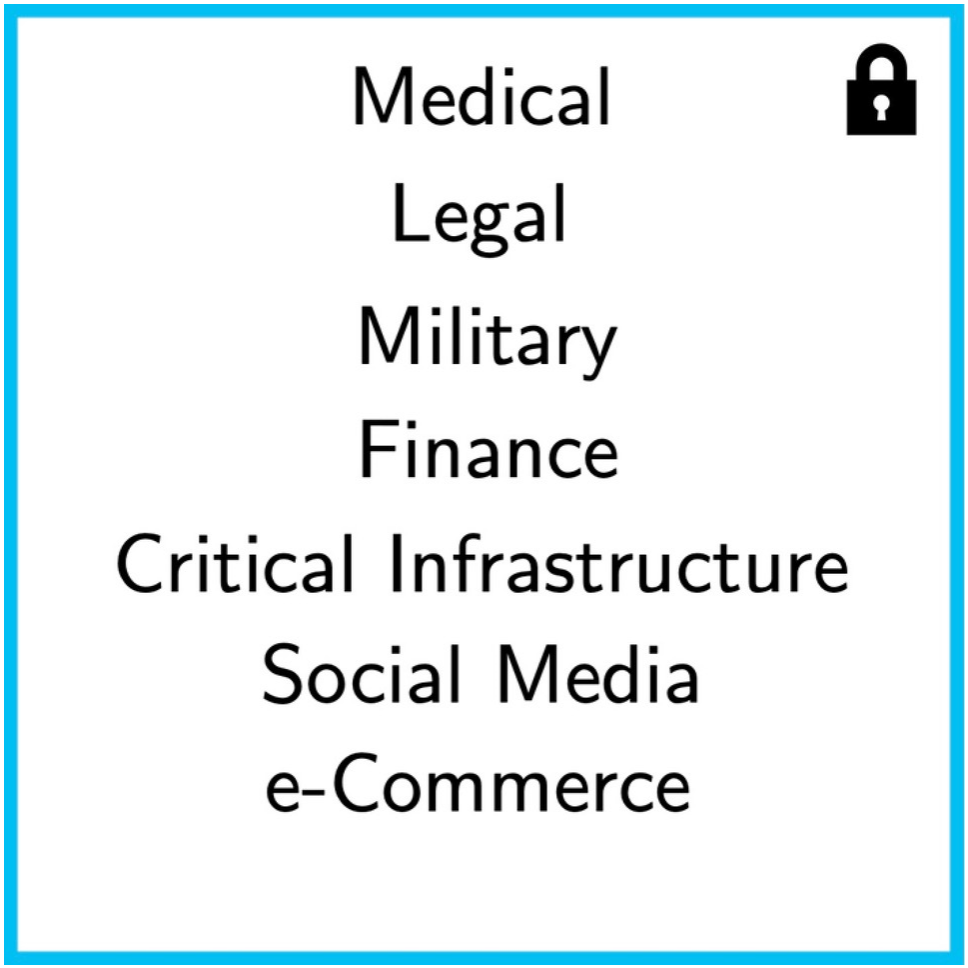
Public Key Cryptography

Simon Pohmann

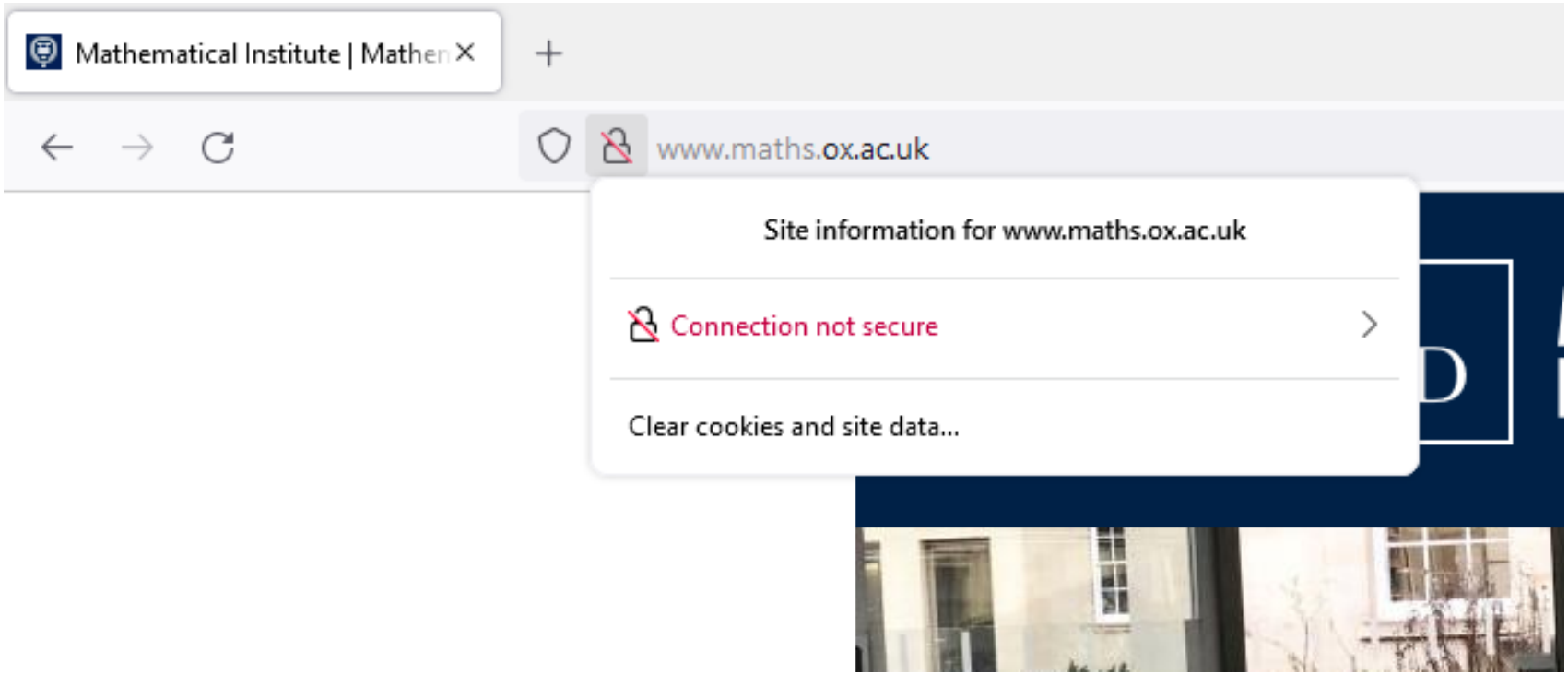
University of Oxford

November 5, 2021

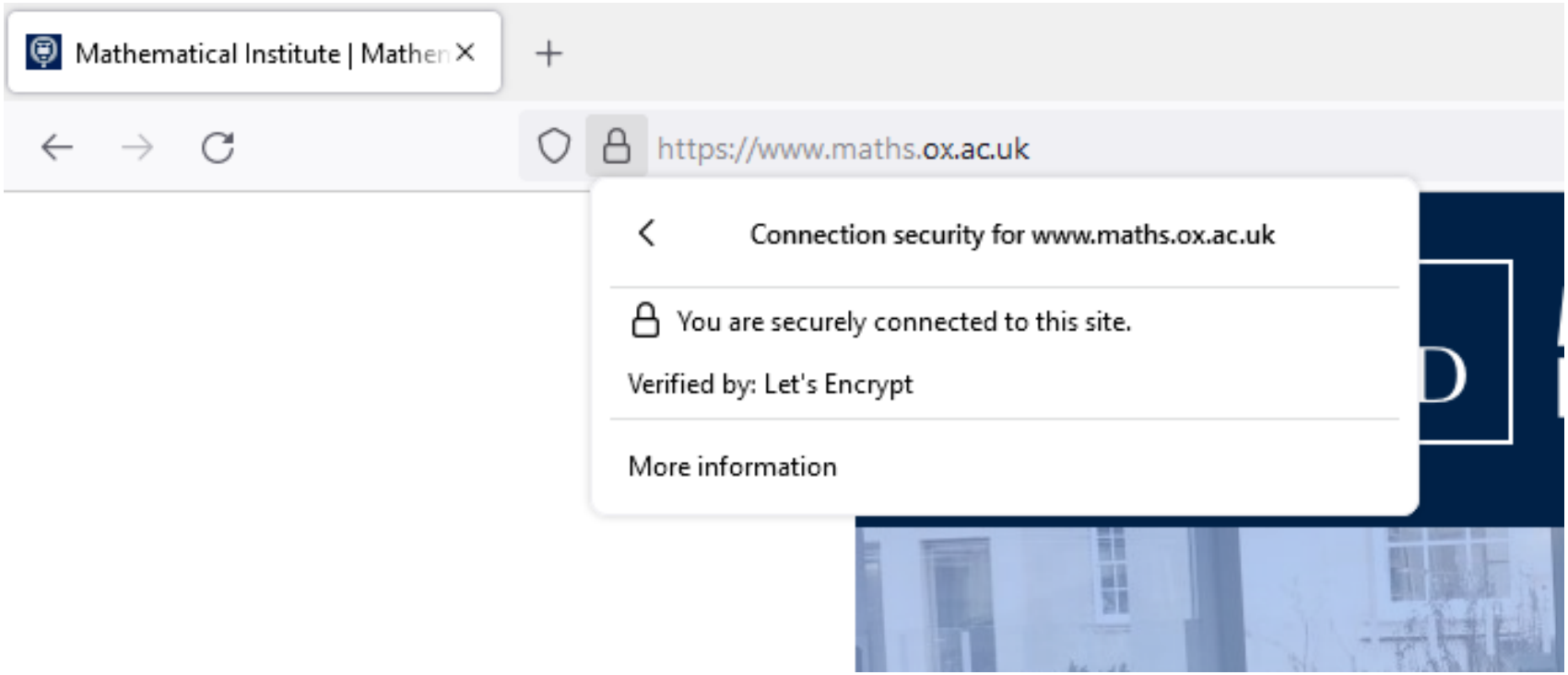
Remember Patrick's talk...



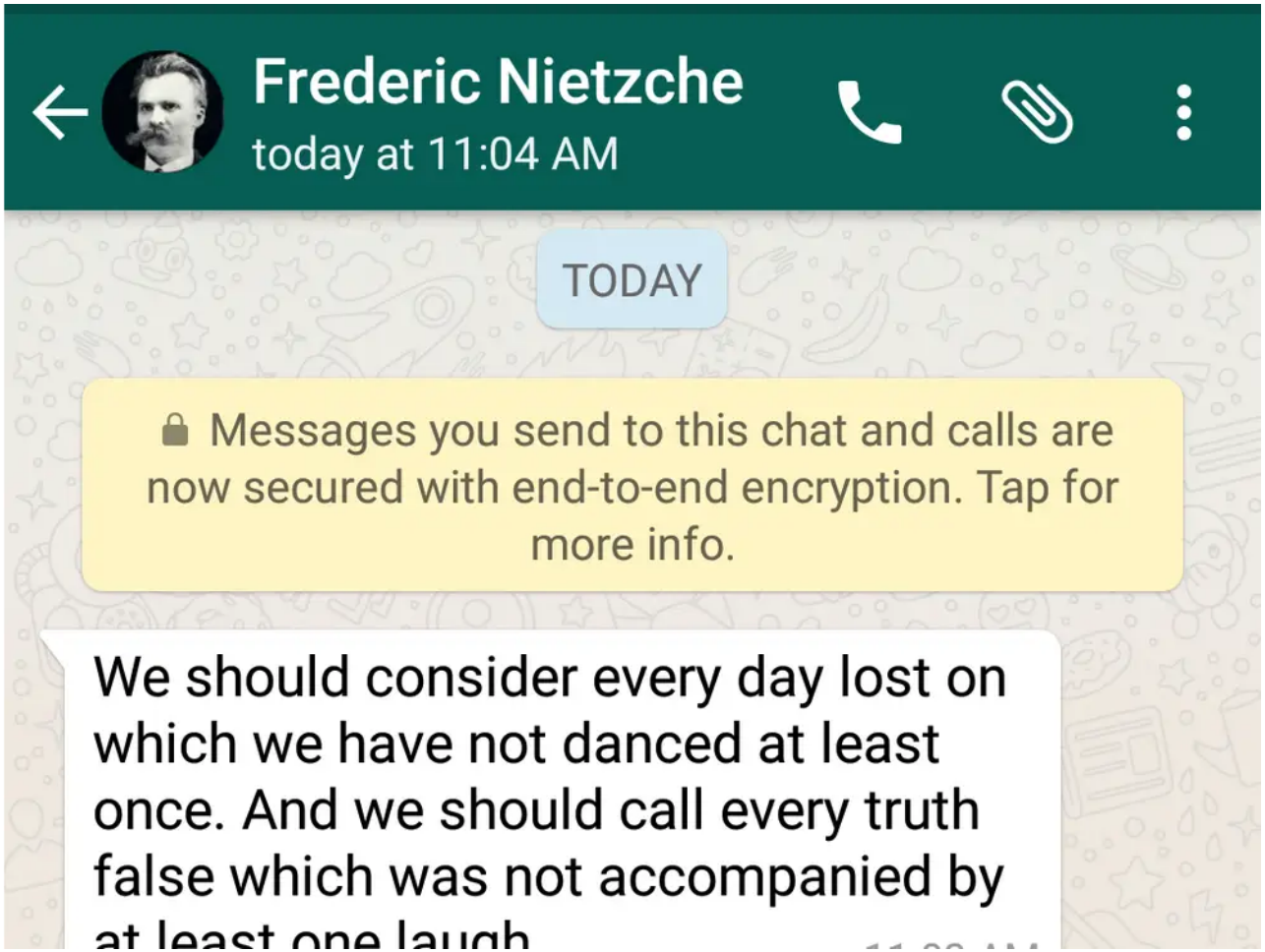
Where do we encounter cryptography?



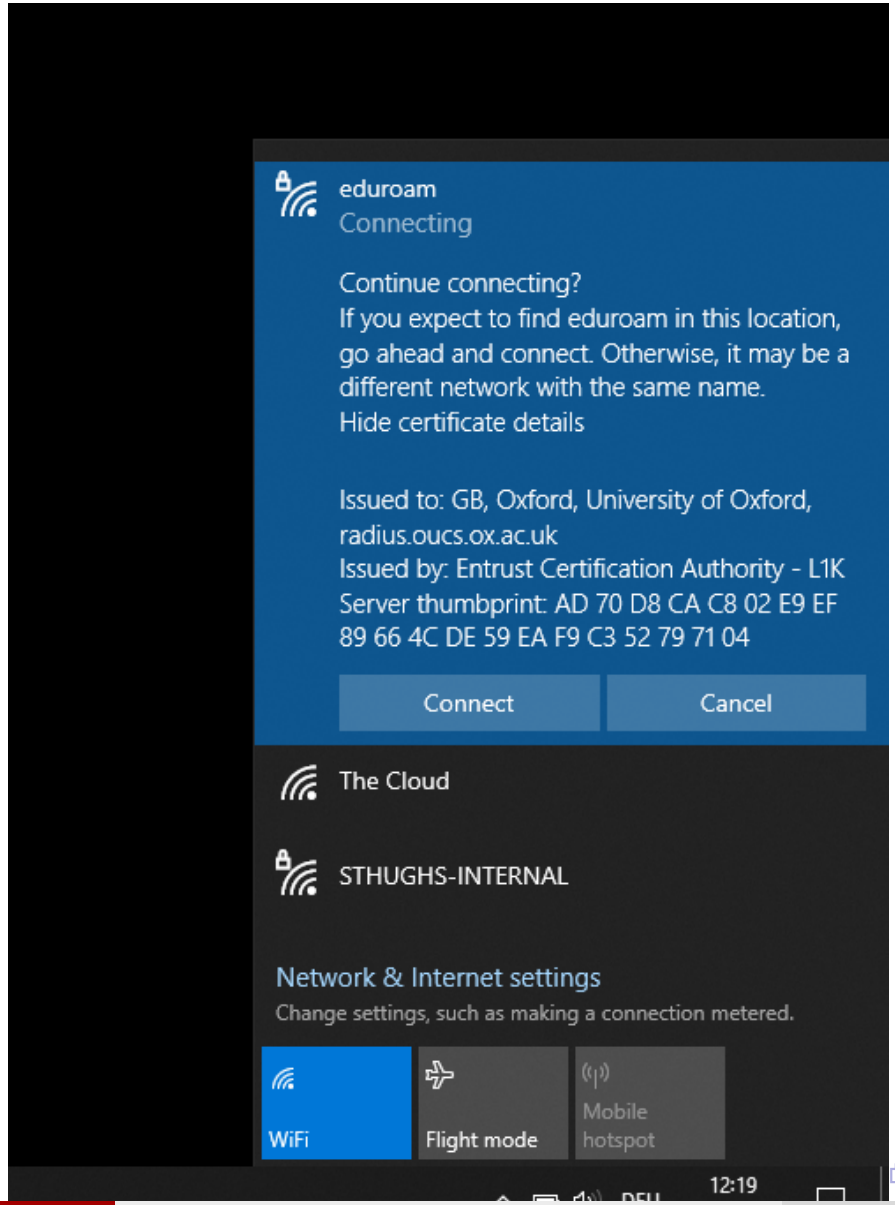
Where do we encounter cryptography?



Where do we encounter cryptography?

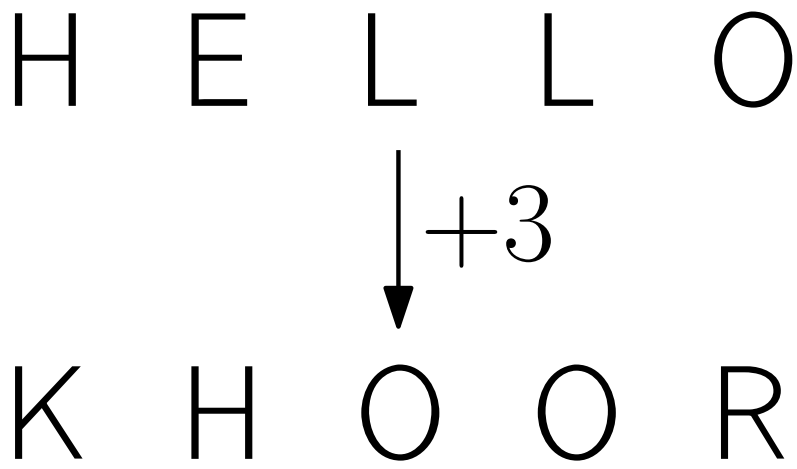


Where do we encounter cryptography?



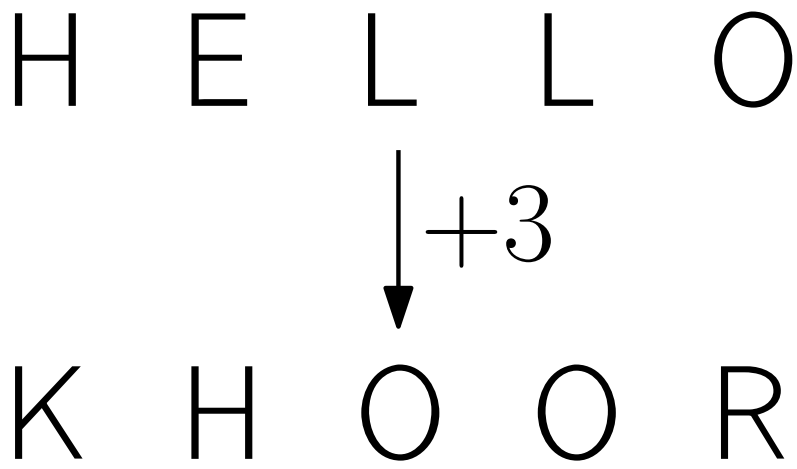
Beginnings of cryptography

Caesar's cipher



Beginnings of cryptography

Caesar's cipher



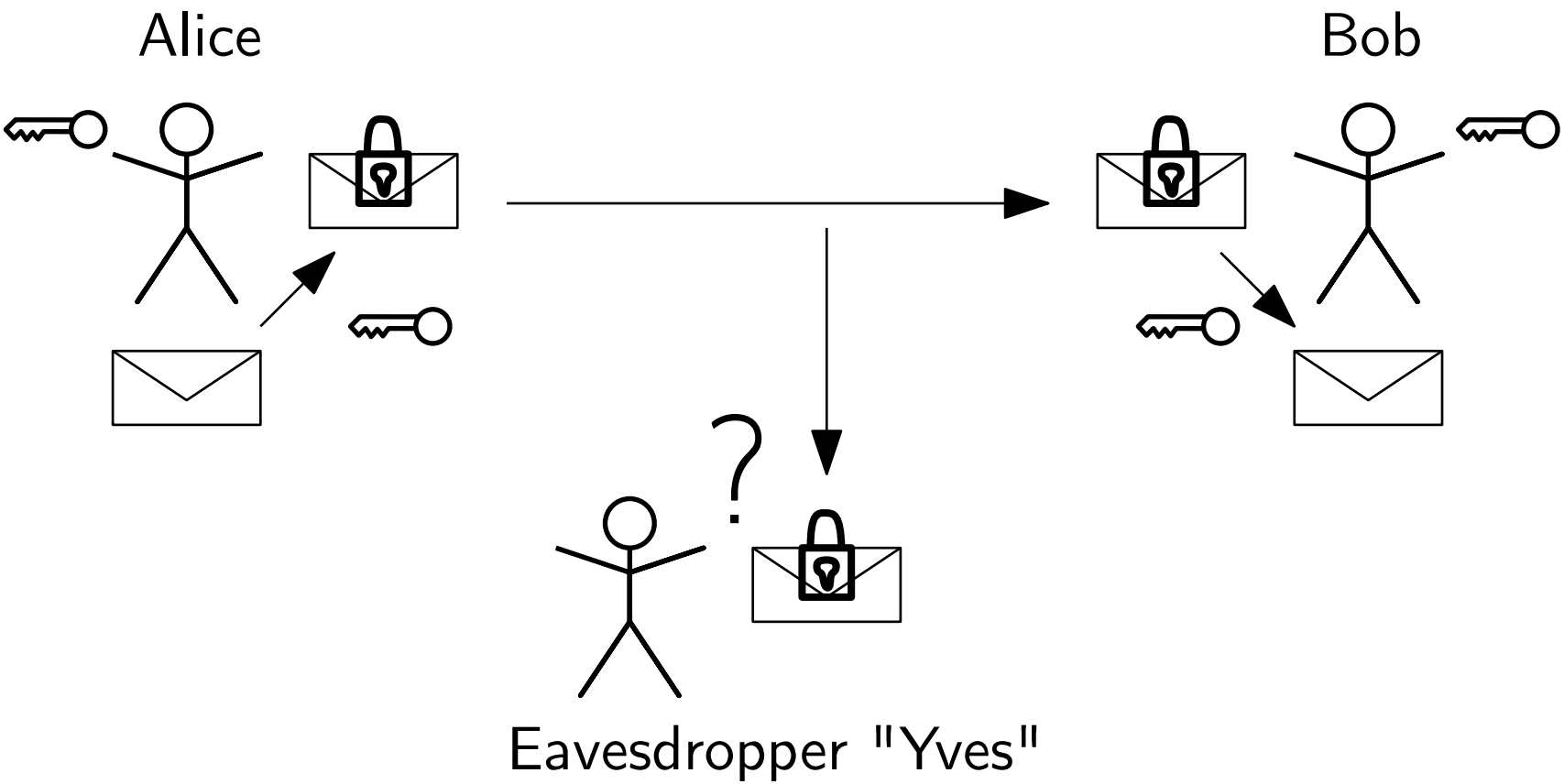
- Very insecure (even if shift is unknown)
- Symmetric cipher

Symmetric cryptography

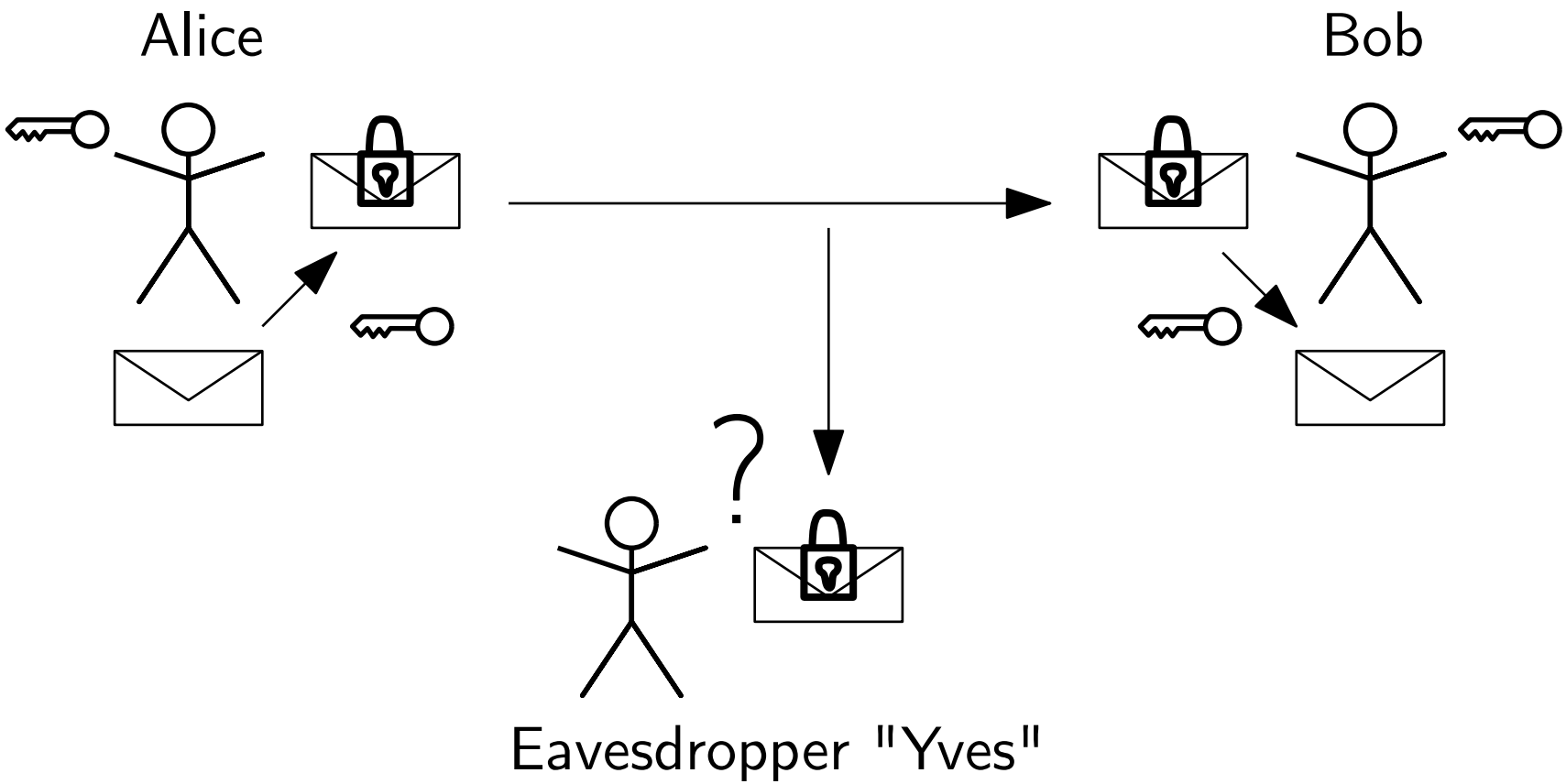
Symmetric cryptography

Symmetric cryptography

Symmetric cryptography

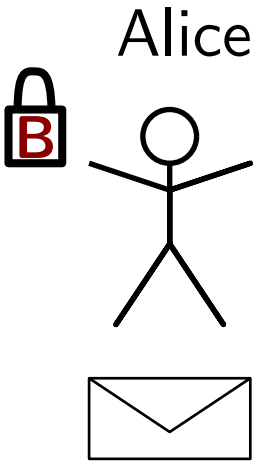


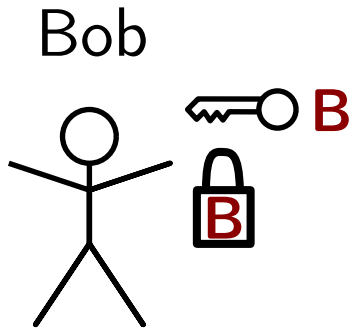
Symmetric cryptography

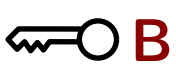


Problem: Key Exchange!

Asymmetric cryptography



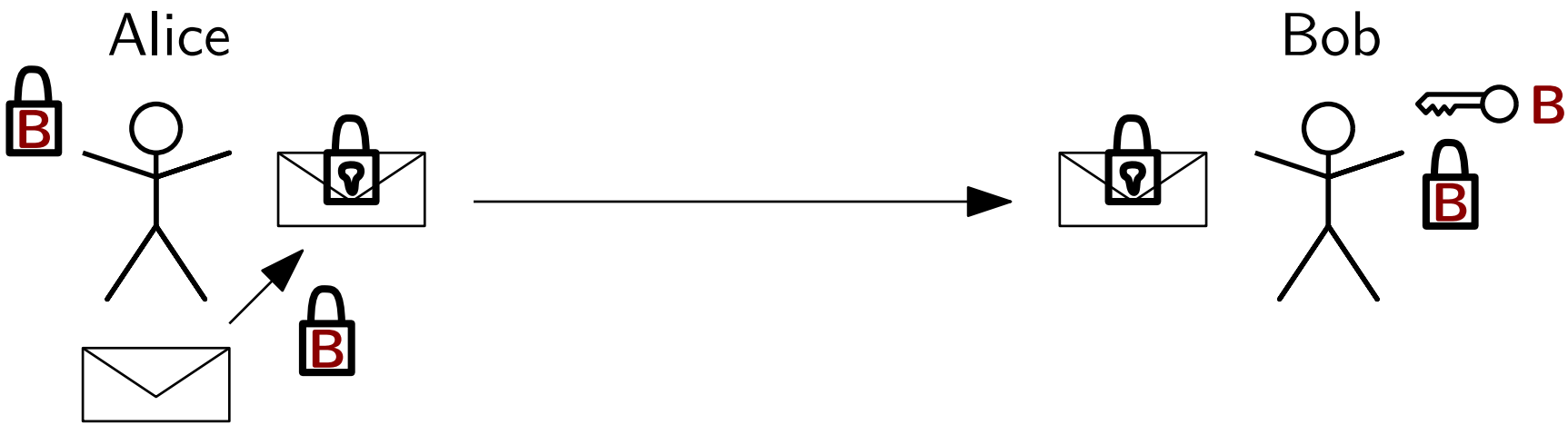




Private Key

Public Key (or "Lock")

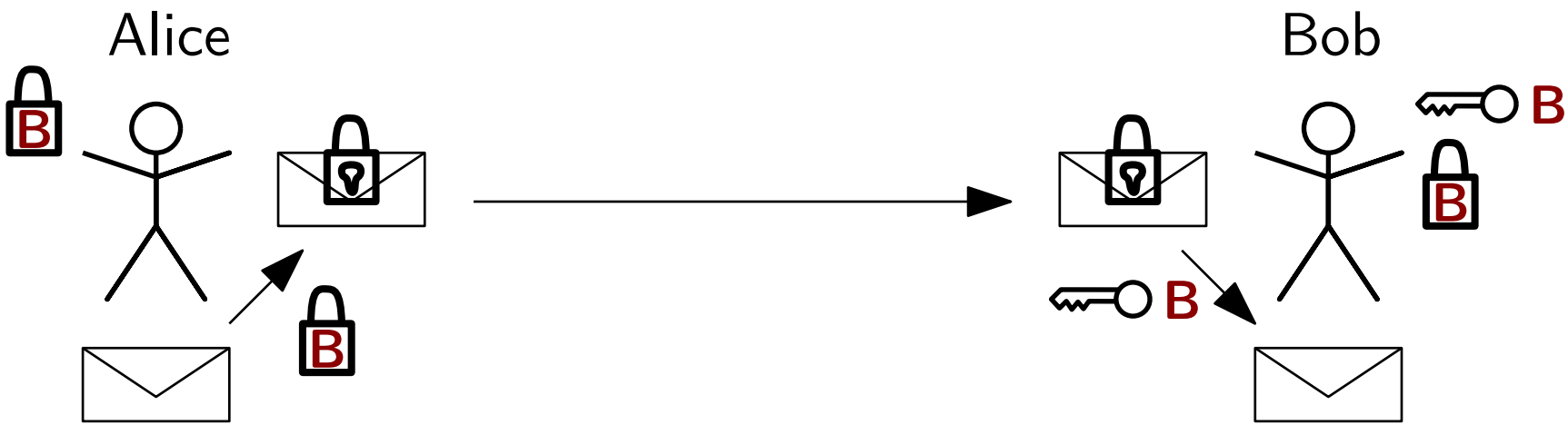
Asymmetric cryptography



B Private Key

B Public Key (or "Lock")

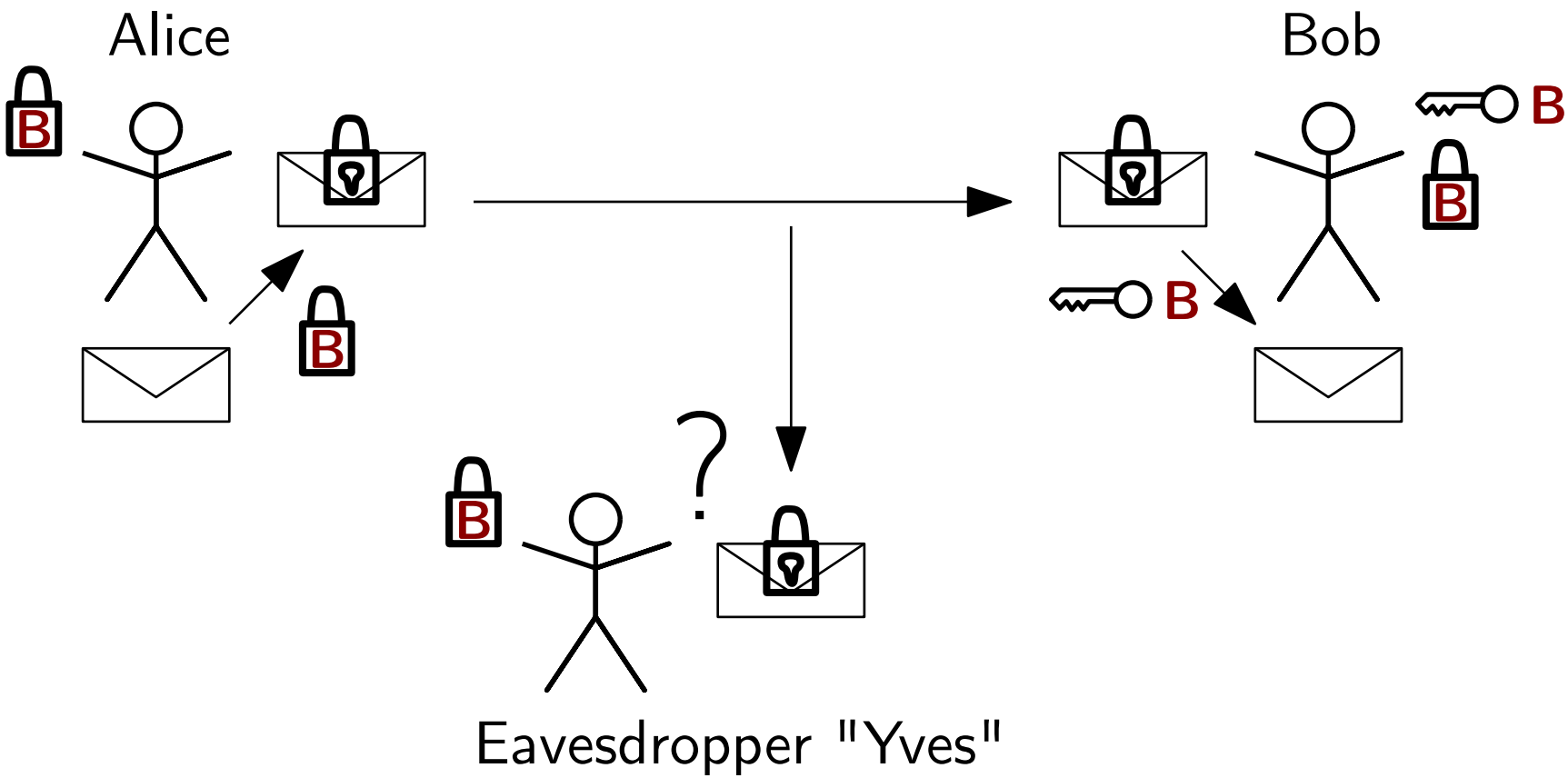
Asymmetric cryptography



B Private Key

B Public Key (or "Lock")

Asymmetric cryptography



An issue in Public Key Crypto

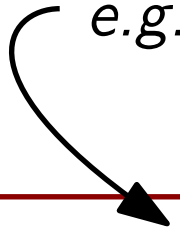
- Symmetric cryptography can (in principle) be "perfectly secure"
- Asymmetric cryptography cannot

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



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**

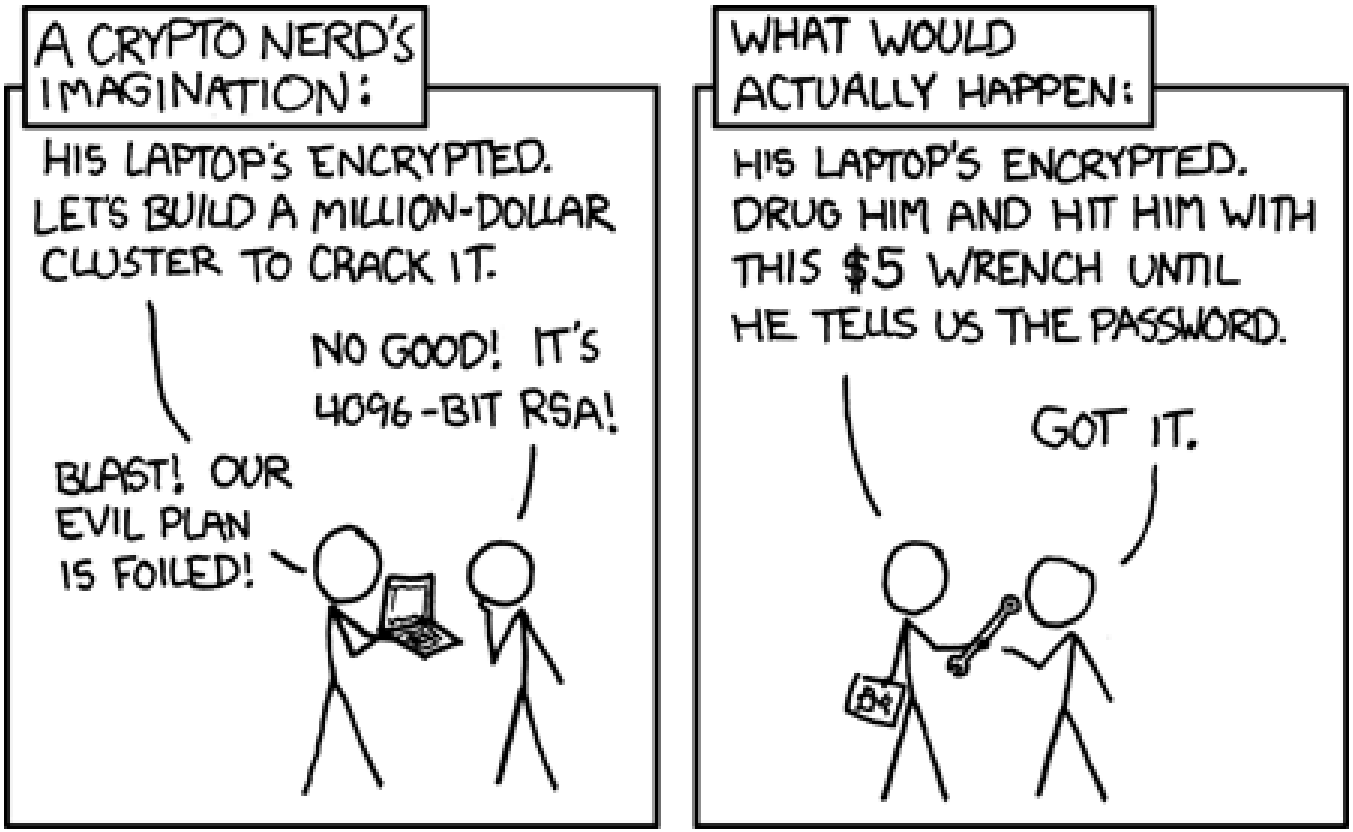
- Usually problems with mathematical structure
- Currently: Prime factorization and discrete logarithm

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

Thank you for listening!



Source: www.xkcd.com