

Introduction to Cryptography








What is cryptography?

- The science of **encryption** and **decryption** of messages
- We want to modify a message in such a way, that an unauthorized person is **not able to understand** it.

What is cryptography?

- **Sender** and **recipient** share a secret information nobody else knows, which is called a **key**
- Without the key you are not able to understand the message.

Where do you encounter encryption in everyday life?

- Messaging Service
 - 
 - 
 - 
 - 
- Browser
 - 
- Internet (Login)
- Wireless 
- E-Mail  etc.

What needs to be protected?

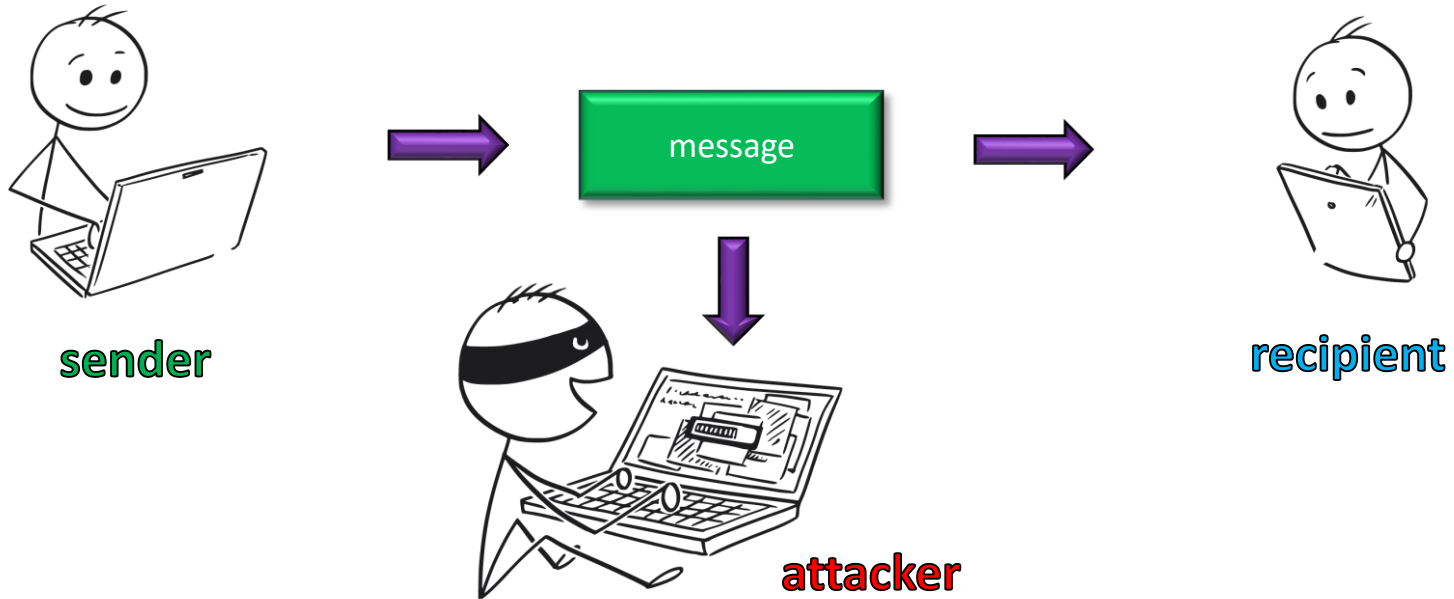
- Personal data
- Confidential communication
- Messages between spies / armies / countrys

Whats not cryptography?

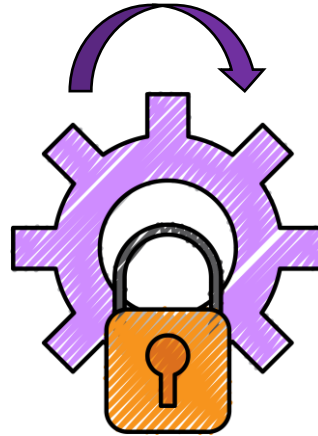
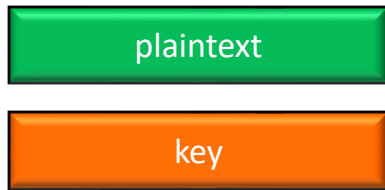
- Hiding messages
- Translating messages

Cryptography always
uses a key!

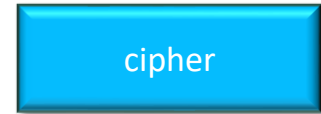
Situation



Sender



Encryption



Situation



sender

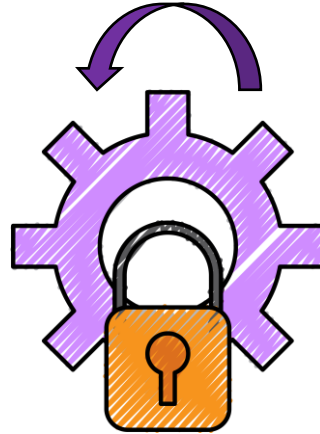
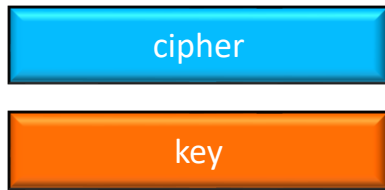


cipher



recipient

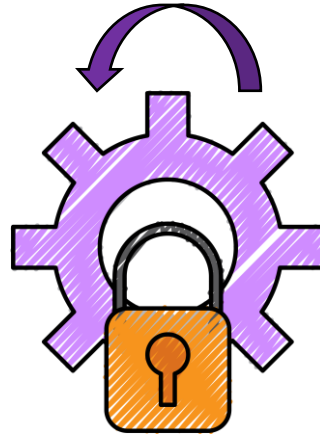
Recipient



Decryption



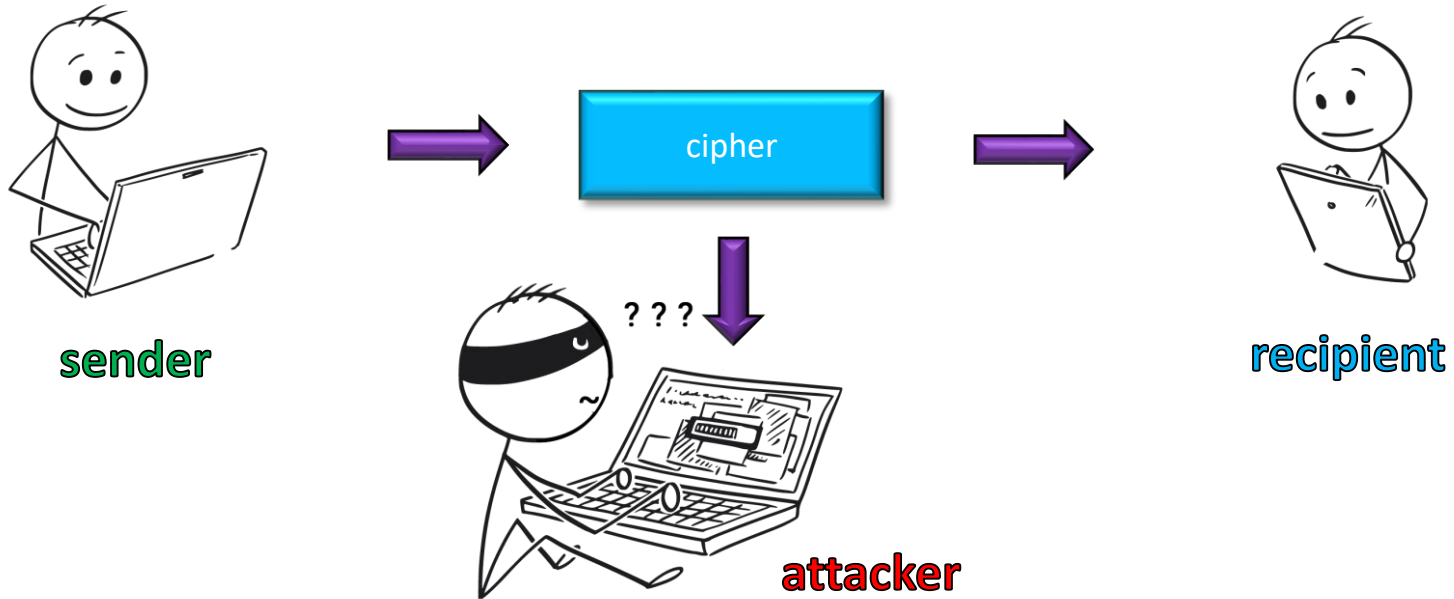
Attacker



Decryption



Situation



Summary

