

Einführung: Kryptographie






Was ist Kryptographie?

- Die Wissenschaft vom **Ver-** und **Entschlüsseln** von Nachrichten
- Wir möchten eine Nachricht so verändern, dass ein unbefugte Person, diese **nicht verstehen kann**.

Was ist Kryptographie?

- **Sender** und **Empfänger** besitzen eine geheime Information, die sonst niemand kennt, diese wird **Schlüssel** genannt.
- Ohne den Schlüssel kann man den Inhalt der Nachricht nicht verstehen.

Wo begegnen euch Verschlüsselungen im Alltag?

- Messenger-Dienste
 - 
 - 
 - 
 - 
- Browser
 - 
- Internet (Login)
- W-LAN 
- E-Mail  usw.

Was muss geschützt werden?

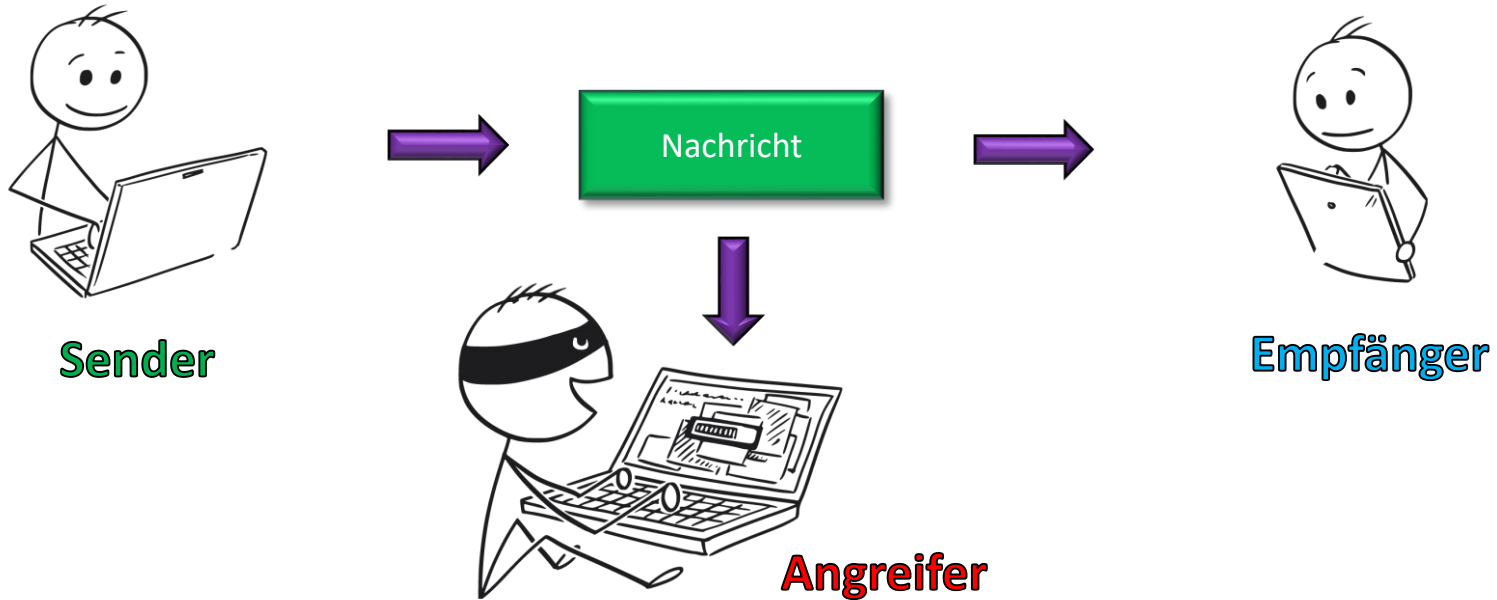
- Persönliche Daten
- Vertrauliche Kommunikation
- Nachrichten zwischen Spionen / Armeen / Staaten

Was ist Kryptographie nicht?

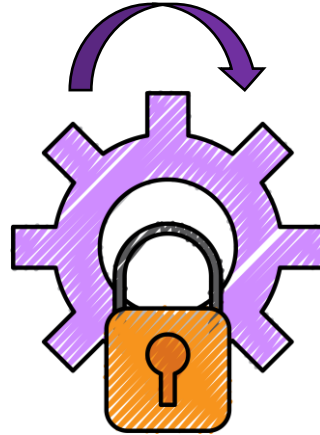
- Verstecken von Nachrichten
(Steganographie)
- Übersetzen von Nachrichten

Bei **Verschlüsselungen** wird
immer ein **Schlüssel** benötigt

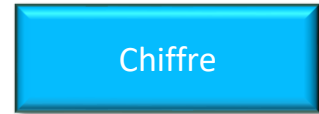
Situation



Sender



Verschlüsseln



Situation



Sender

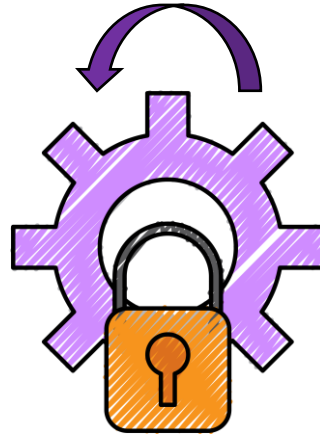


Chiffre

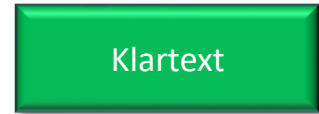


Empfänger

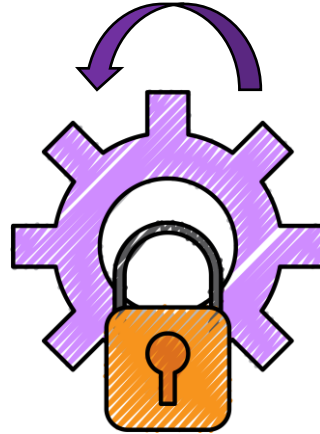
Empfänger



Entschlüsseln

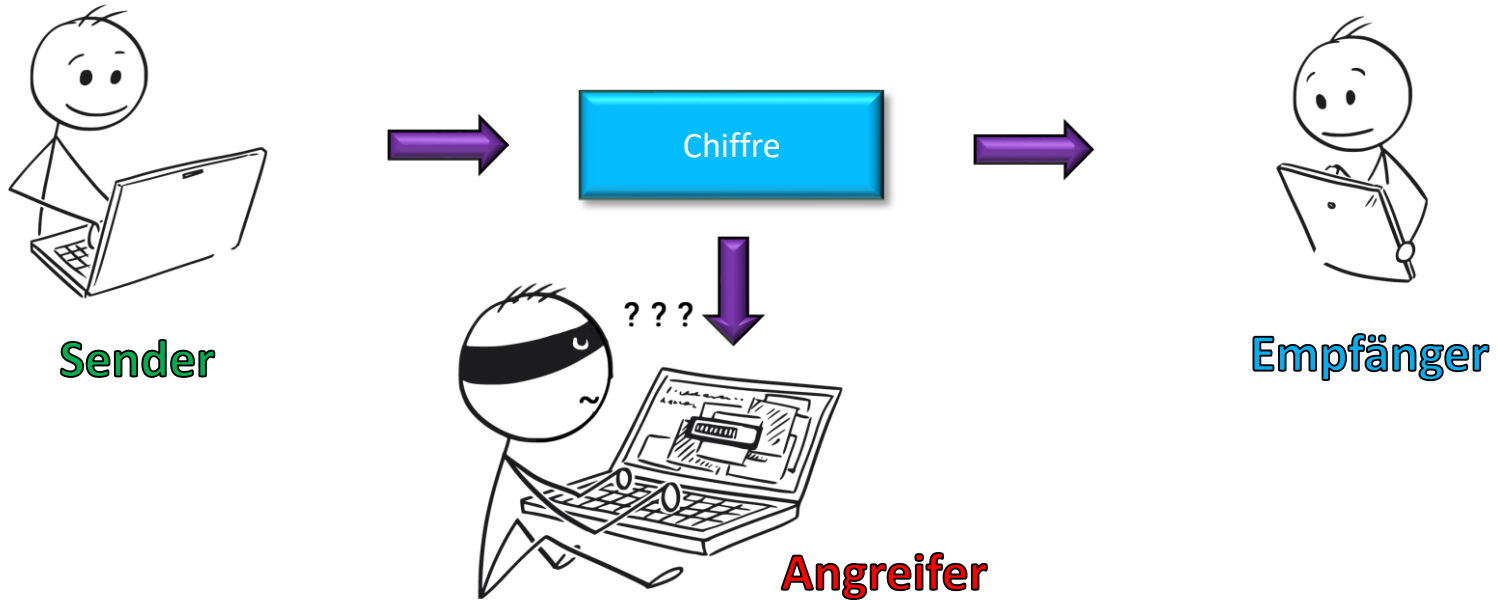


Angreifer



Entschlüsseln

Situation



Zusammenfassung

