Leibniz Gemeinschaft

IPN
Leibniz-Institut für die Pädagogik der Naturwissenschaften und Mathematik

Einführung: Kryptographie

Was ist Kryptographie?

- **Ver-** und **Entschlüsseln** von Nachrichten
- Eine unbefugte Person kann eine Nachricht lesen, soll sie aber nicht verstehen können.
- Sender und Empfänger besitzen Schlüssel

Wo begegnen euch Verschlüsselungen im Alltag?

- Whats-App 

Wo begegnen euch Verschlüsselungen im Alltag?

- Whats-App 
- Browser 

Wo begegnen euch Verschlüsselungen im Alltag?

- Whats-App 
- Browser 

- Internet (LogIn)

Wo begegnen euch Verschlüsselungen im Alltag?

- Whats-App 
- Browser 

- Internet (LogIn)
- W-LAN 

Wo begegnen euch Verschlüsselungen im Alltag?

- Whats-App 
- Browser 

- Internet (LogIn)
- W-LAN 

- E-Mail 

Was muss geschützt werden?

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

Kennt ihr bereits Verschlüsselungen?

- Skytale
- Cäsar
- Enigma

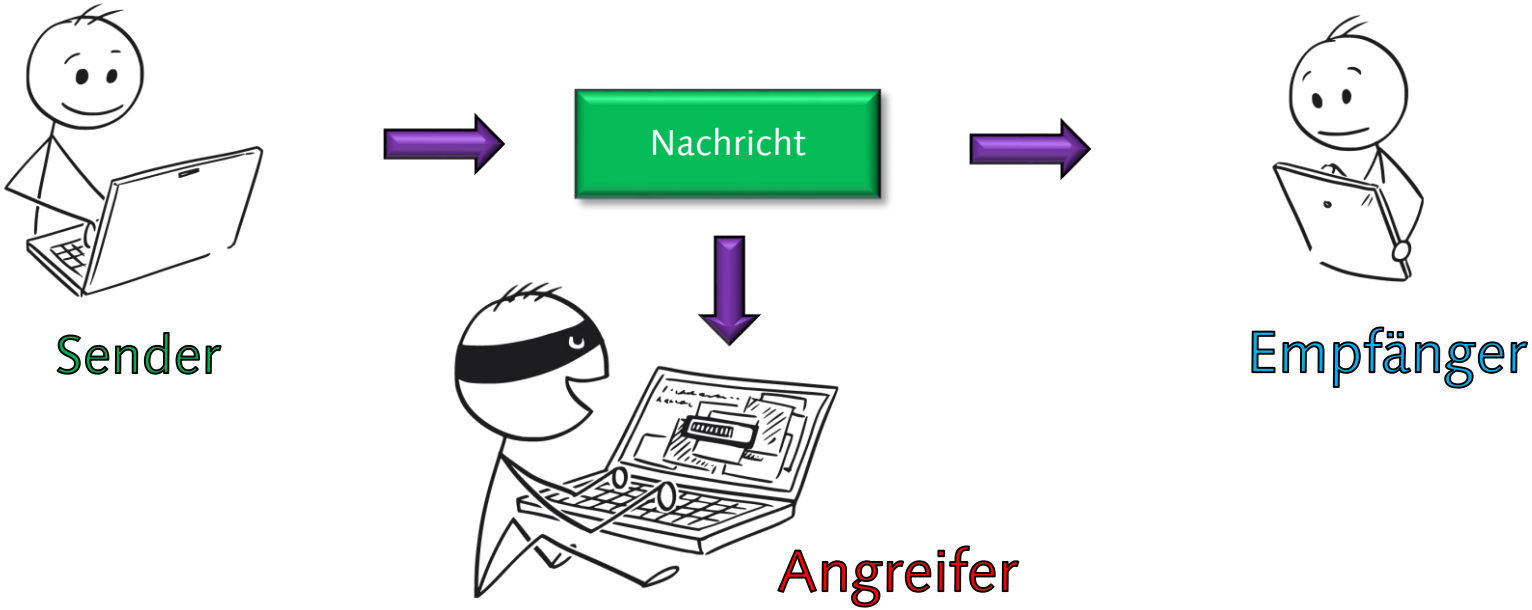
Was ist Kryptographie nicht?

- Verstecken von Nachrichten (Steganograhpie)
- Übersetzen von Nachrichten (Codierungstheorie)

Was ist Kryptographie?

Sender möchte Empfänger eine Nachricht schicken, die ein Unbefugter zwar lesen, aber nicht verstehen kann.

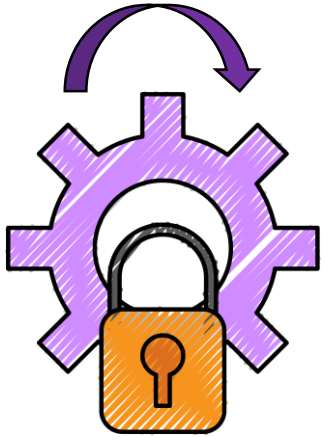
Kommunikations-Modell



Sender

Klartext

Schlüssel

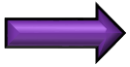


Chiffre

Verschlüsseln

Kommunikations-Modell

Sender

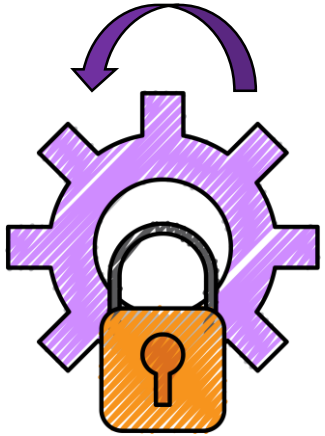


Empfänger

Empfänger

Chiffre

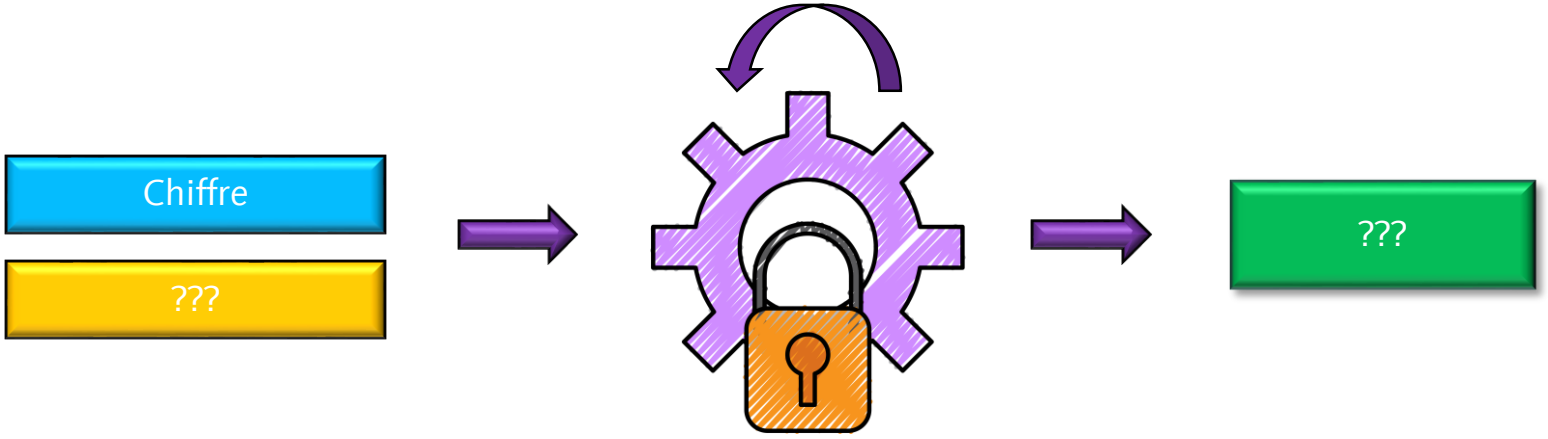
Schlüssel



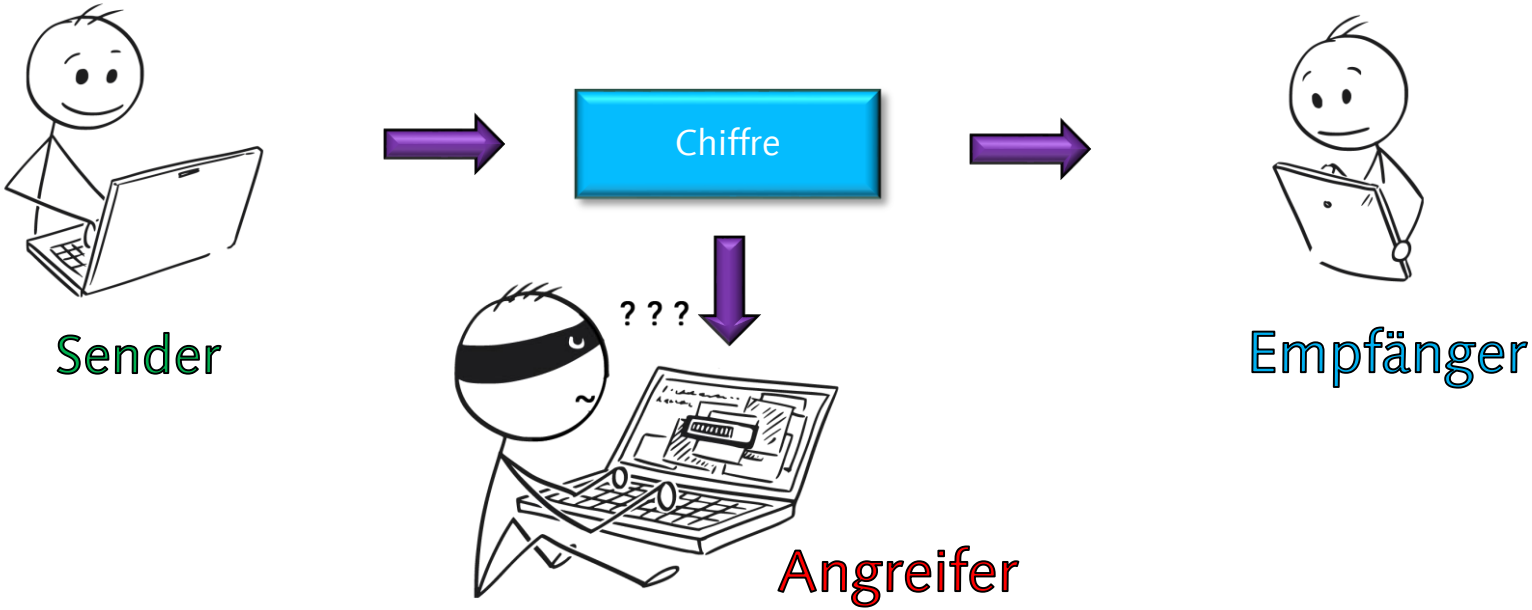
Entschlüsseln

Klartext

Angreifer



Kommunikations-Modell



Sicherheit

Um beurteilen zu können, wie **sicher** eine Verschlüsselung ist, müssen wir die Rolle eines Angreifers einnehmen.

Verwendete Begriffe

- Kryptographie
- Entschlüsselung
- Schlüssel
- Chiffre
- Verschlüsselung
- Nachricht
- Schlüsselraum
- Verschlüsselung knacken

Kryptographie

Wissenschaft der Ver-/ und Entschlüsselung von Informationen.

Verschlüsseln

Macht aus Klartext und Nachricht ein verschlüsselten Text. Dieser soll ohne Schlüsseln nicht „verstehbar“ sein.

Entschlüsseln

Macht aus verschlüsselter Nachricht und Schlüssel den Klartext.

Nachricht

Informationen, die vom Sender zum Empfänger gelangen sollen.

Klartext

Die unverschlüsselte Nachricht.

Chiffre

Die verschlüsselte Nachricht.

Schlüssel

Geheime Information, die nur Sender / Empfänger bekannt sind. Wird benötigt um Ver-/ bzw. Endschlüsseln zu können.

Schlüsselraum

Sammlung aller Schlüssel, die bei einer konkreten Verschlüsselung benutzt werden können.

Verschlüsselung knacken

Versuch eines Unbefugten, den Klartext zu gewinnen, ohne den Schlüssel zu kennen.