# Kryptographie

## Handbuch

# Glossar

| | |
|---|---|
| **Kryptographie** | Wissenschaft der Ver-/ und Entschlüsselung von Informationen. |
| **Verschlüsselung** | Macht aus Klartext und Nachricht einen verschlüsselten Text. Dieser soll ohne Schlüssel nicht „verstehbar“ sein. |
| **Entschlüsseln** | Macht die Verschlüsselung rückgängig, also 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. |
| **Verschlüsselung knacken** | Versuch eines Unbefugten, den Klartext zu gewinnen, ohne den Schlüssel zu kennen. |

# Cäsar-Scheibe

## Verschlüsseln

**(Klartext → Chiffre)**

- Stelle den **Schlüssel** auf der Cäsar-Scheibe ein.
- Außen: **Klartext**-Alphabet
- Innen: **Chiffre**-Alphabet
- Lese auf der Cäsar-Scheibe, für jeden **Klartext**-Buchstaben (**außen**) den **Chiffre**-Buchstaben (**innen**) ab.

## Entschlüsseln

**(Chiffre → Klartext)**

- Stelle den **Schlüssel** auf der Cäsar-Scheibe ein.
- Außen: **Klartext**-Alphabet
- Innen: **Chiffre**-Alphabet
- Lese auf der Cäsar-Scheibe, für jeden **Chiffre**-Buchstaben (**innen**) den zugehörigen **Klartext**-Buchstaben (**außen**) ab.

# Vigenère-Tabelle

## Verschlüsseln

**(Klartext → Chiffre)**

- Trage die **Nachricht** in die Nachrichten-Zeile ein.
- Trage den **Schlüssel** in die Schlüssel-Zeile ein

  (so oft hintereinander, dass jedem Buchstaben der Nachricht ein Schlüssel-Buchstaben zugeordnet ist)
- Übersetze jede einzelne Position mit Hilfe der Tabelle (Spalte: **Nachricht**, Zeile: **Schlüssel**, Schnittpunkt: **Chiffre**,

  finde den Schnittpunkt von Nachricht und Passwort)
- Trage das **Ergebnis** in die Chiffre-Zeile ein.

## Entschlüsseln

**(Chiffre → Klartext)**

- Trage den **Chiffre**-Text in die Chiffre-Zeile ein.
- Trage den **Schlüssel** in die Schlüssel-Zeile ein

  (so oft hintereinander, dass jedem Buchstaben der Nachricht ein Schlüssel-Buchstaben zugeordnet ist)
- Übersetze jede einzelne Position mit Hilfe der Tabelle (Spalte: **Nachricht**, Zeile: **Schlüssel**, Schnittpunkt: **Chiffre**,

  finde die Spalte, deren Schnittpunkt mit dem Schlüssel der Chiffre-Buchstabe ist)
- Trage das **Ergebnis** in die Nachricht-Zeile ein.

# Skytale

## Verschlüsseln

**(Klartext → Chiffre)**

- Wähle einen **Zylinder** aus, dieser ist der **Schlüssel**.
- Wickel einen Papierstreifen um den **Zylinder**.
- **Beschrifte den Papierstreifen entlang der Längsachse**
- Wickel den Streifen vom **Zylinder** ab, die Buchstaben sind in **vertauschter Reihenfolge**.

## Entschlüsseln

**(Chiffre → Klartext)**

- Wähle den richtigen **Zylinder** aus.
- Wickel den **beschrifteten Papierstreifen** um den **Zylinder**.
- **Lese die Nachricht entlang der Längsachse ab**.