**Übersicht**

* Sicherheitsziele:  
  Liste von gängigen Sicherheitszielen und Beispiele, bei denen Sicherheitsziele eine Rolle spielen.
* Als Hilfsmittel für die folgenden Beispiele sind je nach Vorgehensweise die Software [Cryptool](https://www.cryptool.org/de/), [Cryptool 2](https://www.cryptool.org/de/cryptool2) oder [JCryptool](https://www.cryptool.org/de/jcryptool). Im Folgenden wurde in der Regel Cryptool 2 verwendet.
* Cäsar bzw. Rotation:  
  Beispiele für
  + Cäsar: Verschlüsselung   
    Alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ  
    => 25 mögliche Schlüssel (1 bis 25)  
    Klartext frei wählbar.

Dateiname: Caesar.cwm

* + Cäsar: Entschlüsselung per Exhaustionsmethode (Brute-Force)  
    Alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz:.'  
    => 55 verschiedene Schlüssel  
    verschlüsselter Klartext:   
    ZweitesKerkhoffs’sches Prinzip: Das System darf keine Geheimhaltung erfordern.  
    vorhandener Geheimtext: zTBFQBPkBOHELCCPP'EBPpOFKWFMXd:PsVPQBJA:OCHBFKBgBEBFJE:IQRKDBOCLOABOKY  
    Verwendeter Schlüssel: 26

Dateiname: Caesar\_Angriff.cwm

* Transposition:
  + Simulation der Verschlüsselung

Alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ  
Schlüsselwort: INFO

Dateiname: Transposition\_Chriffrierung\_Simulation.cwm

* + Simulation der Entschlüsselung  
    Alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ  
    Schlüsselwort: INFO  
    Dateiname: Transposition\_Dechiffrierung\_Simulation.cwm
* Monoalphabetische Substitution
  + Veranschaulichung Chiffrierung  
    Dateiname: MonoalphabetischeSubstitution\_mit\_Password.cwm
  + Veranschaulichung Dechiffrierung

Dateiname: MonoalphabetischeSubstitution\_mit\_Password\_Entschlüsseln.cwm

* + Häufigkeitsanalyse  
    Die Häufigkeitsanalyse liefert eine Hilfestellung, aber ist nicht eindeutig. Möchte man eine Hilfestellung geben, kann man das erste Wort angeben: Argumentieren (Known-Plain-Text)  
    Passwort: PROGRAMMIERSPRACHE
  + Textdateien: Langer\_Klartext.txt, Langer\_Klartext\_UPPERCASE.txt, VerschlüsselterLangerText.txt
  + Beispieltext für ungünstige Häufigkeitsverteilung:  
    Dateiname: Text\_X\_ungünstigeHäufigkeiten.txt
* Vigenère / Polyalphabetische Substitution
  + Beispiel-Datei zur Ver- und Entschlüsselung:  
    Dateiname: vigenere\_Beispiel.cwm
  + Angriff auf Vigenère (JCryptool):  
    Der Angriff auf einen Vigenère-verschlüsselten Text kann interaktiv mit dem JCryptool durchgeführt werden. Dafür sind diese Dateien geeignet  
    Passwort: AbiturKlausur  
    Dateinamen: LangerNormalerText\_gefiltert\_A-Za-z.txt, LangerNormalerText\_gefiltert\_A-Za-z\_Chiffriert.txt
  + Angriff auf Vigenère (Cryptool2)  
    Passwort: ABITUR  
    Dateinamen: vigenere\_Angriff.cwm, LangerNormalerText\_gefiltert\_A-Z.txt, LangerNormalerText\_gefiltert\_A-Z\_Chiffriert.txt
  + One-Time-Pad

Geheimtext: WQLATIMOQV  
Bekannter Teil des Schlüssels: \_ \_ \_ \_ \_ WMVIL

Erraten des Klartextes ergibt mehrere Möglichkeiten, z.B.:  
MATHEMATIK, INFORMATIK, EMBLEMATIK, Hydromatik, Informatik, Mathematik, Melismatik, Numismatik, Phonematik

* Asymmetrische Verschlüsselungsverfahren:
  + RSA: Das RSA-Verfahren kann zwar anschaulich mit dem JCryptool dargestellt werden, allerdings findet dich Verschlüsselung nicht blockweise sondern Buchstabenweise statt. Damit ist das RSA-Verfahren, wie es im JCryptool implementiert ist, nicht sicherer als eine monoalphabetische Substitutionschiffre  
    Dateinamen: RSA\_Entschlüsselung.cwm, RSA\_Verschlüsselung.cwm
  + Der Diffie-Hellman-Schlüsseltausch kann mit dem JCryptool visualisiert werden.