Kryptographie (Teil 1) **Stoffumfang**

Seiten 1–5:

- Du kannst die Hauptaufgaben der Kryptographie aufzählen.
- Du kannst die Situation, in der die (klassische) Kryptographie stattfindet, mit den entsprechenden Fachbegriffen (Geheimtext, Klartext, Verschlüsselungsfunktion $c = E_k(m)$, Entschlüsselungsfunktion $m = D_k(c)$) graphisch oder sprachlich beschreiben.
- Du kannst das Prinzip von Kerckhoffs beschreiben.
- Du kannst beschreiben, worum es bei der Kryptoanalyse und bei den einzelnen Angriffszenarien geht.
- Du kannst eine Antwort auf die Frage geben, was symmetrische Verschlüsselungsverfahren sind.
- Du kannst die folgenden symmetrischen Verschlüsselungsverfahren an einfachen Beispielen durchführen und ihre Vor- und Nachteile aufzählen.
  - Cäsar-Chiffre
  - Monalphabetische Verschlüsselung
  - Verschlüsselung nach DE VIGENÈRE
  - One Time Pad

Seiten 9–14:

- Du kannst überprüfen, ob eine Kongruenz $a \equiv b \pmod{n}$ wahr ist.
- Du kannst mit Restklassen moduolo n rechnen. (Das ist dasselbe wie mit dem %-Operator in Python oder anderen Programmiersprachen.)
- Du kannst die additive und multiplikative Verknüpfungstafeln für die Restklassenmenge $\mathbb{Z}_n$ aufstellen.
- Du kannst beurteilen, ob eine Restklassenmenge $\mathbb{Z}_n$ zusammen mit der jeweiligen Verknüfpung ($+$ oder $\times$) eine sogenannte Gruppe ist.

  Eine Gruppe G ist eine Menge, auf der eine abgeschlossene Verknüpfung definiert ist, die folgende Eigenschaften hat:

  - Für alle a, b, $c \in G$ gilt: $(a * b) * c = a * (b * c)$ (Assoziativität)
  - Es gibt ein Element $e \in G$ mit der Eigenschaft, dass $a*e = e*a = a$ für alle $a \in G$. (neutrales Element)
  - Zu jedem $a \in G$ gibt es ein $a' \in G$ mit $a * a' = a' * a = e$. (inverses Element)

  Gilt zudem für alle a, $b \in G$, dass $a * b = b * a$, so ist G eine *abelsche Gruppe*.
- Du kannst zu einer „kleinen“ natürlichen Zahl n die Verknüfpungstafel der Gruppe der primen Restklassen $\mathbb{Z}_n^*$ aufstellen.

- Du kannst beschreiben, wann eine Gruppe *zyklisch* ist und was ein *erzeugendes Element* ist.
- Du kannst überprüfen, ob ein Element in $\mathbb{Z}_n$ bzw. $\mathbb{Z}_n^*$ erzeugend ist.
- Du kannst für (noch) nicht zu grosse natürlichen Zahlen n den Wert der Eulerschen Phi-Funktion $\varphi(n)$ bestimmen.