Caesar Verschlüsselung

Der römische Feldherr Julius Cäsar (100 bis 44 v.Chr.) verschlüsselte seine geheimen Nachrichten, indem er jeden Buchstaben durch einen anderen ersetzte. Dabei wurde der Buchstabe immer durch den um eine bestimmte Anzahl von Stellen im Alphabet verschobenen Buchstaben ersetzt. Die Anzahl der Stellen ist der Schlüssel. Ein solches Verschlüsselungssystem wird monoalphabetische Verschlüsselung genannt.

Ein Beispiel für den Schlüssel 3 (Verschiebung um 3 Stellen):

```
Klar:     a b c d e f g h i j k l m n o p q r s t u v w x y z
          | | | | | | | | | | | | | | | | | | | | | | | |
Geheim:   D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
```

Aus dem Klartext „mathematik“ wird somit der Geheimtext „PDWKHPDWLN“.

Aufgabe 1. Leon Battista Alberti vereinfachte das Caesar Verfahren im 15. Jahrhundert durch die Entwicklung der Chiffrierscheibe. Bastle dir eine eigene Caesar Verschlüsselungs-Scheibe. Sie wird für die folgenden Aufgaben hilfreich sein.

Aufgabe 2. Die Caesar Verschlüsselung musste zur Zeit ihrer Entwicklung noch manuell angewandt werden. Verschlüssle den Text "Strenggeheim" mit der "Caesar-Verschlüsselung", indem du eine Verschiebung von 10 Zeichen verwendest (dh. aus A wird K etc.)

Aufgabe 3. Caesar Codebreaker: Versuche den Text zu entschlüsseln. Beschreibe, wie du bei dem Knacken vorgegangen bist.

Aufgabe 4. Untersuche, wie oft welcher Buchstabe im verschlüsselten Text der Aufgabe 3 vorkommt. Erkläre, wie diese Information beim Knacken der Verschlüsselung benutzt werden kann.