Aufgabe 1.1

Zähle die Hauptaufgaben der Kryptographie auf und beschreibe jeweils in knappen Sätzen, worum es dabei geht.

Aufgabe 1.2

Was besagt das Prinzip von *Kerckhoffs*?

Aufgabe 1.3

Was bedeutet der Ausdruck *Kryptoanalyse*?

Aufgabe 1.4

Welche der folgenden Situationen liegt vor?

- Known Ciphertext (KC)
- Known Plaintext (KP)
- Chosen Plaintext (CP)

(a) Es steht das Verschlüsselungsverfahren zur Verfügung.

(b) Es steht ein Stück Geheimtext zur Verfügung.

(c) Es steht ein Stück Klartext und das dazu gehörende Stück Geheimtext zur Verfügung.

Aufgabe 2.1

Was ist ein symmetrisches Verschlüsselungsverfahren?

Aufgabe 2.2

Auf wie viele Arten können die 26 Zeichen des lateinischen Alphabets permutiert, d. h. umkehrbar eindeutig auf sich abgebildet werden?

Aufgabe 2.3

Dechiffriere den Geheimtext

```
HLQ XKU EHLP NROOHJL
```

wenn du weisst, dass die Verschlüsselung mit dem Cäsar-Verfahren durchgeführt wurde und der Text etwas mit dem Gymnasium in Stans zu tun hat.

Aufgabe 2.5

Warum ist eine monoalphabetische Verschlüsselung unsicher?

Aufgabe 2.6

Verschlüssle den Klartext `KAFFEE` mit der Vigenère-Verschlüsselung und dem Schlüssel `GEHEIM`. Verwende dazu das Vigenère-Quadrat.

Aufgabe 2.7

Wie kann man versuchen, die Schlüssellänge des Vigenère-Verfahrens zu bestimmen?

Aufgabe 2.8

Wie kann ein Vigenère-Chiffrierter Text entschlüsselt (geknackt) werden, wenn die Schlüsselwortlänge n bekannt ist?

Aufgabe 2.9

(a) Nenne mindestens einen wesentlichen Nachteil des One Time Pad-Verfahrens?

(b) Wovon hängt die Sicherheit des One Time Pad-Verfahrens ab?

Aufgabe 3.1

Wahr oder falsch?

(a) $113 \equiv 17 \mod 8$

(b) $-352\,989 \equiv 724\,692 \mod 2$

(c) $107\,032 \equiv 0 \mod 3$

Aufgabe 3.2

Berechne das Resultat in der Restklassenmenge $\mathbb{Z}_9$, sofern es überhaupt definiert ist. Die Kennzeichnung der Restklassen kann weggelassen werden.

(a) $7 + 6$

(b) $5 - 8$

(c) $3 \cdot 7$

(d) $1 : 4$

(e) $5 : 6$

(f) 3^{29}

Aufgabe 3.3

Berechne $(25 \cdot 13 + 44 \cdot 8) \mod 7$.

Aufgabe 3.4

Stelle die Verknüpfungstafeln für $(\mathbb{Z}_4, +)$ und $(\mathbb{Z}_4, \times)$ auf.

Aufgabe 3.5

Handelt es sich bei der Menge zusammen mit der angegebenen Verknüpfung um eine Gruppe?

(a) $(\mathbb{Z}_8, +)$

(b) $(\mathbb{Z}_5, \times)$

(c) $(\mathbb{Z}_7 \setminus \{0\}, \times)$

(d) $(\mathbb{Z}_6 \setminus \{0\}, \times)$

Aufgabe 3.6

Stelle die Verknüpfungstafel für die prime Restklassengruppe $\mathbb{Z}_{12}^*$ auf.

Aufgabe 3.7

Überprüfe, ob das Element g die Gruppe $(G, *)$ erzeugt.

(a) $g = 3$, $(\mathbb{Z}_4, +)$ (b) $g = 2$, $(\mathbb{Z}_6, \times)$ (c) $g = 4$, $(\mathbb{Z}_5^*, \times)$

Aufgabe 3.8

Bestimme den Wert der Eulerschen φ-Funktion:

(a) $\varphi(8)$ (b) $\varphi(11)$ (c) $\varphi(24)$ (d) $\varphi(47)$