

Verfahren und Prinzipien der Kryptographie

Die Menschen verwenden schon seit ca. 2500 Jahren Geheimschriften, um geheime Botschaften zu versenden. Vielleicht kennen Sie Geheimschriften aus Detektivgeschichten oder aus dem Unterricht in früheren Jahrgängen.

Aufgabe 1:

- Sammeln Sie an der Tafel oder mit einem kollaborativen Werkzeug Geheimschriften, die Sie kennen oder die Sie sich selbst ausgedacht haben.
- Testen Sie, ob alle Beispiele zur Geheimhaltung einer Nachricht geeignet sind. Achten Sie dabei auf folgende Dinge:
 - Kann der Empfänger der geheimen Botschaft die Nachricht lesbar machen? Was muss er dazu wissen?
 - Kann ein Spion, der die Nachricht abfängt, die geheime Botschaft lesen?
- Wenn Sie bereits Codierungsverfahren wie den ASCII-Code oder RGB-Werte für die Codierung von Farben kennengelernt haben, vergleichen Sie diese mit Ihren Beispielen für Geheimschriften. Begründen Sie, warum sich der ASCII-Code nicht als Geheimschrift eignet.
- Vergleichen Sie die Verfahren, die Sie gesammelt haben, untereinander und teilen Sie sie in Kategorien ein.

Im Laufe der Zeit wurden viele verschiedene Geheimschriften entwickelt. Bei einem Großteil davon handelt es sich um Verschlüsselungsverfahren. Die Wissenschaft, die sich mit der Entwicklung von Verschlüsselungsverfahren beschäftigt, ist die **Kryptographie**. Dabei kommen seit Jahrhunderten immer wieder die gleichen Prinzipien zum Einsatz. Das gilt auch für die modernen Verschlüsselungsverfahren, die uns heute eine sichere, geheime Kommunikation im Internet ermöglichen.

Im Folgenden erhalten Sie einen Überblick über zentrale Begriffe und Prinzipien der Kryptographie.

Wichtige Begriffe aus Codierung und Kryptographie

Bei der **Codierung** wird die Darstellung einer Nachricht bzw. eines Textes verändert. Es gibt unterschiedliche Gründe für eine solche Transformation. Computer beispielsweise arbeiten mit Nullen und Einsen, während Menschen lieber Buchstaben und die Ziffern von Null bis Neun lesen. Jedem Zeichen muss daher eine Darstellung aus Nullen und Einsen zugeordnet werden. Blinde Menschen können Buchstaben nicht sehen, sondern nur ertasten. Dafür wurde die Braille-Schrift erfunden. Die Regeln für die Transformation sind in diesen Fällen allgemein bekannt, so dass jeder die ursprüngliche Darstellung wiederherstellen kann.

Bei anderen Codierungen ist das Ziel die Geheimhaltung der Nachricht. Mit diesen speziellen Codierungsverfahren beschäftigt sich die **Kryptographie**. Auch bei diesen Verfahren wird die Darstellung der Nachricht verändert. Im Gegensatz zum ASCII-Code oder der Braille-Schrift wird bei der Transformation jedoch eine geheime Information verwendet. Nur wer über diese geheime Information verfügt, kann die ursprüngliche Darstellung der Nachricht wiederherstellen und sie lesen. Die geheime Information bezeichnet man als **Schlüssel**. Beim Umwandeln der Darstellung der Nachricht mithilfe des Schlüssels spricht man daher auch von **verschlüsseln** bzw. **entschlüsseln**. Die für jeden lesbare Nachricht wird als **Klartext** bezeichnet, die verschlüsselte Nachricht als **Geheimtext**.

In der Kryptographie unterscheidet man zwei Prinzipien. Die **Transposition** und die **Substitution**. Bei der **Transposition** werden die Zeichen selbst nicht verändert, es werden nur die Positionen nach einem geheimen Muster vertauscht, so dass die Nachricht nicht mehr lesbar ist. Bei der **Substitution** bleibt jedes Zeichen an seinem Platz. Es wird jedoch durch ein anderes geheimes Zeichen ersetzt. Man spricht daher von **Klartextalphabet** und **Geheimtextalphabet** bzw. von **Klartextzeichen** und **Geheimtextzeichen**. Wenn beim Erstellen eines Geheimtextes genau eine Zuordnung zwischen Klartext- und Geheimtextalphabet verwendet wurde, spricht man von **monoalphabetischer Substitution**.

Einen Geheimtext ohne Kenntnis des Schlüssels lesbar zu machen, bezeichnet man umgangssprachlich als **knacken**. Mit der Frage, wie sicher ein Verfahren ist und ob man es knacken kann, beschäftigen sich die **Kryptoanalytiker**. Die entsprechende Wissenschaft nennt sich **Kryptoanalyse**. Über die Vorgehensweise der Kryptoanalytiker lernen Sie später noch mehr.

Die Bereiche Kryptographie und Kryptoanalyse fasst man unter dem Begriff **Kryptologie** zusammen. Neben der Verschlüsselung gibt es noch die Möglichkeit eine Nachricht zu verstecken. Die Nachricht ist dabei ohne Kenntnis eines Schlüssels lesbar. Aber nur, wenn man weiß, wo man sie suchen muss. Diese Art der Geheimhaltung bezeichnet man als **Steganographie**.

Eine Übersicht über die Zusammenhänge der Verfahren und Prinzipien im Bereich der Kryptologie zeigt Abbildung 1.

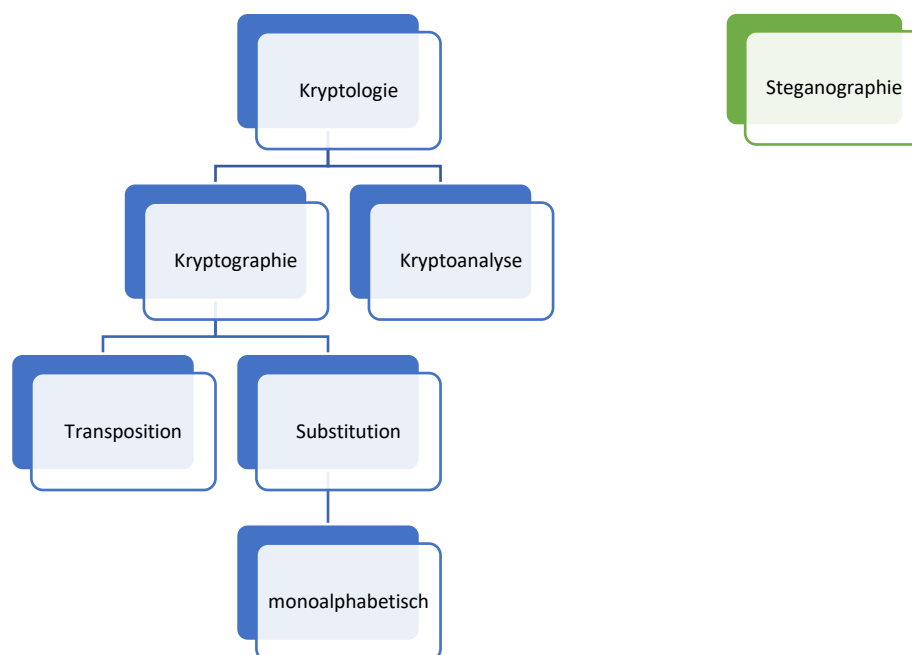
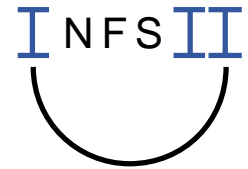


Abbildung 1: Übersicht Kryptologie

Aufgabe 2:

- Untersuchen Sie, in welche Kategorie, sich die Beispiele, die Sie gesammelt haben, jeweils einordnen lassen. Ergänzen Sie ggf. weitere Beispiele, so dass Sie zu den Prinzipien Transposition und Substitution mindestens zwei verschiedene Verfahren beschreiben können.
- Geben Sie für die Beispiele, bei denen es sich um Verschlüsselungsverfahren handelt, den Schlüssel an.



Dieses Werk ist lizenziert unter einer [Creative Commons Namensnennung - Nicht-kommerziell - Weitergabe unter gleichen Bedingungen 4.0 International Lizenz](https://creativecommons.org/licenses/by-nc-sa/4.0/). Sie erlaubt Bearbeitungen und Weiterverteilung des Werks unter Nennung meines Namens und unter gleichen Bedingungen, jedoch keinerlei kommerzielle Nutzung.