

Verfahren und Prinzipien der Kryptographie

Geheimschriften

Wolltest du schon einmal jemandem ein Geheimnis mitteilen, ohne dass jemand anderes davon erfährt? Wie hast du das gemacht? Vielleicht habt ihr euch heimlich getroffen und nur im Flüsterton gesprochen? Manchmal ist das nicht möglich und man muss die Nachricht aufschreiben. Dann kann man versuchen die Nachricht so aufzuschreiben, dass nur derjenige, für den das Geheimnis bestimmt ist, die Nachricht lesen kann.

Aufgabe 1:

- a) Erstellt in Partnerarbeit ein Poster zu einer Geheimschrift, die ihr kennt oder die ihr euch selbst ausgedacht habt.
- b) Probiert verschiedene Geheimschriften, die auf den Postern dargestellt sind, aus. Achtet 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?

Die Menschen versuchen schon seit tausenden von Jahren ihre Nachrichten geheim zu halten. Geheime Botschaften spielen oft eine Rolle in kriegerischen Auseinandersetzungen. Aber auch die Prinzessin, die sich in einen einfachen Jungen aus dem Volk verliebt hat, musste vielleicht geheim kommunizieren, weil die Eltern damit nicht einverstanden waren. Früher wurden die Nachrichten von einem Boten überbracht. Heute versenden wir unsere Nachrichten meist über das Internet. Aber das Problem ist gleichgeblieben. In beiden Fällen gibt es Lauscher und Spione, die die Nachrichten eventuell mitlesen.

Deshalb hat sich über die Jahre eine Wissenschaft entwickelt, die sich mit der Geheimhaltung von Nachrichten beschäftigt: die **Kryptographie**

Im Laufe der Zeit wurden viele verschiedene Verfahren entwickelt. Dabei kommen jedoch immer wieder die gleichen Prinzipien zum Einsatz. Das gilt auch für die modernen Verschlüsselungsverfahren, die uns heute eine sichere, geheime Kommunikation im Internet ermöglichen.

Aufgabe 2: Vergleicht die Verfahren, die ihr auf euren Postern dargestellt habt. Welche Gemeinsamkeiten und welche Unterschiede könnt ihr erkennen? Lassen sich die Verfahren in Kategorien einteilen?

Der folgende Text gibt euch einen Überblick über zentrale Begriffe und Vorgehensweisen 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 zu den eingangs beschriebenen Beispielen 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**.

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 lernst du 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 dir Abbildung 1.

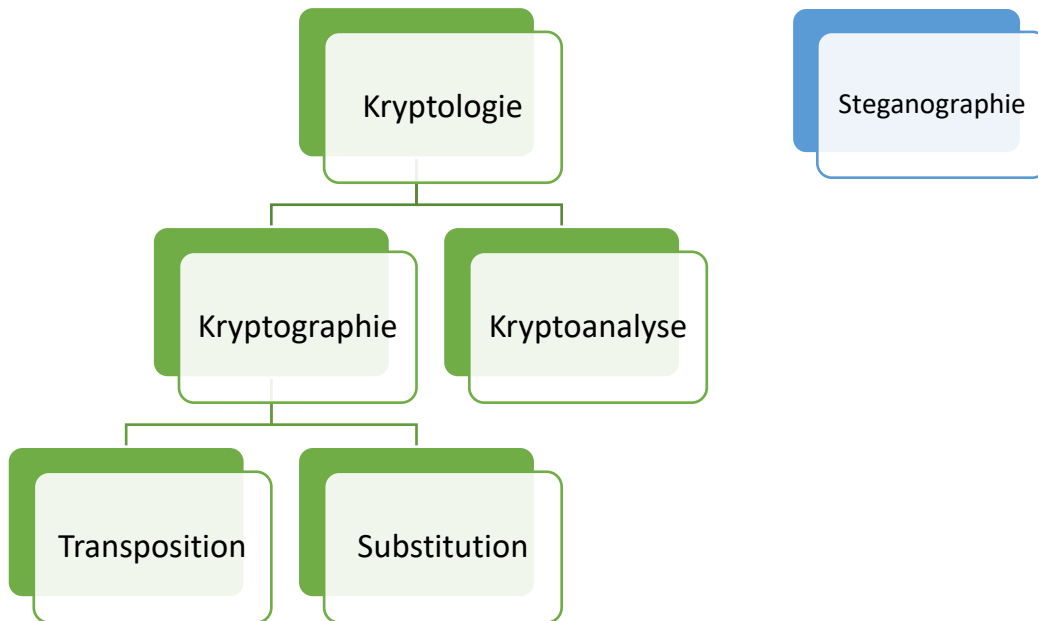


Abbildung 1: Zusammenhang zwischen den Verfahren und Prinzipien der Kryptologie

Aufgabe 3: Untersucht für jedes Verfahren auf euren Postern die folgenden Punkte:

- Handelt es sich bei dem Verfahren um eine allgemein bekannte Codierung, eine Verschlüsselung oder ein steganographisches Verfahren. Diskutiert jeweils, wie gut das Verfahren zur Geheimhaltung geeignet ist.
- Welches ist bei den Verschlüsselungsverfahren die geheime Information, die den **Schlüssel** darstellt?
- Handelt es sich bei den Verschlüsselungsverfahren um eine **Transposition** oder eine **Substitution**?

Dieses Werk ist lizenziert unter einer [Creative Commons Namensnennung - Nicht-kommerziell - Weitergabe unter gleichen Bedingungen 4.0 International Lizenz](#). Sie erlaubt Bearbeitungen und Weiterverteilung des Werks unter Nennung meines Namens und unter gleichen Bedingungen, jedoch keinerlei kommerzielle Nutzung.