

Kryptologie in der Einführungsphase

Didaktische Hinweise

Zielgruppe & Voraussetzungen

Die Materialien zur Kryptologie richten sich an Schüler*innen in der Einführungsphase.

Für die Abgrenzung der Verschlüsselung gegen allgemein bekannte Codierungsverfahren, wie dem ASCII-Code, ist es hilfreich, wenn die Kompetenz „Die Schülerinnen und Schüler beschreiben grundlegende Codierungen von Daten, u. a. Dualzahlen, ASCII, RGB-Modell“ bereits erworben wurde.

Für die Implementierung des Caesar-Verfahrens muss das Entwerfen und Implementieren von Algorithmen unter Verwendung elementarer Zeichenkettenoperationen beherrscht werden.

Weiterhin ist im Zusammenhang mit der Häufigkeitsanalyse die Implementierung eines Textanalysetools vorgesehen. Dafür ist auch das Erstellen eigener Operationen hilfreich.

Die entsprechenden algorithmischen Konzepte können entweder im Vorfeld, parallel oder im Anschluss erarbeitet werden. In jedem Fall sind die Verfahren der Kryptologie als Kontext für die zeichenweise Verarbeitung von Zeichenketten vorgesehen.

Die Materialpakete mit den Leitfäden zur zeichenweisen Verarbeitung von Zeichenketten in Snap! bzw. Processing enthalten entsprechende Aufgaben aus dem Kontext der Kryptographie, insbesondere zur Implementierung des Caesar-Verfahrens, so dass diese gut in Kombination mit diesem Materialpaket eingesetzt werden können. Ein möglicher Ablauf wird weiter unten vorgestellt.

Lernziele

Anhand der vorliegenden Materialien können die folgenden Kompetenzen aus dem Modul *Kryptologie* im Lernfeld *Informationen und Daten* des niedersächsischen Kerncurriculums für die gymnasiale Oberstufe¹ erworben werden.

Die Schülerinnen und Schüler ...

- beschreiben das Prinzip der Transposition und Substitution zur Verschlüsselung von Daten.
- erläutern das Prinzip der Häufigkeitsanalyse.
- beurteilen die Sicherheit einfacher Verschlüsselungsverfahren.

Neben dem Beschreiben und Erläutern der Prinzipien sehen die Materialien auch die Anwendung entsprechender Verfahren vor, sowohl aus Sicht des Kryptographen als auch aus Sicht des Kryptoanalytikers. Insbesondere bei der Häufigkeitsanalyse wird das Vorgehen mit seinen Möglichkeiten aber auch Schwierigkeiten erst beim Durchführen transparent.

Außerdem sind die Materialien so angeordnet, dass die Schüler*innen die Möglichkeit haben, zumindest im Ansatz die schrittweise Verbesserung der Substitutionsverfahren als Resultat des Wettlaufs zwischen Kryptographie und Kryptoanalyse nachzuvollziehen. Auf die polyalphabetische Verschlüsselung am Beispiel des Vigenère-Verfahrens wird hier verzichtet, da dies im KC erst für die Qualifikationsphase vorgesehen ist. Ein entsprechender Ausblick wäre hier aber passend.

¹ Niedersächsisches Kultusministerium (Hrsg.) (2017) *Kerncurriculum für das Gymnasium – gymnasiale Oberstufe, die Gesamtschule – gymnasiale Oberstufe, das Kolleg. Informatik*. Hannover: unidruck

Die Kompetenz „Die Schülerinnen und Schüler implementieren monoalphabetische Verfahren, u. a. Caesar-Verfahren.“ wird im Rahmen des Materialpakets zur zeichenweisen Verarbeitung von Zeichenketten erarbeitet.

Mögliche Abfolge der Materialien

- AB01_Einstieg_Kryptographie
- AB02: Caesar-Verfahren
- *Exkurs: Zeichenweise Verarbeitung von Zeichenketten (gesondertes Materialpaket) inkl. Implementierung von Caesar*
- AB03_Textanalysetool, ggf. mit Exkurs zu eigenen Operationen
- AB04_MonoalphabetischeSubstitution
- AB05_Häufigkeitsanalyse

Die kursiv geschriebenen Punkte können ggf. auch erst im Anschluss erfolgen.

Didaktische Anmerkungen zu den Arbeitsblättern

Für eine digitale Beispielsammlung in AB01 bietet sich z. B. das kollaborative Werkzeug <https://flinga.fi/tools> an². Ziel des AB01 ist, dass die Prinzipien Transposition und Substitution an verschiedenen Beispielen deutlich werden und ersichtlich wird, dass alle Verschlüsselungsverfahren nach einem dieser Prinzipien oder auch einer Kombination arbeiten. Im Idealfall nennen die Schüler*innen selbst ausreichend vielfältige Beispiele, da hier in der Regel schon Vorwissen vorhanden ist. Wenn ein Beispiel für eines der Prinzipien fehlt, können entsprechende Verfahren, z. B. mithilfe der Materialien aus dem Spioncamp der Uni Wuppertal³ ergänzt werden.

Ein weiteres Ziel ist die Abgrenzung der Verschlüsselungsverfahren gegen allgemein lesbare Codierungen oder steganographische Verfahren. Hier ist zu erwarten, dass die Schüler*innen zunächst auch Beispiele nennen, die in die beiden letzteren Kategorien gehören.

Anhand der Beispiele, die die Schüler*innen sich selbst ausgedacht haben, kann ggf. noch thematisiert werden, dass die Decodierung mithilfe des Schlüssels eindeutig sein muss.

Für die Bearbeitung des AB02 zur genaueren Untersuchung des Caesar-Verfahrens wird eine Caesar-Scheibe benötigt. Hier kann z. B. die Vorlage aus dem Spioncamp der Uni Wuppertal³ verwendet werden. Diese hat den Vorteil, dass der Schlüssel zusätzlich als Zahl angezeigt wird, was später für die Implementierung hilfreich ist.

Ein monoalphabetisches Verfahren wie in AB04 haben die Schüler*innen vermutlich in ihren Beispielen bereits beschrieben. Es dient hier nur noch einmal zur Vorbereitung der Häufigkeitsanalyse.

Je nachdem wie erfolgreich die Schüler*innen bei der Implementierung ihres Textanalysetools waren, kann dieses zum Zählen der Zeichen eingesetzt werden. Alternativ können die Zeichen auch mithilfe der Ersetzen-Funktion einer Textverarbeitung gezählt werden⁴. Oder man stellt ein entsprechendes Analyseprogramm zur Verfügung. Damit besteht auch die Möglichkeit, die Arbeitsblätter AB04 und AB05 vor der Einführung der zeichenweisen Verarbeitung von Zeichenketten

² Nähere Informationen zu Flinga unter <http://www.nordtouch.fi/> [Datum des Zugriffs: 06.05.2021]

³ Didaktik der Informatik an der Bergischen Universität Wuppertal (2012). Spioncamp. <https://ddi.uni-wuppertal.de/www-madin//material/spioncamp.html> [Datum des Zugriffs: 15.01.2021]

⁴ Nach einer Idee aus Modrow, E. & Strecker, S. (2016). *Didaktik der Informatik*. S. De Gruyter: Berlin, Boston

einzusetzen. Dabei ist der Vorteil, dass die Überlegungen zur schrittweisen Verbesserung der Substitutionsverfahren nicht unterbrochen werden.

Dieses Werk ist lizenziert unter einer [Creative Commons Namensnennung - Nicht kommerziell - Keine Bearbeitungen 4.0 International Lizenz](#). Sie erlaubt Download und Weiterverteilung des vollständigen Werkes unter Nennung unserer Namen, jedoch keinerlei Bearbeitung oder kommerzielle Nutzung.