

Didaktische Hinweise zu einer Unterrichtseinheit Kryptologie in der Sek I

Vorbemerkung

In der Literatur und im Internet sind verschiedene Materialien und Unterrichtssequenzen aus dem Bereich Kryptologie zugänglich, die unterschiedliche Schwerpunkte setzen. Im Anhang erfolgt eine Übersicht, die aber weder einen Anspruch auf Vollständigkeit erhebt noch eine Wertung vorsieht.

Die hier vorgestellte Unterrichtssequenz stellt den Wettlauf zwischen Kryptologen und Kryptographen in den Vordergrund und lässt die Schüler*innen Teile der historischen Entwicklung der Geheimschriften nacherleben. Dabei können sie sukzessive alle Kompetenzen erwerben, die das niedersächsische Kerncurriculum für die Sekundarstufe I im Bereich *Datensicherheit* vorsieht (vgl. [8]). Es können aber je nach Lerngruppe und zur Verfügung stehender Zeit auch nur Teile der Sequenz unterrichtet werden, so dass nur die Basiskompetenzen oder nur die Basis- und Vertiefungskompetenzen erworben werden.

Zu Beginn stehen Verfahren im Vordergrund, die die Schüler*innen bereits als Vorwissen mitbringen oder sich selbst ausgedacht haben. Ist die Erarbeitung und Anwendung bestimmter Verfahren notwendig, wird z. T. auf die Materialien des *Spioncamps* der Universität Wuppertal zurückgegriffen (s. [3]). An den entsprechenden Stellen erfolgt ein Hinweis.

Zielgruppe

Die Unterrichtseinheit richtet sich vor allem an Schüler*innen von Klasse 8 bis 10. Das Erproben historischer und entwerfen eigener Verschlüsselungsverfahren ist bereits in früheren Jahrgängen möglich.

Voraussetzungen

Inhaltlich benötigen die Schüler*innen keine zwingenden Voraussetzungen.

Soll die Motivation des Themas über die unsicheren Kommunikationswege des Internets erfolgen, ist es jedoch sinnvoll, wenn die Schüler*innen sich bereits mit der Struktur des Internets auskennen.

Dazu steht im Lernfeld *Daten und ihre Spuren* das Materialpaket „Einstieg in die Nutzungsmöglichkeiten und Struktur des Internets“ zur Verfügung. Für Version 1 des ersten Arbeitsblattes wird zusätzlich der Umgang mit der Simulationssoftware Filius (s. 12) vorausgesetzt. Version 2 kann ohne entsprechende Vorkenntnisse bearbeitet werden.

Um die Verschlüsselung als besondere Form der Codierung einzuordnen, die nur mithilfe einer zusätzlichen geheimen Information durchgeführt werden kann, ist es hilfreich, wenn die Schüler*innen bereits allgemein bekannte Codierungen (z. B. den ASCII-Code) und die dahinterstehenden Konzepte kennengelernt haben.

Lernziele

Die Möglichkeit, Nachrichten durch Verschlüsselung geheim zu halten, ist eine wichtige Grundlage für unsere moderne Kommunikation über das Internet. Auch wenn die Mathematik aktuell sicherer Verschlüsselungsverfahren für Schüler*innen in der Sekundarstufe I zu komplex ist, können anhand historischer Verfahren wichtige Konzepte der Kryptographie veranschaulicht werden, die auch in

aktuellen Verfahren noch zur Anwendung kommen. Ebenso können die prinzipiellen Ansätze der Kryptoanalyse verdeutlicht werden.

Das niedersächsische Kerncurriculum für die Sek I sieht in dem Modul *Datenschutz und Datensicherheit* im Lernfeld *Daten und ihre Spuren* für den Teilbereich Datensicherheit den Erwerb der folgenden Kompetenzen vor (s. [8]):

| | Basis | Vertiefung | Ergänzung |
|---------------------------------|---|--|---|
| | Die Schülerinnen und Schüler ... | | |
| Datenschutz und Datensicherheit | <ul style="list-style-type: none"> - nennen mögliche Formen des Datenmissbrauchs. - nennen Maßnahmen, wie z. B. Schutz durch Passwörter oder Verschlüsselung, um sicher in Netzwerken zu kommunizieren und Daten vor Fremdzugriff zu sichern. | <ul style="list-style-type: none"> - erläutern das Prinzip der Substitution und Transposition als Grundlage der Datenverschlüsselung. - wenden einfache symmetrische Verschlüsselungsverfahren an, z. B. Caesar-Code, Vigenère-Verfahren - beurteilen die Sicherheit von einfachen Verschlüsselungsverfahren. | <ul style="list-style-type: none"> - beschreiben das Prinzip der asymmetrischen Verschlüsselung. - unterscheiden zwischen symmetrischen und asymmetrischen Verfahren. - verschlüsseln und signieren Daten mithilfe aktueller Software. |

Tabelle 1: Auszug aus dem Modul Datenschutz und Datensicherheit im Lernfeld Daten und ihre Spuren

In einer Unterrichtseinheit zum Erwerb dieser Kompetenzen sollten die folgenden Aspekte deutlich werden, da es sich dabei um Konzepte handelt, die unabhängig von einem konkreten Beispiel auch heute noch bedeutsam für die Kryptologie sind:

Basis

- Wo könnten Nachrichten im Internet mitgelesen oder sogar verändert werden? Wer könnte ein Interesse daran haben?
- Was ist der Unterschied zwischen einem Passwort und einer Verschlüsselung? Welche Ziele werden beim Einsatz von Passwörtern bzw. Verschlüsselungsverfahren verfolgt?

Vertiefung

- Verschlüsselung als spezielle Form der Codierung, die zusätzlich zu dem gewählten Verfahren eine geheime Information erfordert, die notwendig ist, um die Nachricht zu decodieren: den Schlüssel¹
- Transposition und Substitution als Grundlage sowohl historischer als auch moderner Verschlüsselungsverfahren
- Wettlauf zwischen Kryptographen und Kryptoanalytikern: Wenn der Inhalt einer Nachricht durch Verschlüsselung schützenswert ist, gibt es auch „Angreifer“, die versuchen, die Nachricht ohne Kenntnis des Schlüssels zu lesen (zu knacken). Für viele Verfahren ist das im Laufe der Geschichte gelungen, so dass daraufhin neue, sicherere Verfahren entwickelt wurden. Hinter den Angriffen der Kryptoanalytiker stecken systematische Verfahren, die beim Entwurf eines sicheren Verfahrens berücksichtigt werden müssen. Es bleibt dann nur noch das Ausprobieren aller möglichen Schlüssel.

¹ Damit zusammen hängt die Erfahrung der Kryptographie, dass das Verfahren einer Verschlüsselung nicht langfristig geheim gehalten werden kann. Die Sicherheit eines Verfahrens basiert daher auf der Geheimhaltung des Schlüssels. Die Nachricht darf ohne Schlüssel nicht lesbar sein und der Schlüssel darf sich nicht aus der geheimen Nachricht rekonstruieren lassen. Sehr anschaulich wird das von Beutelspacher beschrieben (s. [1], S. 7).



Ergänzung

- Alle symmetrischen Verschlüsselungsverfahren stehen vor dem Problem, den Schlüssel zunächst über einen sicheren Kommunikationskanal austauschen zu müssen.
- Das Schlüsselaustauschproblem hat zur Entwicklung asymmetrischer Verschlüsselungsverfahren geführt. Auch diese können auf einer schematischen Ebene bereits in der Sek I betrachtet und ihre Anwendungsmöglichkeiten (z. B. Vertraulichkeit, Authentifikation) erarbeitet werden.

Aufbau und Materialien der Unterrichtseinheit

Es wird zunächst ein tabellarischer Überblick über die Unterrichtseinheit gegeben. Anschließend folgen nähere Erläuterungen zu den einzelnen Themenblöcken.

| Zeit | Thema | geförderte Kompetenzen Die Schülerinnen und Schüler | Material / Methoden |
|---------|---|---|---|
| 1 DStd. | Motivation: Welche Probleme können bei ungesicherter Kommunikation im Internet auftreten? | <ul style="list-style-type: none"> - nennen mögliche Formen des Datenmissbrauchs. - nennen Maßnahmen, wie z. B. Schutz durch Passwörter oder Verschlüsselung, um sicher in Netzwerken zu kommunizieren und Daten vor Fremdzugriff zu sichern. | <p>Analyse eines Datenprotokolls einer Kommunikation in einem Netzwerk erstellt mit Filius</p> <p>Version 1: Simulation des Datenverkehrs in Filius (s. [13]): <i>AB1_AnalyseDatenverkehrNetzwerk_V1.pdf</i> <i>Filius_Netzwerk_Biblix.flx</i>²</p> <p>Version 2: Verwendung gegebener Protokolle ohne Einsatz von Filius <i>AB1_AnalyseDatenverkehrNetzwerk_V2.pdf</i> <i>01_Router - 192.168.0.1.txt</i> <i>02_Router - 192.168.2.1.txt</i> <i>03_Router - 192.168.1.1.txt</i></p> |
| 1 DStd. | Überblick über verschiedene Arten der Verschlüsselung | <ul style="list-style-type: none"> - erläutern das Prinzip der Substitution und Transposition als Grundlage der Datenverschlüsselung. - wenden einfache symmetrische Verschlüsselungsverfahren an | <p>SuS erstellen Poster zu bekannten / ausgedachten Verfahren und probieren einige Verfahren aus</p> <p>Erarbeitung zentraler Begriffe und Prinzipien der Kryptographie an den SuS-Beispielen: <i>AB2_Uebersicht_Kryptographie.pdf</i></p> <p>nur falls die SuS-Beispiele nicht vielfältig genug sind, z. B. keine Transposition: Ergänzung bekannter historischer</p> |

² Die kursiv geschriebenen Dateinamen beziehen sich auf die Dateien des beiliegenden Schülermaterials.

| | | | |
|---------|---|---|--|
| | | | Verfahren, z. B. Skytale, Freimaurer mit Material aus dem Spioncamp (s. [3]) |
| 3 DStd. | Der Wettlauf zwischen Kryptographen und Kryptoanalytikern | <ul style="list-style-type: none"> - wenden einfache symmetrische Verschlüsselungsverfahren an, z. B. Caesar-Code, Vigenère-Verfahren - beurteilen die Sicherheit von einfachen Verschlüsselungsverfahren. | <p>Erprobung und Analyse des Caesar-Verfahrens: Caesar-Scheibe (s. [3]) <i>AB3_Aufgaben_Caesar.pdf</i></p> <hr/> <p><i>AB4_Aufgaben_monoSubstitution.pdf</i></p> <p>Häufigkeitsanalyse für monoalphabetisch verschlüsselte Geheimtexte: <i>AB5_Haeufigkeitsanalyse.pdf</i> <i>geheimtext1.docx</i> <i>geheimtext2.docx</i> <i>geheimtext3.docx</i> Textverarbeitungsprogramm</p> <hr/> <p>Gruppenpuzzle zu erweiterten Substitutionsverfahren (homophon, polyalphabetisch): <i>AB6_Gruppenpuzzle_Substitutionsverfahren.pdf</i> Rotoren (s. [3])</p> |
| 3 DStd. | Das Problem mit dem Schlüssel: Prinzip und Anwendungsmöglichkeiten asymmetrischer Verschlüsselungsverfahren | <ul style="list-style-type: none"> - beschreiben das Prinzip der asymmetrischen Verschlüsselung. - unterscheiden zwischen symmetrischen und asymmetrischen Verfahren. - verschlüsseln und signieren Daten mithilfe aktueller Software. | <p>Softwarepaket Gpg4win (s. [5]) <i>Leitfaden_AsymmetrischeVerschluesselung.pdf</i> <i>Anleitungen zu Kleopatra oder GPA</i></p> |
| 1 DStd. | Erstellen eines Lexikons zur Kryptologie | <ul style="list-style-type: none"> - kommunizieren unter Verwendung der Fachsprache über informatische Inhalte | <p><i>AB7_Lexikon</i> ggf. kollaboratives Textverarbeitungsprogramm</p> |

Motivation

Für die Informatik spielen Verschlüsselungsverfahren vor allem im Zusammenhang mit der Kommunikation über unsichere Kommunikationskanäle eine Rolle. Wenn die Schüler*innen sich bereits mit dem Aufbau des Internets vertraut gemacht haben, ist einsichtig, dass es sich bei der Kommunikation über das Internet um einen solchen unsicheren Kanal handelt. Dabei kann die Kommunikation per Mail, per Messenger, über eine Webseite oder auch per Anruf über einen Internetdienst erfolgen. Unabhängig vom verwendeten Dienst passiert eine Nachricht auf dem Weg durchs Internet viele Rechner (Router, Server), auf denen leicht eine Kopie gespeichert werden kann, so dass jeder, der Zugang zu einem dieser Rechner hat, die Nachricht mitlesen oder mithören kann. Die Nachricht könnte vor der Weiterleitung sogar verändert oder ausgetauscht werden. Dies soll anhand der Aufgaben des ersten Arbeitsblattes transparent gemacht werden.

Verschickt man in der beiliegenden Simulation eines Netzwerks für die Lernsoftware *Filius* (s. [13]) eine Nachricht per E-Mail und ruft diese anschließend ab, so kann man im Nachrichtenprotokoll sehen, dass der Inhalt der E-Mail und sogar das Passwort und der Benutzername des Mailaccounts für jeden lesbar verschickt werden. Verwendet man das pop3-Protokoll für seinen Mailaccount ohne eine zusätzliche Verschlüsselung, könnte tatsächlich jeder, der den Netzwerkverkehr mithört, die Nachricht und die Zugangsdaten lesen.

Haben die Schüler*innen bereits mit *Filius* gearbeitet und etwas Erfahrung mit dem Aufbau von Netzwerken, gibt das Arbeitsblatt AB1 in der Version 1 den Schüler*innen in den Aufgaben 1 bis 3 Impulse für eine eigenständige Analyse des Datenverkehrs.

Wenn die Schüler*innen noch nicht mit der Lernsoftware *Filius* gearbeitet haben, kann stattdessen das Arbeitsblatt AB1 in der Version 2 verwendet werden. Hier ist die Analyse eines bereits vorhandenen Datenprotokolls, das aus *Filius* exportiert wurde, vorgesehen.

Im Sinne der zu erwerbenden Basiskompetenzen können die Schüler*innen diskutieren, zu welchen Problemen es kommen kann, wenn die Nachrichten, die über das Internet verschickt werden, in falsche Hände gelangen. Und welche Maßnahmen sie kennen, um das Mitlesen der Daten zu verhindern. Allen Schüler*innen sollte bewusst werden, dass es wichtig ist,

1. sichere Passwörter zu verwenden und diese geheim zu halten.
2. darauf zu achten, nur Webseiten und Nachrichtendienste zu verwenden, die die Nachrichten verschlüsselt versenden .

Das Arbeitsblatt bietet auch hier in beiden Versionen entsprechende Impulse und Arbeitsaufträge an. Für das Erstellen der Tabelle in Aufgabe 4 (Version 1) bzw. Aufgabe 3 (Version 2) bietet sich das kollaborative Arbeiten an einem gemeinsamen Textdokument an.

Ergänzend zu den Aufgaben des Arbeitsblattes kann thematisiert werden, dass unverschlüsselte Nachrichten an den Routern und Servern nicht nur abgefangen, sondern auch verändert werden könnten.

Sollen nur die Basiskompetenzen zum Thema Datensicherheit erworben werden, kann die Einheit hier bereits abgeschlossen werden.

Überblick über verschiedene Arten der Verschlüsselung

Geheimschriften üben von sich aus bereits eine gewisse Faszination aus. Die Möglichkeit mit der besten Freundin oder dem besten Freund Nachrichten auszutauschen, ohne dass Eltern,

Lehrer*innen oder Mitschüler*innen mitlesen können, ist attraktiv. Die meisten Schüler*innen kennen Geheimschriften aus Detektivgeschichten oder Knobelheften.

Um die Schüler*innen dort abzuholen, wo sie stehen, sieht Arbeitsblatt 2 vor, dass die Schüler*innen zunächst einzeln oder in 2er-Teams ein Plakat entwerfen, auf dem sie ein Verschlüsselungsverfahren darstellen, das sie kennen oder sich selbst ausgedacht haben. Anhand der Beispiele können dann die folgenden Aspekte herausgearbeitet werden:

- Was unterscheidet eine Verschlüsselung von einer allgemein lesbaren Codierung?
- Welche Voraussetzungen muss ein Verschlüsselungsverfahren erfüllen, damit die Nachricht von dem rechtmäßigen Empfänger wieder entschlüsselt werden kann?
- Welche Arten der Verschlüsselung gibt es? – Viele werden hier ein Substitutions- oder Transpositionsverfahren wählen, ggf. auch ein steganographisches Verfahren, so dass die Beispiele der Schüler*innen in zwei bis drei Kategorien eingeteilt werden können.
- Die Substitutionsverfahren unterscheiden sich meist in den Geheimtextzeichen. Hier entsteht ggf. die Frage, ob ein Verfahren mit möglichst exotischen Geheimtextzeichen sicherer ist als ein Verfahren, das z. B. nur jeden Buchstaben durch einen anderen Buchstaben ersetzt. Hier besteht bei Schüler*innen oft die Fehlvorstellung, dass dies mit Ja zu beantworten sei. Diese Fehlvorstellung muss dann ggf. später im Rahmen der Häufigkeitsanalyse korrigiert werden.

Sind die Beispiele der Schüler*innen nicht hinreichend unterschiedlich und exemplarisch für die verschiedenen Kategorien, können beispielsweise die Materialien des Spioncamps (s. [3]) verwendet werden, um die Schüler*innen ein Beispiel für ein Verfahren einer fehlenden Kategorie erproben zu lassen.

Der Wettlauf zwischen Kryptographen und Kryptoanalytikern

Um den Wettlauf zwischen Kryptographen und Kryptoanalytikern zu veranschaulichen, bietet es sich an, mit den Schüler*innen den Weg vom Caesar-Verfahren, über eine beliebige monoalphabetische Substitution bis zur polyalphabetischen Substitution nachzuzeichnen und die Schüler*innen dabei wechselweise die Rolle der Kryptographen und der Kryptoanalytiker einnehmen zu lassen.

Im Idealfall entwickeln die Schüler*innen selbst Ideen, wie die Verfahren jeweils geknackt und mit Blick auf diese Angriffsmöglichkeiten sicherer gemacht werden können. Die jeweils letzte Aufgabe auf den Arbeitsblättern 3 bis 5 gibt hier entsprechende Impulse.

Caesar-Verfahren

Das Caesar-Verfahren ist ein Beispiel für ein sehr einfaches monoalphabetisches Substitutionsverfahren. Ein entsprechend verschlüsselter Text kann sehr leicht geknackt werden, da es nur 25 verschiedenen Schlüssel gibt.

Für die Aufgaben des Arbeitsblattes *AB3_Aufgaben_Caesar* wird eine Caesar-Scheibe benötigt. Hier bietet sich z. B. die Vorlage³ und Seite 1 der Erläuterung⁴ aus dem Spioncamp der Uni Wuppertal an (s. [3]). Eine digitale Caesar-Scheibe steht unter <https://www.inf-schule.de/kids/datennetze/verschluesselung/schritt4> (s. [7]) zur Verfügung.

³ <https://ddi.uni-wuppertal.de/www-madin//material/spioncamp/dl/substitution-m-caesar-mat0.pdf>

⁴ <https://ddi.uni-wuppertal.de/www-madin//material/spioncamp/dl/substitution-m-caesar-station.pdf>

Monoalphabetische Substitution und Häufigkeitsanalyse

Eine beliebige Zuordnung von Klartext- und Geheimtextzeichen stellt eine erste Verbesserung des Caesar-Verfahrens dar. Diese Möglichkeit können die Schüler*innen mithilfe des Arbeitsblattes *AB4_Aufgaben_monoSubstitution* erproben. Wenn die Schüler*innen hier selbst die Idee entwickeln, einen monoalphabetisch verschlüsselten Text mithilfe einer Analyse der Häufigkeiten der verschiedenen Zeichen zu knacken, können die Hinweise auf dem Arbeitsblatt zur Häufigkeitsanalyse (*AB5_Hauefigkaitesanalyse*) entsprechend gekürzt werden.

Nach einer Idee von Eckart Modrow und Kerstin Strecker wird die Häufigkeitsanalyse mithilfe eines Textverarbeitungsprogramms durchgeführt, so dass anwendungsbezogen gleichzeitig Kompetenzen in diesem Bereich erworben werden können (s. [9], 113f.).

Geheimtext 1 wurde mit einer Zuordnungstabelle wie die Schüler*innen sie aus dem vorhergehenden Arbeitsblatt kennen, verschlüsselt. ä, ö, ü und ß wurden dabei durch ae, oe, ue und ss ersetzt. Die Satzzeichen sind unverändert. Wichtig ist, dass der Text alleine in einer Datei steht. Da eine zusätzliche Aufgabenstellung oder Informationen in der Kopf- oder Fußzeile die Anzahl der Geheimtextzeichen verfälschen würden.

Die Geheimtexte 2 und 3 dienen der Differenzierung. In Geheimtext 2 wurden statt der Buchstaben des Alphabets Zahlen und Sonderzeichen verwendet. Eine Häufigkeitsanalyse dieses Textes soll zeigen, dass das Verfahren unabhängig von den verwendeten Geheimtextzeichen funktioniert, um eventuellen Fehlvorstellungen entgegenzuwirken. Allerdings ist dabei zu berücksichtigen, dass den Schüler*innen die Durchführung hier eventuell geringfügig schwerer fällt, da zunächst eine Liste aller verwendeten Geheimtextzeichen erstellt werden muss. Satzzeichen behalten wieder ihre Bedeutung. Geheimtext 3 ist vergleichsweise kurz und weist zudem keine typische Häufigkeitsverteilung auf. Daran kann verdeutlicht werden, dass der Erfolg einer Häufigkeitsanalyse auch von der Struktur des verschlüsselten Textes abhängt. Entsprechende Kriterien werden in Aufgabe 4 gesammelt.

Verbesserungen der monoalphabetischen Substitution

Im Rahmen des Gruppenpuzzles in *AB6_Gruppenpuzzle_Substitutionsverfahren* sollen die Schüler*innen sich folgende Aspekte erarbeiten:

Eine Häufigkeitsanalyse ist bei einem Substitutionsverfahren immer dann möglich, wenn die Häufigkeitsverteilung der Klartextzeichen auf die Geheimtextzeichen übertragen wird. Das ist auch der Fall, wenn wie bei dem Polybios-Verfahren das Geheimtextzeichen aus zwei Zeichen besteht, da diese Tupel wie ein Zeichen behandelt werden können.

Eine *homophone Substitution* gleicht die unterschiedlichen Häufigkeiten aus, indem häufigere Zeichen durch verschiedene Geheimtextzeichen verschlüsselt werden. Dadurch ist eine Häufigkeitsanalyse nicht mehr so leicht möglich.

Bei der *polyalphabetischen Substitution* gibt es mehrere Zuordnungen zwischen Klartext und Geheimtextzeichen. Man spricht von mehreren Geheimtextalphabeten. Der Schlüssel legt die Reihenfolge der verwendeten Geheimtextalphabete fest, so dass ein Klartextzeichen unterschiedlichen Geheimtextzeichen zugeordnet wird. Anders als bei der homophonen Verschlüsselung steht aber auch jedes Geheimtextzeichen für unterschiedliche Klartextzeichen. Dadurch ist auch in diesem Fall keine Häufigkeitsanalyse mehr möglich.

Die Materialien enthalten eine Erläuterung und Aufgaben zum Polybios-Verfahren, zur homophonen Substitution und zum Vigenère-Verfahren für die Expertengruppen. Entsprechende Materialien zu der polyalphabetischen Verschlüsselung mit Rotoren (Prinzip der Enigma) können den Materialien des Spioncamps entnommen werden (s. [3]).

Das Gruppenpuzzle könnte noch um eine weitere Expertengruppe mit einem klassischen monoalphabetischen Substitutionsverfahren wie der Freimaurerchiffre erweitert werden. Wird hier das Material des Spioncamps (s. [3]) verwendet, bietet es sich jedoch an, den Hinweis, dass es sich um eine monoalphabetische Substitution handelt, zu entfernen.

In einem Ausblick sollte deutlich werden, dass auch die erprobten polyalphabetischen Verfahren heute für sensible Nachrichten nicht mehr ausreichend sicher sind. Ist bei den polyalphabetischen Verfahren bekannt, nach wie vielen Zeichen im Text sich die Geheimtextalphabet wiederholen, ist eine Häufigkeitsanalyse wieder möglich. Beim Vigenère-Verfahren steckt diese Information in der Länge des Schlüssels. Wird bei einem Schlüsselwort der Länge 4 jedes erste, fünfte, neunte usw. Zeichen betrachtet, so ergeben diese Zeichen allein einen monoalphabetisch verschlüsselten Text, da diese Zeichen alle mit dem gleichen Geheimtextalphabet verschlüsselt wurden. Aufbauend auf der Annahme, dass die Schlüssellänge herausgefunden wurde, können sich daher auch schon Schüler*innen in der Sekundarstufe I das weitere Vorgehen zum Knacken eines Vigenère-verschlüsselten Textes überlegen. Unter Verwendung entsprechender Programme können heutzutage unterschiedliche Schlüssellängen einfach ausprobiert werden, um eine Nachricht, die mit dem Vigenère-Verfahren verschlüsselt wurde, zu knacken.

Die statistischen Verfahren zum Bestimmen der Schlüssellänge (z. B. den Kasiski-Test) sind für die Sekundarstufe I in der Regel zu komplex sind. Ein Beispiel und eine Aufgabe zum Knacken des Vigenère-Verfahrens enthält z. B. das Arbeitsmaterial A2.11 aus den IT2School-Materialien in Modul A2: Kryptologie (s. [14]).

Auch die homophone Verschlüsselung bietet noch Angriffsmöglichkeiten. Da die Zweierkombination von Buchstaben, die Bigramme, ebenfalls unterschiedlich häufig vorkommen, können hierüber Rückschlüsse auf die Zuordnung von Geheimtext- zu Klartextzeichen gezogen werden. Eine entsprechende Analyse ist aber deutlich aufwändiger.

Asymmetrische Verschlüsselung

Das RSA-Verfahren ist das am häufigsten verwendete asymmetrischen Verschlüsselungsverfahren. Die mathematischen Hintergründe sind für die Sekundarstufe I noch zu komplex. Leider gibt es hier kaum einfachere Varianten wie bei den symmetrischen Verfahren, die leichter nachzuvollziehen sind. Jens Gallenbacher schlägt ein solches vereinfachtes asymmetrisches Verfahren vor (s. [4]). Pfiffige Schüler*innen finden hier jedoch einen Zusammenhang zwischen öffentlichem und privatem Schlüssel.

Die Erläuterung des Prinzips der asymmetrischen Verschlüsselung muss daher auf der Ebene schematischer Darstellungen erfolgen, z. B. mithilfe einer Schlüssel-Schloss-Analogie. Gallenbacher stellt die Vorgänge bei der asymmetrischen Verschlüsselung sehr anschaulich dar (s. [4])

Hier wird noch ein anderer Zugang vorgestellt, bei dem die asymmetrische Verschlüsselung mithilfe geeigneter Software angewendet und das Vorgehen dabei analysiert wird. Das verwendete Programmpaket ist Gpg4win-3.1.15 (s. [5]), welches die beiden relevanten kryptografischen Standards OpenPGP und S/MIME (X.509) unterstützt. Es enthält Komponenten zur Schlüsselverwaltung sowie

zur Ver- und Entschlüsselung sowie zur Signatur von Texten, E-Mails und Dateien. Ein entsprechendes Programmpaket steht mit GPG Suite auch für das Betriebssystem macOS zur Verfügung (s. [6]). Inzwischen sind die Verschlüsselungsverfahren auch in vielen E-Mail-Programmen integriert. Um das Vorgehen transparenter zu machen, wird hier jedoch weiterhin die eigenständige Software genutzt. Mithilfe des Leitfadens zur asymmetrischen Verschlüsselung können sich die Schüler*innen die Prinzipien der Asymmetrischen Verschlüsselung erarbeiten und parallel mithilfe der Programme *Kleopatra* oder *GPA* aus dem Programmpaket Gpg4win erproben. Um den Lesefluss des Leitfadens nicht zu stören, befinden sich die Anleitungen zum Umgang mit den Programmen in separaten Dateien.

Das Programm Kleopatra erlaubt in der hier verwendeten Version das Erzeugen eines Schlüsselpaares ohne Passwort. Da die Schüler*innen das Passwort zum Teil mit dem privaten Schlüssel verwechseln, kann dies für das Verständnis der Konzepte von Vorteil sein. In GPA ist hingegen das Ver- und Entschlüsseln sowie das Signieren von Texten in der Zwischenablage nach Ansicht der Autorin anschaulicher und übersichtlicher. Außerdem sind private und öffentliche Schlüssel in der Schlüsselverwaltung von GPA durch ein doppeltes zweifarbiges bzw. ein einfaches einfarbiges Schlüsselsymbol deutlich zu unterscheiden. Während Kleopatra bei der Installation des Programmpaketes vorausgewählt ist, muss GPA explizit angewählt werden.

Der Leitfaden stellt den Unterschied des öffentlichen und privaten Schlüssels in den Vordergrund. Das Problem des Vertrauens wird thematisiert. Ziel ist hier jedoch nur die Schüler*innen für eine Überprüfung des Schlüssels zu sensibilisieren, was z. B. im persönlichen Gespräch über den Fingerabdruck erfolgen kann. Zertifikate, die eine dritte, vertrauenswürdige Instanz involvieren erscheinen für die Sekundarstufe I zu komplex und werden daher nicht im Detail erläutert.

Während die Verschlüsselung mittels OpenPGP auf der Ebene der Personen durchgeführt wird, laufen die entsprechenden Verfahren bei der Kommunikation mit Webservern über das https-Protokoll auf der Ebene der Rechner ab. Die Verschlüsselung von Webseiten wird für Lerngruppen, die sich nicht mit der asymmetrischen Verschlüsselung beschäftigen, bereits auf dem ersten Arbeitsblatt angesprochen. Ist der Einsatz des Leitfadens zur asymmetrischen Verschlüsselung geplant, können die entsprechenden Aufgaben zu Beginn ausgelassen werden. Alternativ können die redundanten Aufgabenteile bei der abschließenden Betrachtung ausgelassen werden.

Das Konzept der hybriden Verschlüsselung wird im Zusammenhang mit der Verschlüsselung von Webseiten angedeutet jedoch nicht umfänglich erläutert. Bei der Verwendung von gpg4Win wird vereinfachend davon ausgegangen, dass die gesamte Nachricht mit dem asymmetrischen Verfahren verschlüsselt wird. In der Praxis wäre dies zu aufwändig. Die Nachricht wird daher mit einem symmetrischen Schlüssel verschlüsselt. Nur der verwendete Schlüssel, wird mit dem asymmetrischen Verfahren verschlüsselt, so dass er einfach an die Nachricht angehängt und mitgeschickt werden kann.

Lexikon

Im Themenbereich Kryptologie werden viele neue Fachbegriffe erlernt, die notwendig sind, um kryptographische Verfahren zu erläutern, zu typisieren und über ihre Sicherheit zu diskutieren. Damit die Schüler*innen dabei nicht den Überblick verlieren, bietet es sich an, ein Lexikon zu erstellen. Dies

kann begleitend zum Unterricht oder als Selbstkontrolle und Vorbereitung einer Lernzielkontrolle zum Abschluss erfolgen.

Hier bietet sich auch das kollaborative Arbeiten der Schüler*innen an einem gemeinsamen Dokument an. Zum Beispiel kann jeder/jede zunächst einen Begriff erläutern. Zwei andere Schüler*innen sind dann für eine Kontrolle und ggf. Korrektur zuständig.

Fällt den Schüler*innen das Formulieren eigener Definitionen schwer, können die Begriffe und Definitionen auch getrennt vorgegeben werden, so dass nur noch die richtige Zuordnung erfolgen muss.

Die Auswahl der Begriffe in der beiliegenden Datei Lexikon muss ggf. angepasst werden, je nachdem welche Aspekte im Unterricht thematisiert wurden.

Ausblick

Eine spannende Geschichte umgibt die Beale-Chiffren aus dem 19. Jahrhundert, die bis heute nicht vollständig geknackt wurden und angeblich eine Schatzkarte enthalten. Diese bieten sich für interessierte Schüler*innen als Recherche-Aufgabe an. Die zweite Beale-Chiffre, die geknackt wurde, liefert ein weiteres Beispiel für eine homophone Verschlüsselung.

2019 hat Florian Bies ein Jugend-forscht-Projekt zu den Beale-Chiffren erstellt (s. [2]). Auf YouTube ist eine Dokumentation von ZDFinfo über die Beale-Chiffren abrufbar (s. [10]). Nach dem Kryptographen Klaus Schmech ist allerdings davon auszugehen, dass die Geschichte um die Beale-Chiffren nur eine Fiktion ist (s. 11).

Die Implementierung der kryptographischen Verfahren wäre für viele Schüler*innen in der Sek I noch eine Überforderung, da dies in der Regel fortgeschrittene Kompetenzen im Bereich Algorithmik voraussetzt, wie das zeichenweise Verarbeiten von Zeichenketten. Sollen die Themen Codierung und Kryptographie trotzdem mit einem praktischen Projekt im Bereich Algorithmik verknüpft werden, bietet sich die Implementierung einer virtuellen Schatzsuche an, wie sie im Materialpaket [Projektidee Escape Room oder virtuelle Schatzsuche](#) vorgestellt wird. Dort wird auch beschrieben, wie die erlernten Verfahren alternativ beim Entwurf eines realen Escape Rooms eingebracht werden können.

Anhang

Überblick über Materialien zum Thema Kryptologie

Die Auflistung erhebt keinen Anspruch auf Vollständigkeit und nimmt keine Wertung vor.

| Quelle und kurze Beschreibung | Kategorie |
|---|--|
| <p>CrypTool-Portal https://www.cryptool.org/de/ [Datum des Zugriffs: 19.01.2021]</p> <p>Das Portal bietet die Open-Source Lernsoftware CrypTool in verschiedenen Versionen an. Mit der Software können verschiedene Verfahren der Kryptographie und der Kryptoanalyse praktisch erprobt werden.</p> | Lernsoftware |
| <p>Didaktik der Informatik an der Bergischen Universität Wuppertal (2012). <i>Spioncamp</i>. https://ddi.uni-wuppertal.de/www-madin//material/spioncamp.html [Datum des Zugriffs: 15.01.2021]</p> <p>Ein Stationenlernen zur Erprobung vieler verschiedener Codierungs- und Verschlüsselungsverfahren. Jedes Verfahren wird in die Kategorien Codierung, Steganographie, Transposition oder Substitution eingeordnet. Die Materialien zu den einzelnen Verfahren können auch in anderen methodischen Szenarien einzeln eingesetzt werden.</p> | Stationenlernen |
| <p>Jens Gallenbacher (2008). <i>Abenteuer Informatik. (2. Aufl.) Kapitel 9 - Mit Sicherheit</i>. Spektrum Akademischer Verlag: Heidelberg.</p> <p>Anschauliche Erläuterung der Prinzipien der symmetrischen und der asymmetrischen Verschlüsselung zum Selbstlernen mit Materialien zum Ausprobieren.</p> | Buch |
| <p>Andreas Gramm, Malte Hornung & Helmut Witten. Informatik im Kontext. Email (nur?) für Dich https://medienwissenschaft.uni-bayreuth.de/inik/entwuerfe/email-nur-fuer-dich/ [Datum des Zugriffs: 19.01.2021]</p> <p>Im Kontext der Kommunikation per E-Mail werden Aspekte zur Vertraulichkeit, Integrität und Authentizität erarbeitet. Für ältere Schüler*innen ab Klasse 10.</p> | Material für eine Unterrichtseinheit |
| <p>Michèle Keller-Butteli (2020). https://www.inf-schule.de/kids/datennetze/verschluesselung [Datum des Zugriffs: 19.01.2021]</p> <p>Kurze Einheit mit Hinführung durch lebensnahe Beispiele, in denen Nachrichten durch Verschlüsselung schützenswert sind; je ein Beispiel zur Substitution (Caesar) und zur Transposition (Skytale). Abschließend entwickeln die Schüler*innen eigene Geheimschriften.</p> | Interaktive Webseite als digitales Schulbuch |
| <p>Stefan Müller (2017). Brickscience TV - Kryptographie. https://www.youtube.com/watch?v=QhwcD4XHHJ8 [Datum des Zugriffs: 27.01.2021]</p> <p>Animationsfilm aus Lego, der die Geschichte der Kryptographie bis in die Gegenwart zusammenfasst.</p> | Video |
| <p>Simon Singh (2004). <i>Codes: die Kunst der Verschlüsselung. Geschichte – Geheimnisse – Tricks</i>. dtv.</p> | Buch |

| | |
|---|---|
| <p>Lebendig wie in einem Roman erzählt Simon Singh die Entwicklung der Kryptographie und gibt Einblicke in verschiedene Verfahren der Kryptographie und Kryptoanalyse. Es handelt sich um die Jugendbuch-Version des Buchs <i>Geheime Botschaften</i> vom gleichen Autor (s. [12]).</p> | |
| <p>Wissensfabrik. IT2School-Materialien: Modul A2: Kryptologie https://www.wissensfabrik.de/downloadmaterial-it2school/#modul-a2-kryptologie [Datum des Zugriffs: 19.01.2021]</p> <p>Im Kontext einer Detektivgeschichte erarbeiten sich die Schüler*innen unterschiedliche Aspekte zur Kryptographie und Kryptoanalyse. Über die Carl von Ossietzky Universität Oldenburg können die IT2School Materialien ohne Anmeldung heruntergeladen werden: https://cs.uol.de/s/CdkRCgRtgB8YZ3F [Datum des Zugriffs: 19.01.2021]</p> | <p>Material für eine Unterrichtseinheit</p> |

Literatur

- [1] Beutelspacher, A. (2009). *Kryptologie. Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen*. 9. Aufl. Vieweg + Teubner.
- [2] Bies, F. (2019). Mögliche Entschlüsselungen der Beale-Chiffre und Bewertung von Klartexten. <https://www.jugend-forscht.de/projektdatenbank/moegliche-entschuesselungen-der-beale-chiffre-und-bewertung-von-klartexten.html> [Datum des Zugriffs: 27.01.2021]
- [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] Gallenbacher, J. (2008). *Abenteuer Informatik*. (2. Aufl.) Spektrum Akademischer Verlag: Heidelberg.
- [5] Gpg4win. GNU Privacy Guard for Windows. <https://www.gpg4win.de/> [Datum des Zugriffs: 27.01.2021]
- [6] GPG Suite. <https://gpgtools.org/> [Datum des Zugriffs: 19.04.2021]
- [7] Keller-Buttelt, M. (2020). <https://www.inf-schule.de/kids/datennetze/verschluesselung> [Datum des Zugriffs: 19.01.2021]
- [8] Niedersächsisches Kultusministerium (2014). *Kerncurriculum für die Schulformen des Sekundarbereichs I Schuljahrgänge 5 – 10. Informatik*. Hannover: Unidruck
- [9] Modrow, E. & Strecker, S. (2016). *Didaktik der Informatik*. De Gruyter: Berlin, Bosten
- [10] Rose, S. für ZDFinfo (2015). *Der Schatz des Thomas Beale*. <https://www.youtube.com/watch?v=OHINq97oISQ> [Datum des Zugriffs: 27.01.2021]
- [11] Schmech, K. (2007). *Die Jäger des verschlüsselten Schatzes*. <https://www.heise.de/tp/features/Die-Jaeger-des-verschluesselten-Schatzes-3416489.html> [Datum des Zugriffs: 05.05.2021]
- [12] Singh, S. (2012). *Geheime Botschaften*. 11. Aufl. dtv: München.
- [13] Universität Siegen (2021). *Lernsoftware FILIUS*, Version 1.11.0. <https://www.lernsoftware-filius.de/> [Datum des Zugriffs: 27.01.2021]
- [14] Wissensfabrik. IT2School-Materialien: Modul A2: Kryptologie
<https://www.wissensfabrik.de/downloadmaterial-it2school/#modul-a2-kryptologie> [Datum des Zugriffs: 19.01.2021]



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 meines Namens, jedoch keinerlei Bearbeitung oder kommerzielle Nutzung.