Symmetrische Verschlüsselungsverfahren in der Qualifikationsphase
Didaktische Hinweise

Zielgruppe & Voraussetzungen

Die Materialien richten sich an Schüler*innen in der Qualifikationsphase, die einen Informatikkurs auf grundlegendem oder erhöhtem Niveau belegt haben. Die Materialien bauen auf den Kompetenzen auf, die im Modul *Kryptologie* im niedersächsischen Kerncurriculums für die gymnasiale Oberstufe[1] zum Erwerb in der Einführungsphase vorgesehen sind. Ein entsprechendes Materialpaket für die Einführungsphase steht ebenfalls zur Verfügung.

In AB04_Kryptoanalyse Vigenère werden außerdem grundlegende Kompetenzen beim Umgang mit Snap![2] vorausgesetzt. Wird im Unterricht eine andere Programmierumgebung genutzt, muss das vorhandene Snap!-Programm ggf. von der Lehrkraft in diese Programmiersprache übersetzt werden.

Lernziele

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

Die Schülerinnen und Schüler …

- beschreiben das Prinzip der Transposition und der Substitution zur Verschlüsselung von Daten.
- implementieren monoalphabetische Verfahren, u. a. Caesar-Verfahren.
- erläutern das Prinzip der Häufigkeitsanalyse.
- beschreiben das Prinzip der polyalphabetischen Substitution, u. a. am Beispiel des Vigenère-Verfahrens.
- beurteilen die Sicherheit eines gegebenen symmetrischen Verschlüsselungsverfahrens.

Erweiterung für eA:

- entwerfen und implementieren ein symmetrisches Verschlüsselungsverfahren.

Zu beachten ist, dass sich die Materialien zwar am niedersächsischen Kerncurriculum für die gymnasiale Oberstufe orientieren, jedoch keinen Anspruch auf Vollständigkeit hinsichtlich der für die Abiturprüfung erwarteten Kompetenzen erheben. Die Autorinnen haben zum Teil individuelle Schwerpunkte gesetzt, die auch über die im KC geforderten Kompetenzen hinausgehen können. Verbindlich für das Abitur in Niedersachsen sind allein das niedersächsische Kerncurriculum für die gymnasiale Oberstufe sowie die ergänzenden Hinweise[3] in der jeweils aktuellen Fassung. Es obliegt daher den jeweiligen Fachlehrer*innen, den Unterricht so zu gestalten, dass die Schüler*innen umfassend auf

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

[2] Snap*!* wird von der University of California, Berkeley zur Verfügung gestellt: https://snap.berkeley.edu

[3] Niedersächsisches Kultusministerium (Hrsg.) (2018) *Ergänzende Hinweise zum Kerncurriculum Informatik für die gymnasiale Oberstufe am Gymnasium, an der Gesamtschule sowie für das Kolleg.* https://cuvo.nibis.de/cuvo.php?p=download&upload=174 [Datum des Zugriffs: 01.09.2020]

das Abitur vorbereitet werden. Die vorliegenden Materialien stellen somit nur eine Anregung dar, die an die individuellen Bedürfnisse der Lerngruppe angepasst werden müssen.

Didaktische Anmerkungen zu den Arbeitsblättern

Mithilfe der Aufgaben in *AB01_Kryptologie_Wdh* können die Inhalte aus Jahrgang 11 wiederholt werden. Es bietet sich dabei ein Austausch in Kleingruppen an, damit die Schüler*innen ihr Vorwissen gegenseitig ergänzen können. Für eine Sicherung und anschließende Besprechung im Plenum kann z. B. jede Kleingruppe die Lösung zu einer Aufgabe in einem kollaborativen Dokument festhalten. Aufgabe 6 ist optional und stellt bereits eine Überleitung zu den Inhalten in Jahrgang 12 her. Wenn die Schüler*innen hier keine eigenen Ideen haben, sollten diese nicht vorgegeben, sondern mithilfe des Gruppenpuzzles in AB02 erarbeitet werden.

Das Gruppenpuzzle in AB02 sieht die Erarbeitung verschiedener Substitutionsverfahren vor. An diesen Beispielen können dann sowohl die Unterschiede zwischen einfacher, homophoner und polyalphabetischer Substitution herausgearbeitet werden, als auch die jeweilige Sicherheit in Bezug auf den Angriff durch eine Häufigkeitsanalyse. Als zweites Beispiel für ein polyalphabetisches Verfahren sind dabei die Rotoren aus dem Spioncamp der Uni Wuppertal[4] vorgesehen. Die Rotoren sollten im Vorfeld einmal vorbereitet werden und können dann in verschiedenen Lerngruppen genutzt werden. Die Materialien stehen über die folgenden Links zur Verfügung:

- https://ddi.uni-wuppertal.de/website/repoLinks/v277_substitution-p-rotor-station.pdf
- https://ddi.uni-wuppertal.de/website/repoLinks/v249_substitution-p-rotor-mat0.pdf
- https://ddi.uni-wuppertal.de/website/repoLinks/v299_substitution-p-rotor-ab1.pdf

Das Vigenère -Verfahren, das im Gruppenpuzzle erarbeitet wird, und eine Einordnung als polyalphabetisches Verfahren werden im niedersächsischen Abitur verbindlich vorausgesetzt. Hier ist daher eine zusätzliche Festigung sinnvoll, beispielsweise mit AB03 als Hausaufgabe oder als Inhalt einer Folgestunde.

AB04 bietet eine Vertiefung des Vigenère-Verfahrens hinsichtlich der Möglichkeiten der Kryptoanalyse an. Die Rekonstruktion des Klartextes zu einem Geheimtext, der mit dem Vigenère -Verfahren erstellt wurde und zu dem zwar nicht der Schlüssel, aber die Schlüssellänge bekannt ist, wird im Kerncurriculum nicht explizit als Kompetenz aufgelistet. Entsprechende Überlegungen fördern aber die Kompetenz „Die Schülerinnen und Schüler beurteilen die Sicherheit eines gegebenen symmetrischen Verschlüsselungsverfahrens“ und bieten sich damit als ergänzendes Material an.

AB05 fördert ebenfalls die Kompetenz, ein gegebenes Verfahren hinsichtlich der Sicherheit zu beurteilen, indem exemplarisch ein Transpositionsverfahren angewendet und untersucht wird.

Abschließend dient AB06 einer Systematisierung der Angriffsmöglichkeiten bei symmetrischen Verschlüsselungsverfahren, insbesondere bei den verschiedenen Arten der Substitution. Anhand des in Aufgabe 1 erarbeiteten Schemas können in Aufgabe 2 dann weitere Substitutionsverfahren hinsichtlich ihrer Sicherheit untersucht werden. Insbesondere für Kurse auf erhöhtem Niveau bietet sich an dieser Stelle auch der Entwurf eines eigenen Verschlüsselungsverfahrens an. Dabei können

[4] Didaktik der Informatik an der Bergischen Universität Wuppertal (2012). Spioncamp. https://ddi.uni-wuppertal.de/www-madin//material/spioncamp.html [Datum des Zugriffs: 08.01.2024], speziell:

die Schüler*innen ihre bisherigen Erfahrungen nutzen, die sie bei der Untersuchung bekannter Verfahren gemacht haben, um ein möglichst sicheres Verfahren zu entwerfen bzw. die Sicherheit ihres eigenen Verfahrens einzuschätzen. Aufgabe 3 leitet den Entwurf eines eigenen Verfahrens daher entsprechend an.

Über die Arbeitsblätter dieses Materialpakets hinaus bieten sich die Abituraufgaben vergangener Jahre an, um die Kompetenzen im Modul Kryptologie anhand verschiedener Verschlüsselungs-verfahren zu festigen und zu vertiefen.

Kryptologie und Algorithmik

Kryptographische Verfahren stellen einen geeigneten Kontext dar, um verschiedene algorithmische Kompetenzen zu vertiefen und zu festigen: Für das Caesar- und das Vigenère-Verfahren reicht der Umgang mit Zeichenketten aus, während für eine beliebige monoalphabetische Substitution der Einsatz einer Reihung von Vorteil ist. Einfache Transpositionsverfahren lassen sich nur mithilfe von Zeichenkettenoperation realisieren, während für das Transpositionsverfahren aus AB05 der Einsatz von zweidimensionalen Reihungen hilfreich ist. Wenn die Lerngruppe bereits über die algorithmischen Grundlagen verfügt, können verschiedene Verschlüsselungs-verfahren begleitend zum Thema Kryptologie auch implementiert werden, um die entsprechenden Kompetenzen im algorithmischen Problemlösen zu festigen. Die Arbeitsblätter AB03 und AB05 enthalten Aufgaben, die eine Implementierung des jeweiligen Verfahrens vorsehen.

Wird das Thema Kryptologie bereits zu Beginn der Qualifikationsphase Unterricht, wenn noch nicht alle algorithmischen Kompetenzen erarbeitet wurden, können die Aufgaben zur Implementierung auch erst zurückgestellt werden. Sie sind daher mit einem Stern gekennzeichnet. Entsprechende Aufgaben zur Implementierung verschiedener Verfahren können dann aufgegriffen werden, wenn die jeweiligen algorithmischen Kompetenzen erarbeitet werden. Die Leitfäden zum Thema Zeichenkettenverarbeitung[5] sowie zu „Reihungen in Processing und Java“ enthalten ebenfalls entsprechende Aufgaben zur Implementierung kryptographischer Verfahren und auch zu Aspekten der Häufigkeitsanalyse.

Für Kurse auf erhöhtem Niveau sieht das niedersächsische Kerncurriculum auch die Implementierung eines eigenen Verschlüsselungsverfahrens vor. Dies kann mit Arbeitsblatt AB_06 vorbereitet werden und dann in einem größeren Programmierprojekt münden. Die Aufgabe 3, insbesondere 3c) zur Implementierung des selbst entworfenen Verfahrens richtet sich daher vor allem an Kurse auf erhöhtem Niveau.

[5] für Processing enthalten im Materialpaket Einstieg in die textbasierte Programmierung mit Processing