Unterrichtsmaterialien in digitaler und in gedruckter Form

Auszug aus:

Grundlagen der Kryptographie

Das komplette Material finden Sie hier:

School-Scout.de

A.I.11

Information und Daten – Unterrichtseinheit

Grundlagen der Kryptographie – Klassische symmetrische Verschlüsselungsverfahren

Ein Beitrag von Johann Georg Vogelhuber

Anhand einfacher und historisch relevanter Chiffren betrachten ihre Schülerinnen und Schüler ausgehend von der klassischen Cäsar-Verschlüsselung einige mono- und polyalphabetische Verschlüsselungen. Dabei werden die Grundbegriffe der Kryptographie und die fundamentale Idee der symmetrischen Verschlüsselung erarbeitet. Neben den Verfahren selbst erhalten die Schülerinnen und Schüler auch einen spannenden Einblick in deren Sicherheit und entwickeln mögliche Angriffe, um diese Chiffren zu entziffern. Zur Untersuchung der Sicherheit werden die Häufigkeitsanalyse von Buchstaben und Bigrammen sowie der Kasiski-Test zur Ermittlung der Schlüssellänge thematisiert.

KOMPETENZPROFIL

LEARNING Snacks

Klassenstufe:	9–11 (in Teilen auch: 7/8)
Dauer:	5–8 Unterrichtsstunden
Lernziele:	Die Lernenden 1. ver- und entschlüsseln mithilfe mono- und polyalphabetischer Verschlüsselungsverfahren, 2. argumentieren, indem sie verschiedene Chiffren und deren Sicherheit begründet miteinander vergleichen, 3. kommunizieren und kooperieren, indem sie untereinander verschlüsselte Nachrichten austauschen.
Thematische Bereiche:	Kryptographie, Kryptoanalyse, symmetrische Verschlüsselungsverfahren, Cäsar-Verschlüsselung, Häufigkeitsanalyse, Kasiski-Test
Kompetenzen:	Argumentieren, Kommunizieren und Kooperieren

A.I.11

Information und Daten – Unterrichtseinheit

Grundlagen der Kryptographie – Klassische symmetrische Verschlüsselungsverfahren

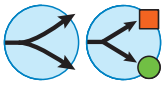
Ein Beitrag von Johann-Georg Vogelhuber

Anhand einfacher und historisch relevanter Chiffren betrachten Ihre Schülerinnen und Schüler ausgehend von der klassischen Cäsar-Verschlüsselung einige mono- und polyalphabetische Verschlüsselungen. Dabei werden die Grundbegriffe der Kryptographie und die fundamentale Idee der symmetrischen Verschlüsselung erarbeitet. Neben den Verfahren selbst erhalten die Schülerinnen und Schüler auch einen spannenden Einblick in deren Sicherheit und entwickeln mögliche Angriffe, um diese Chiffren zu entziffern. Zur Untersuchung der Sicherheit werden die Häufigkeitsanalyse von Buchstaben und Bigrammen sowie der Kasiski-Test zur Ermittlung der Schlüssellänge thematisiert.

KOMPETENZPROFIL

Klassenstufe:	9–11 (in Teilen auch: 7/8)
Dauer:	5–8 Unterrichtsstunden
Lernziele:	Die Lernenden 1. ver- und entschlüsseln mithilfe mono- und polyalphabetischer Verschlüsselungsverfahren, 2. argumentieren, indem sie verschiedene Chiffren und deren Sicherheit begründet miteinander vergleichen, 3. kommunizieren und kooperieren, indem sie untereinander verschlüsselte Nachrichten austauschen.
Thematische Bereiche:	Kryptographie, Kryptoanalyse, symmetrische Verschlüsselungsverfahren, Cäsar-Verschlüsselung, Häufigkeitsanalyse, Kasiski-Test
Kompetenzen:	Argumentieren, Kommunizieren und Kooperieren

Symbolerklärungen

	Diese Symbole markieren eine Einzel-, Partner- bzw. Gruppenarbeit.
	Diese Symbole markieren alternative Durchführungsmöglichkeiten bzw. alternative Durchführungsmöglichkeiten nach Niveaustufen.
	Tauchen diese Symbole auf, handelt es sich um binnendifferenzierte Materialien.
	Dieses Symbol markiert Materialien auf einfacherem G-Niveau bzw. Materialien eher für niedrigere Klassenstufen.
	Dieses Symbol markiert Materialien auf Normalniveau (M-Niveau).
	Dieses Symbol markiert Materialien auf höherem E-Niveau bzw. Materialien eher für höhere Klassenstufen oder Exkursmaterialien.
	Dieses Symbol markiert Hilfestellungen bzw. Tipps.
	Dieses Symbol markiert Zusatzaufgaben für schnelle Lernende.
	Dieses Symbol markiert Merkkästen und wichtige Inhalte.
	Dieses Symbol markiert am Laptop/PC zu bearbeitende Aufgaben.
	Dieses Symbol taucht auf, wenn ein Dateidownload notwendig ist.
	Dieses Symbol markiert interaktive Aufgaben zur Bearbeitung mit einem digitalen Endgerät.
	Dieses Symbol markiert das Einbinden eines Videos/Films.
	Dieses Symbol markiert eine Internetrecherche.
	Dieses Symbol taucht auf, wenn näher recherchiert werden soll oder tiefergreifende Informationen hinterlegt sind.
	Diese Symbole markieren Pro- und Kontraargumente bzw. eine Diskussion.
	Dieses Symbol markiert Aufgaben zum Ankreuzen.
	Dieses Symbol markiert Aufgaben, bei denen gerechnet werden muss.

Wie kann die Erarbeitung des Themas im Unterricht erfolgen?

Vorbereitung

- Stellen Sie ausreichend Tablets/Laptops für die Aufgaben zur Entzifferung der Geheimtexte zur Verfügung, idealerweise ein Gerät pro Schülerpaar.
- Stellen Sie ausreichend Tablets/Smartphones mit Internetzugang für die Verwendung der verlinkten Onlinetools zur Verfügung, idealerweise ein Gerät pro Schülerpaar.

Benötigte Dateien

- *Bilanz2021.xlsx* (Für Aufgabe 2 in **M 1**)
- *MonoalphabetischeSubstitution.xlsx* (Für Aufgabe 2 in **M 7**)

Varianten der Durchführung

Im Unterrichtsverlauf können, je nach verfügbarer Zeit und Leistungsstärke der Klasse, die Aufgaben zur Entzifferung der verschiedenen Chiffren ausgelassen werden. So eignet sich das Material beispielsweise auch für die Klassenstufen 7/8. Dazu können Sie als Lehrkraft auch alternativ die Entzifferung der jeweiligen Verschlüsselungen vorführen. Beispielsweise kann die Klasse einen Geheimtext erstellen, der dann von Ihnen als Lehrkraft entziffert wird. Dabei sollte darauf geachtet werden, dass der Geheimtext ausreichend lang ist. So wird auch die Notwendigkeit für bessere Verschlüsselungsverfahren deutlich.

Tipp: Zur Entzifferung der verschiedenen Chiffren oder zur Kontrolle der Schülerlösungen können folgende Webseiten hilfreich sein:

Link	Beschreibung
https://cryptii.com	Nützliche Seite, um diverse Chiffren auszuprobieren. Kann gut verwendet werden, um alle Möglichkeiten der Cäsar-Verschlüsselung schnell auszuprobieren.
https://www.guballa.de/substitution-solver	Tool zum automatisierten Entziffern von Geheimtexten, die mit einer monoalphabetischen Verschlüsselung erzeugt wurden.
https://www.guballa.de/vigenere-solver	Tool zum automatisierten Entziffern von Geheimtexten, die mit dem Vigenère-Verfahren verschlüsselt wurden.

Einstieg

Der Einstieg in die Unterrichtseinheit erfolgt mit der in **M 1** vorgestellten Handlungssituation, in der die dringend benötigten Zugangsdaten für ein wichtiges Dateidokument nur in verschlüsselter Form vorliegen. Neben den verschlüsselten Daten gibt es eine zusätzliche Tabelle mit zwei verschobenen Alphabeten. Die Schülerinnen und Schüler sollen zunächst die Situation analysieren und in Partnerarbeit einen Handlungsplan für das weitere Vorgehen entwickeln. Dazu können die Analysefragen auf dem Arbeitsblatt verwendet werden. Anschließend versuchen die Schülerinnen und Schüler, das benötigte Passwort aus den gegebenen Informationen zu rekonstruieren. Zur Kontrolle der Ergebnisse überprüfen die Lernenden ihre Lösung, indem sie die Datei *Bilanz2021.xlsx* unter dem oben bzw. auf dem Arbeitsblatt genannten Link bzw. QR-Code herunterladen und ihr Ergebnis zum Öffnen der Datei verwenden.

In dieser Unterrichtsphase sollen die Schülerinnen und Schüler bewusst mit den vorhandenen Daten experimentieren und versuchen, selbstständig einen Lösungsansatz für das vorliegende Problem zu finden. So können sie ein erstes Verständnis für unbekannte Verschlüsselungen entwickeln. Bei Bedarf kann über den QR-Code bzw. Link auf dem Arbeitsblatt eine kurze Hilfestellung in Form eines Erklärvideos abgerufen werden.

An die Bearbeitung des Arbeitsauftrags sollte sich eine kurze Präsentations- und Reflexionsphase anschließen, in der unterschiedliche – auch ggf. nicht erfolgreiche – Lösungsansätze vorgestellt und bewertet werden.

Ausgehend von diesen Erfahrungen werden die ersten Begriffe der Kryptographie mithilfe des Arbeitsblatts **M 2** erarbeitet und die Verwendungsweise des Cäsar-Verfahrens eingeübt.

Als Motivation und Überleitung zur Erarbeitung von mono- und polyalphabetischen Verschlüsselungsverfahren bewerten die Schülerinnen und Schüler die Sicherheit des Cäsar-Verfahrens, indem sie mithilfe von **M 3** versuchen, eine Chiffre ohne gegebenen Schlüssel zu entziffern. Dazu sollen sie zunächst mit Aufgabe 1 mögliche Lösungsansätze zur Entzifferung entwickeln, die anschließend in den folgenden Aufgaben erprobt werden.

Erarbeitung

In der sich anschließenden Erarbeitungsphase der Unterrichtseinheit betrachten die Schülerinnen und Schüler zunächst drei verschiedene monoalphabetische Substitutionen in Form eines Gruppenpuzzles (**M 4**). Dazu wird für jedes Verschlüsselungsverfahren in Expertengruppen ein kurzer Steckbrief erstellt (**M 5**), den sich die Schülerinnen und Schüler in den Stammgruppen gegenseitig vorstellen. Nach dem Abschluss des Gruppenpuzzles sollte eine kurze Reflexion durchgeführt werden, in der die Erfahrungen während der vorangegangenen Arbeitsphase thematisiert werden. In dieser Phase sollte auch die Gemeinsamkeit der drei vorgestellten Verfahren herausgearbeitet und der Begriff der „monoalphabetischen Substitution“ eingeführt und erläutert werden, um den Schülerinnen und Schülern zu verdeutlichen, dass hinter allen drei Chiffren dieselbe Idee zur Verschlüsselung steckt und alle Chiffren demnach dieselbe Stärke bzw. Schwäche haben, unabhängig von den verwendeten Symbolen.

Davon ausgehend kann mit den Materialien **M 6** und **M 7** die Sicherheit dieser Verfahren analysiert werden. Dazu führen die Schülerinnen und Schüler eine Häufigkeitsanalyse für einen gegebenen Quelltext durch und rekonstruieren so den ursprünglichen Geheimtext. Auch hier sollte sich eine Reflexionsphase anschließen, in der die Schwächen der monoalphabetischen Substitution für deutschsprachige Klartexte herausgearbeitet werden. Die statistischen Eigenschaften des Textes werden durch die Verschlüsselung nicht verschleiert und ermöglichen so eine Rekonstruktion des Klartextes.

Durch diese Angriffsmöglichkeit auf monoalphabetische Substitutionen motiviert, wird dann in ähnlicher Weise das Vigenère-Verfahren erarbeitet (**M 8**) und untersucht (**M 9**). Die Schritte zur Ermittlung der Schlüssellänge werden dabei aus Gründen der didaktischen Reduktion durch ein Onlinetool durchgeführt. Ähnlich zu den vorangegangenen Erarbeitungsschritten bietet sich auch hier eine gemeinsame Plenumsphase zur Reflexion und Bewertung des Verfahrens an.

Ergebnissicherung

Zur abschließenden Ergebnissicherung der Unterrichtseinheit kann das Material **M 10** verwendet werden. Hier müssen die Schülerinnen und Schüler die wichtigsten Konzepte und Ideen noch einmal in eigenen Worten zusammenfassen. Zusätzlich können sie über den verlinkten *LearningSnack* individuell ihren Lernerfolg überprüfen.

Auf einen Blick

Benötigt

☐ Tablet/Laptop pro Schülerpaar für die Aufgaben zur Entzifferung der Geheimtexte
☐ Tablet/Smartphone mit Internetzugang pro Schülerpaar zur Verwendung verlinkter Onlinetools

Einstieg

Thema: Monoalphabetische Verschlüsselung

M 1 **Wie lautet das Passwort? – Einstieg in die Verschlüsselung**

Benötigt: *Bilanz2021.xlsx*

M 2 **Das Cäsar-Verfahren**
M 3 **Wie sicher ist das Cäsar-Verfahren?**

Erarbeitung

Thema: Vergleich der Funktion und Sicherheit verschiedener monoalphabetischer Verschlüsselungsverfahren

M 4 **Symmetrische Verschlüsselungsverfahren – Informationen**
M 5 **Symmetrische Verschlüsselungsverfahren – Steckbrief**
M 6 **Häufigkeitsanalyse für monoalphabetische Verschlüsselungen**
M 7 **Wie schwer ist die Entzifferung monoalphabetischer Substitutionschiffren?**

Benötigt: *MonoalphabetischeSubstitution.xlsx*

Thema: Polyalphabetische Verschlüsselung mit dem Vigenère-Verfahren

M 8 **Das Vigenère-Verfahren als Beispiel für eine polyalphabetische Substitution**
M 9 **Entzifferung des Vigenère-Verfahrens**

Ergebnissicherung

Thema: **Zusammenfassende Übungsaufgaben**

M 10 **Zusammenfassung zu symmetrischen Verschlüsselungsverfahren**

Benötigte Dateien

☐ *Bilanz2021.xlsx*
☐ *MonoalphabetischeSubstitution.xlsx*

Unterrichtsmaterialien in digitaler und in gedruckter Form

Auszug aus:

Grundlagen der Kryptographie

Das komplette Material finden Sie hier:

School-Scout.de

A.I.11

Information und Daten – Unterrichtseinheit

Grundlagen der Kryptographie – Klassische symmetrische Verschlüsselungsverfahren

Ein Beitrag von Johann Georg Vogelhuber

Anhand einfacher und historisch relevanter Chiffren betrachten ihre Schülerinnen und Schüler ausgehend von der klassischen Cäsar-Verschlüsselung einige mono- und polyalphabetische Verschlüsselungen. Dabei werden die Grundbegriffe der Kryptographie und die fundamentale Idee der symmetrischen Verschlüsselung erarbeitet. Neben den Verfahren selbst erhalten die Schülerinnen und Schüler auch einen spannenden Einblick in deren Sicherheit und entwickeln mögliche Angriffe, um diese Chiffren zu entziffern. Zur Untersuchung der Sicherheit werden die Häufigkeitsanalyse von Buchstaben und Bigrammen sowie der Kasiski-Test zur Ermittlung der Schlüssellänge thematisiert.

KOMPETENZPROFIL

LEARNING Snacks

Klassenstufe:	9–11 (in Teilen auch: 7/8)
Dauer:	5–8 Unterrichtsstunden
Lernziele:	Die Lernenden 1. ver- und entschlüsseln mithilfe mono- und polyalphabetischer Verschlüsselungsverfahren, 2. argumentieren, indem sie verschiedene Chiffren und deren Sicherheit begründet miteinander vergleichen, 3. kommunizieren und kooperieren, indem sie untereinander verschlüsselte Nachrichten austauschen.
Thematische Bereiche:	Kryptographie, Kryptoanalyse, symmetrische Verschlüsselungsverfahren, Cäsar-Verschlüsselung, Häufigkeitsanalyse, Kasiski-Test
Kompetenzen:	Argumentieren, Kommunizieren und Kooperieren