A.I.11

Information und Daten – Unterrichtseinheit

Grundlagen der Kryptographie – Klassische symmetrische Verschlüsselungsverfahren

Ein Beitrag von Johann-Georg Vogelhuber

© alengo/E+

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

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**

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

Situationsbeschreibung

In der Entwicklungsabteilung der MeViTo GmbH wird Sicherheit großgeschrieben. Alle Dokumente müssen mit einem sicheren Passwort verschlüsselt werden. Zudem ist es nicht erlaubt, diese Passwörter zu notieren. Nachdem der langjährige Mitarbeiter Herr Schneider in den Ruhestand verabschiedet wurde, soll die Auszubildende Marie eine Übersicht über die vorhandenen Dokumente erstellen, um den aktuellen Stand der Arbeitsergebnisse von Herrn Schneider zu überprüfen. Dabei stellt Marie fest, dass ihr die Passwörter zum Öffnen der zugehörigen Dateien fehlen. Da Herr Scheider zuletzt sehr vergesslich war, vermutet sie, dass doch Aufzeichnungen zu den Passwörtern existieren. Leider findet sie nur einen Notizzettel (siehe links) mit merkwürdigen Buchstabenfolgen und eine Tabelle (siehe unten) auf der Unterseite von Herrn Schneiders Computertastatur.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F

CRUX: SAKTINKTLAYYHGRR
KDIKR:YINTKOJKXXKTZK2021

Aufgabe 1

Arbeitet in Partnerarbeit. Analysiert die Ausgangssituation und versucht einen Lösungsweg zu entwickeln. Nutzt dabei die unten angegebenen Analysefragen und beantwortet diese.

Analyse

Welche Aufgabe hat Marie?

Welche Informationen hat sie zur Verfügung?

Wie könnte sie dazu vorgehen?

Aufgabe 2

Versucht die Datei *Bilanz2021.xlsx* mithilfe der gegebenen Informationen zu öffnen. Notiert eure Lösungsansätze und ob diese erfolgreich waren.

Symmetrische Verschlüsselungsverfahren – Informationen

M 4

Das Cäsar-Verfahren ist nicht besonders sicher. Es kann mit geringem Aufwand entziffert werden. Um Nachrichten sicher übermitteln zu können, müssen also bessere Verfahren zur Verschlüsselung gefunden werden. Mit der folgenden Gruppenarbeit werden drei symmetrische Chiffren untersucht.

Aufgabe 1

Teilt euch in Dreier-Gruppen auf. Legt gemeinsam fest, wer sich mit welchem der drei Verschlüsselungsverfahren beschäftigt. Notiert die Namen der Verantwortlichen in der Tabelle.

Chiffre	Wer ist verantwortlich?
Freimaurer-Alphabet	
Polybios-Chiffre	
Aristocrat-Chiffre	

Aufgabe 2

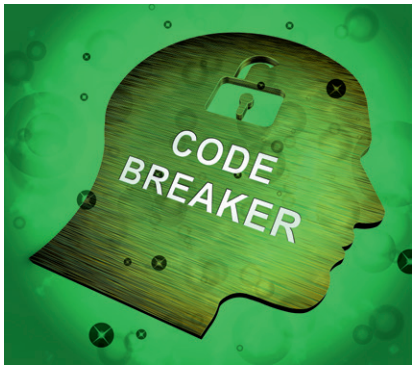
Jeder von euch macht sich so schnell wie möglich zu einem Experten für das gewählte Verschlüsselungsverfahren. Dazu bildet ihr Expertengruppen aus maximal vier Personen für die einzelnen Chiffren. Informationen zu den einzelnen Verfahren können von euch über die unten angegebenen QR-Codes bzw. Links abgerufen werden. In den Expertengruppen wird gemeinsam eine Übersicht zum gewählten Thema erstellt, indem ihr das Arbeitsblatt **M 5** ausfüllt.

Chiffre	Erklärvideo	Ausführliche Erläuterungen
Freimaurer-Alphabet	https://raabe.click/Freimaurer-Alphabet-Erklaervideo	https://raabe.click/Freimaurer-Alphabet-Erlaeuterungen
Polybios-Chiffre	https://raabe.click/Polybios-Chiffre-Erklaervideo	https://raabe.click/Polybios-Chiffre-Erlaeuterungen
Aristocrat-Chiffre		https://raabe.click/Aristocrat-Chiffre-Erklaerungen

Aufgabe 3

Findet euch in den ursprünglichen Dreier-Gruppen zusammen. Erklärt euch gegenseitig die Verschlüsselungsverfahren und bearbeitet die von euren Mitschülern erstellten Übungsaufgaben.

M 9 Entzifferung des Vigenère-Verfahrens



© stuartmiles99/iStock/Getty Images Plus

Die Vigenère-Verschlüsselung galt viele Jahrhunderte als sicher. Allerdings hat dieses Verfahren eine Schwachstelle, die eine Entzifferung ermöglicht. Mit den nächsten Aufgaben lernst du, wie man das Vigenère-Verfahren brechen kann.

Als Beispiel betrachten wir den folgenden Geheimtext:

Cqullh Rwzy hej gphpv vgy ytrxnbmdvwkjbdxwp kyfxkeoyy Ijhphoij. Gy yyxokjepplg 1941 kcp ijuay qyfmaczrkhhysmyg, wlzkjctgrikvlopvlg, mlpm htvaceeopycfstl Lpgzguglwujphp mf dphlijgy Awiavwoyoltlwsrmpn xpv Ogsn, oif Evgaylgy.

Aufgabe 1

Überlege zunächst, warum man mit einer einfachen Häufigkeitsanalyse aller Buchstaben diesen Geheimtext nicht entschlüsseln kann.

Erklärvideo:

Link:

https://www.youtube.com/watch?v=Y6qimy-9o3f4

Bei der Analyse einer Vigenère-Chiffre ist das wichtigste Ziel die Bestimmung der Schlüssellänge k, denn wenn man diese bestimmt hat, so funktioniert der Rest der Entschlüsselung wie bei einer gewöhnlichen monoalphabetischen Verschlüsselung. Sowohl der Kasiski-Test als auch der Friedmann-Test sind Verfahren zur Bestimmung der Schlüssellänge. Der Kasiski-Test sucht im Geheimtext nach Wiederholungen von Zeichenfolgen und misst deren Abstand. Das Verfahren stützt sich darauf, dass sich ein im Verhältnis zur Textlänge relativ kurzes Schlüsselwort ständig wiederholt.

Aufgabe 2

Ermittle die Schlüssellänge für den obigen Text. Verwende dazu die Seite *Cryptool.org*. Anschließend kannst du die einzelnen Verschiebungen des Alphabets so verändern, dass nach und nach der Text entschlüsselt wird. Dazu werden dir die entsprechenden Häufigkeitsverteilungen angezeigt. Über die Buttons „Links“ und „Rechts“ kannst du die Verschiebung einstellen.

https://raabe.click/cryptpool-vigenerebreak

Tipp: Die wahrscheinlichste Schlüssellänge ist in diesem Fall richtig.
Bei der Auswahl der Verschiebung muss die angezeigte „Autokorrelation“ möglichst klein werden.

Aufgabe 3

Überlege dir, wie man das Vigenère-Verfahren sicher einsetzen kann. Auf welche Dinge muss man achten, damit der beschriebene Angriff nicht so leicht durchzuführen ist?

Teste dein Wissen!

M 10

Markiere eine der Antwortmöglichkeiten für jede Frage oder fülle die Lücken aus. Es können auch mehrere Antwortmöglichkeiten richtig sein.
Alternativ kannst du auch den *LearningSnack* öffnen und dort die Fragen beantworten:
https://raabe.click/LearningSnack-Verschluesselung

Was zeichnet symmetrische Verschlüsselungsverfahren aus?

Sender und Empfänger verwenden den gleichen Schlüssel.	Sender und Empfänger verwenden verschiedene Schlüssel.
Der Geheimtext besteht nur aus symmetrischen Buchstaben.	Der Buchstabe A wird durch B verschlüsselt, B durch C, usw.

Welche der genannten Verfahren sind symmetrische Verschlüsselungsverfahren?

Aristocrat	Diffie-Hellman
RSA	Cäsar

Verschlüssele den folgenden Text mit einer Cäsar-Verschiebung von 3 Stellen:
kryptographie
Verwende nur Großbuchstaben, um deine Lösung in das folgende Feld einzutragen:

_____

Der folgende Text wurde mit dem Cäsar-Verfahren verschlüsselt. Der Schlüssel ist nicht bekannt. Versuche, den Text zu entschlüsseln: RYFWAVHUHSFZL

_____

Mit welchem Verfahren kann man eine monoalphabetische Substitution entziffern?

Friedman-Test	Häufigkeitsanalyse
Kasiski-Test	Autokorrelation

Welches Prinzip verwendet die Vigenère-Verschlüsselung?

Steganographie	Monoalphabetische Substitution
Polyalphabetische Substitution	Sehr komplizierte geheime Symbole