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

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

Auf einen Blick

Benötigt

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

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 sicher ist die Entschlüsselung monoalphabetischer Substitutionschiffren?**

Benötigt: *MonoalphabetischeSubstitution.xlsx*

Thema: Polyalphabetische Verschlüsselung mit dem Vigenère-Verfahren

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

Ergebnissicherung

Thema: **Zusammenfassende Übungsaufgaben**

M 10 **Zusammenfassung zu symmetrischen Verschlüsselungsverfahren**

Benötigte Dateien

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

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 Schneider zuletzt sehr vergesslich war, vermutet sie, dass doch Aufzeichnungen zu den Passwörtern existieren. Leider findet sie nur einen Notizzettel (siehe links) mit merkwürdigen Buchstaben- 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			w	x	y	z
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W		Y	Z	A			D	E	

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 dabei vorgehen?

Aufgabe

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

Das Cäsar-Verfahren

M 2

Die Passwörter in der Einstiegssituation von **M 1** wurden mithilfe des Cäsar-Verfahrens **verschlüsselt**. Dieses Verfahren geht der Legende nach auf den römischen Feldherrn Julius Cäsar zurück (100–44 v. Chr.), der mit diesem Verfahren Geheimbotschaften übermittelte. Er verschlüsselte dabei seine Botschaften, indem er die einzelnen Buchstaben im Alphabet einfach um drei Stellen verschob.

© Murat T... The Image Bank

...klärvideo:

https://raabe.click/...esar-Verfahren

Das Cäsar-Verfahren ist ein Beispiel für ein **symmetrisches** Verschlüsselungsverfahren. Bei einem symmetrischen Verschlüsselungsverfahren haben Absender und Empfänger einer Nachricht denselben **Schlüssel**, mit dem die Nachricht verschlüsselt und entschlüsselt wird. Sie verfügen damit über ein gemeinsames Geheimnis. Absender und Empfänger müssen also vor dem Austausch der verschlüsselten Nachricht diesen gemeinsamen S...sel festlege...

Verschlüsselung mit dem Cäsar-Verfahren

Im Cäsar-Verfahren verschiebt man jeden Buchstaben des **Kla...textes** im Alphabet u...en bestimmten Abstand, z. B. drei Stellen, nach hinten. So erhält ...an den z...gen **Geheimtext**. Dieser Abstand – also im Beispiel drei Buchstaben – ist der geh...schlüssel, d... nur Absender und Empfänger kennen dürfen. Diesen Abstand haben ...ender und Empfänger v...her vereinbart und halten ihn geheim.

Um die Verschlüsselung und auch die Entschlü...ung z... ...n man Klartext- und Geheimtextalphabet in einer Tabelle notieren.

Beispiel: In der folgenden Tabelle wu... das Alphabet um sec...ellen verschoben:

Klartext	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
Geheimtext	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

Aus dem Klartext „kryptogra...“ wird so der G...heimtext „QXEVZUMXGVNOK“.

Entschlüsselung mit ...m Cäsar-V...fahren

Wenn der Empfänger den ...die V...erschlüsselung verwendeten Schlüssel kennt, kann er damit die Verschiebung buchstabenweis... ...der rückgängig machen und damit den Geheimtext entschlüsseln. So erhält ...m Geheimt... ...der den Klartext.

Aufgabe 1

Versch...üsse...den folgenden Te...t mit dem Cäsar-Verfahren und der Verschiebung um fünf Stellen:

dies ist ...e erste ueb... ...n verschluesseln

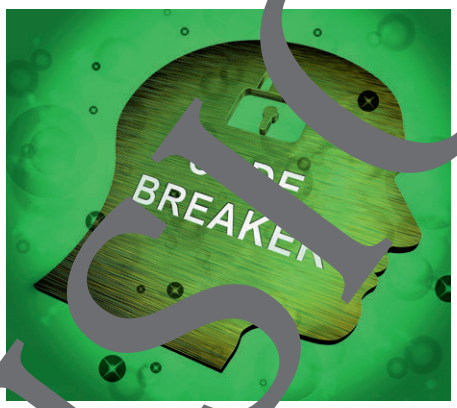
Häufigkeitsanalyse für monoalphabetische Verschlüsselungen

M 6

Monoalphabetische Substitution

Die drei in **M 5** vorgestellten Verfahren haben alle eine Gemeinsamkeit. Jedem Buchstaben des Alphabets wird ein festes Symbol zugeordnet, das diesem Buchstaben im Geheimtext entspricht. D. h. ein bestimmter Buchstabe wird immer durch dasselbe Geheimtextsymbol ersetzt. Di[illegible] Art von Verschlüsselung nennt man auch **monoalphabetische Substitution**.

Durch die Analyse der Buchstabenhäufigkeiten ist es beim Cäsar-Verfahren möglich, den Geheimtextbuchstaben für das ‚e' zu ermitteln und so die Verschiebung des Alphabets zu berechnen. Mit einer **Häufigkeitsanalyse** von einzelnen Buchstaben und von Buchstabenpaaren kann man eine monoalphabetische Substitution ähnlich leicht überwinden wie die Cäsar-Verschlüsselung.



© st[illegible]miles99/iStock[illegible]mages Plus

Die einzelnen Buchstaben kommen in einem deutschen Text unterschiedlich häufig vor. Besonders häufig sind die Buchstaben ‚e', ‚n', ‚i', ‚r', ‚t', ‚s' und ‚a'. Zählt man die Buchstaben im Geheimtext, so wird der häufigste Buchstabe wahrscheinlich dem ‚e', der zweithäufigste Buchstabe dem ‚n' usw. entsprechen. Diese Geheimtext[illegible]uchstaben tauscht man dann durch die vermuteten Klartextbuchstaben aus[illegible]xtstücke, die man durch sinnvolles Vervollständigen und Ausprobieren schnell[illegible]ntziffern kann.

Genauso kann man die Häufigkeit von Buchstabenpaaren (Digrammen) zählen. In deutschen Texten kommen die Kombinationen ‚en', ‚er'[illegible]ch' besonders oft vor.

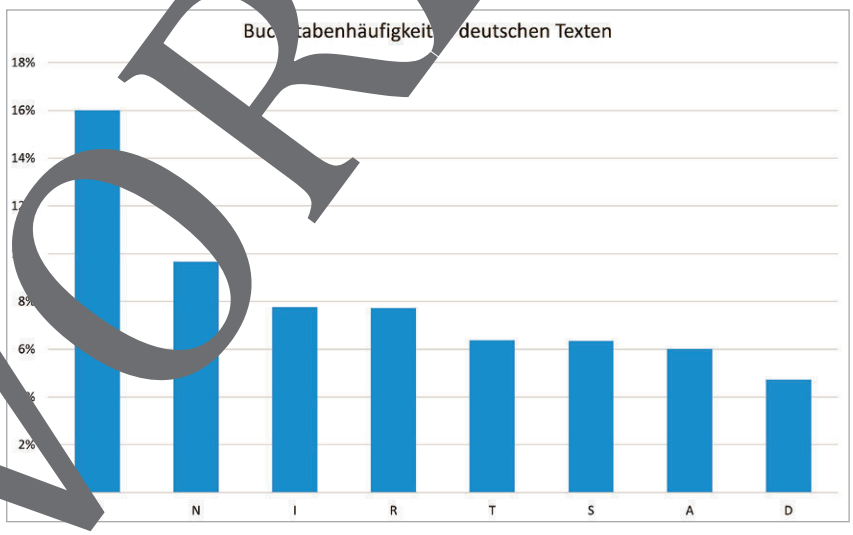
Erklärvideo:

https://raabe.click/Erklaervideo-Buchstabenhaeufigkeit

Die wichtigsten Buchstabenhäufigkeiten sind im nachfolgenden Diagramm dargestellt. Für weitere Tabellen zu einzelnen Häufigkeiten kannst du den entsprechenden *Wikipedia*-Artikel über den verlinkten QR-Code aufrufen.

Wikipedia:

https://raabe.click/Wikipedia-Buchstabenhaeufigkeit

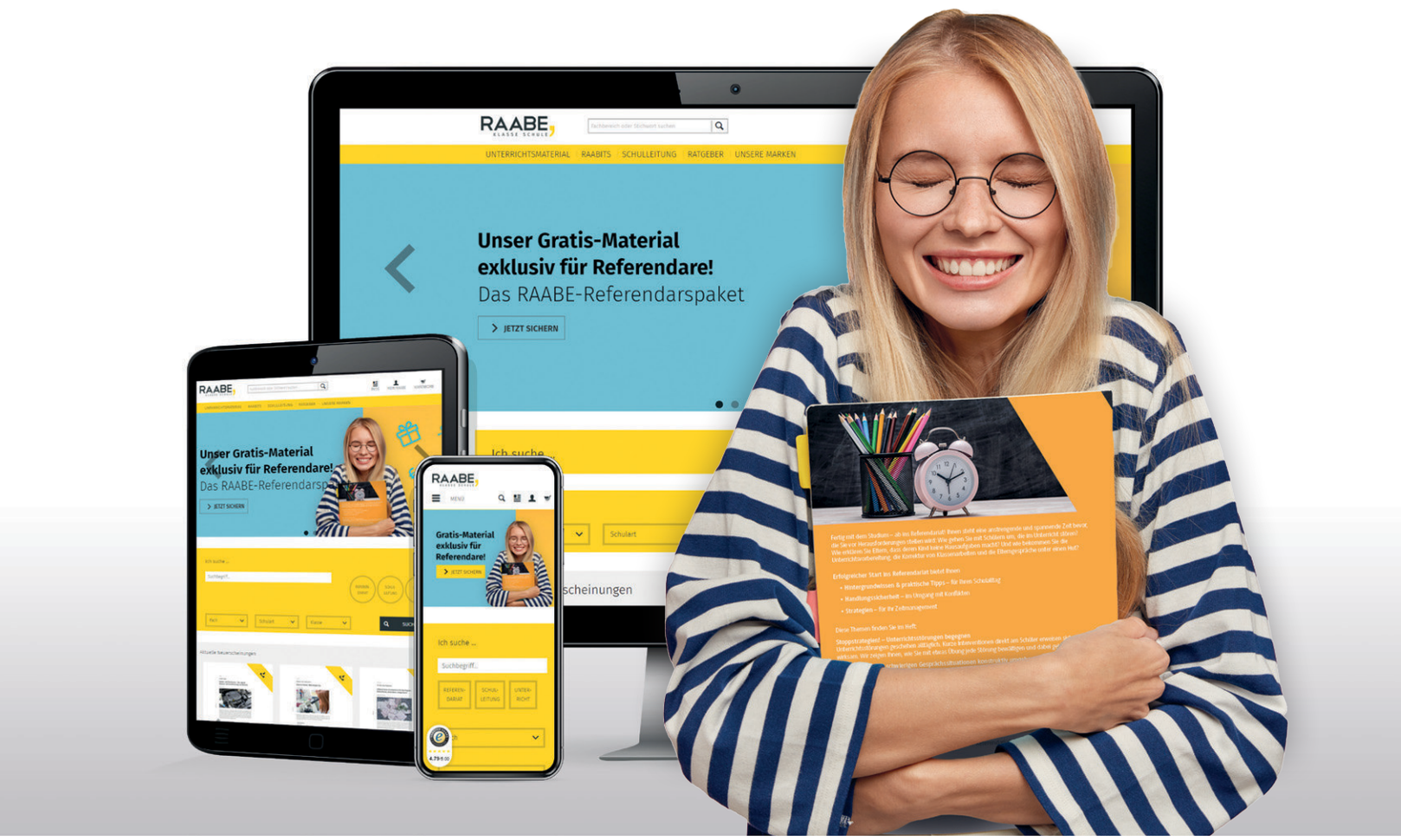


Datenquelle: Leibniz-Institut für Deutsche Sprache,
https://www.ids-mannheim.de/digspra/kl/projekte/methoden/derewo#derechar

RAABE
KLASSE SCHULE

Sie wollen mehr für Ihr Fach?

Bekommen Sie: Ganz einfach zum Download
im RAABE Webshop.



- **Über 5.000 Unterrichtseinheiten**
  sofort zum Download verfügbar
- **Webinare und Videos**
  für Ihre fachliche und
  persönliche Weiterbildung
- **Attraktive Vergünstigungen** für Referendar:innen
  mit bis zu 15% Rabatt
- **Käuferschutz**
  mit Trusted Shops

TRUSTED SHOPS GUARANTEE

Jetzt entdecken:

www.raabe.de