

A.I.10

Information und Daten – Unterrichtseinheit

Einführung in die Kryptographie – Verschlüsselungsmethoden kennenlernen und anwenden

Ein Beitrag von Christina Hund



© Christina Hund

Verschlüsselung war, ist und bleibt wichtig. Während wir schon seit Langem unsere Wertsachen mit Schloss und Schlüssel verschließen, ist uns heutzutage die Sicherheit unserer digitalen Daten wichtig. In dieser als Stationenarbeit durchführbaren Unterrichtseinheit lernen Ihre Schülerinnen und Schüler historische Verschlüsselungen, wie die Gartenzaun-Verschlüsselung, das Freimaurer-Alphabet und die Caesar-Chiffre, kennen und erlangen so Grundlagen, wie digitale Schlüssel funktionieren könnten. Kleine Videos mit eingeblendeten interaktiven Fragen sowie ein interaktiver Test als digitale Lernzielkontrolle runden den motivierenden Unterricht ab.

KOMPETENZPROFIL – UNTERRICHTSEINHEIT

Klassenstufe:	5–7
Dauer:	5–6 Unterrichtsstunden
Lernziele:	Die Lernenden ... 1. definieren die Grundlagen der Verschlüsselung, 2. erstellen Kriterien für ein sicheres Passwort, 3. erläutern analoge Verschlüsselungsverfahren für Nachrichten und wenden diese an, 4. erarbeiten und erklären historische Kryptographie-Maschinen und deren Verschlüsselung am Beispiel „Enigma“.
Thematische Bereiche:	symmetrische Verschlüsselung(-smethoden), Kryptographie, Gartenzaun-Verschlüsselung, Freimaurer-Alphabet, Caesar-Scheibe
Kompetenzbereiche:	Darstellen und Interpretieren, Kommunizieren und Kooperieren, Schützen und sicher Agieren, Probleme lösen und Handeln, Analysieren und Reflektieren

Auf einen Blick

- Laptop/PC/mobiles Endgerät mit Internetanschluss



Einstieg (1 Stunde)

Thema: Einstieg in die Verschlüsselung im Alltag und digital

M 1 **Verschlüsselung oder Kryptographie – Was ist das?**

M 2 **Zettelbotschaften als selbst gemachter Infoschutz**

Benötigt: Video **V 1** <https://raabe.click/Video-Einleitung-Kryptografie> bzw. als mp4-Dateidownload oder PowerPoint-Präsentation *Einleitung-Kryptographie.pptx*



Erarbeitung 1 (2 Stunden)

Thema: Kennenlernen und Anwenden verschiedener Verschlüsselungsverfahren

M 3 **Gartenzaun-Verschlüsselung – Zick-Zack-Geheimschrift**

M 4 **Freimaurer-Alphabet – Verschlüsseln durch Ersetzen**

M 5a **Ave Codesar! – Caesar-Chiffre**

M 5b **Caesar-Chiffre – Basteln einer Caesar-Scheibe**

Benötigt: Schere
 Musterbeutelklammern
 Briefumschläge mind. A 5
 ggf. PowerPoint-Präsentation *Verschlusselungsarten.pptx* bzw. Video **V 2:** <https://raabe.click/Video-Verschlusselungsarten> bzw. als mp4-Dateidownload



Erarbeitung 2 (2 Stunden)

Thema: Die Akte „Enigma“

M 6a **Die Akte „Enigma“ – Der (fast) ungeknackte Code**

M 6b **Unterlagen aus der Akte im Fall „Enigma“**

Benötigt: Optional zum Basteln der „Enigma“-Akte durch die Lehrkraft:
 DIN-A4-Kraftpapier
 DIN-A4-Laminierfolie (matt)
 Schere/Schneidemaschine
 Klebstoff
 Büroklammern
 Drucker
 ggf. „Top Secret“-Stempel

Übung und Ergebnissicherung (1 Stunde)

Thema: Sicherheitsaspekte von Verschlüsselungen

M 7 **Der perfekte Schlüssel – Optimieren der Sicherheit eines Bildercodes**
M 8 **Tippskarten zu M 7 „Der perfekte Schlüssel“**

Benötigt:

- Interaktive Lernzielkontrolle (H5P):
<https://raabe.click/Lernzielkontrolle-Kryptografie>
- Endgerät





Benötigte Dateien

- Einleitung Kryptographie (Video **V 1**/mp4 H5P): <https://raabe.click/Video-Einleitung-Kryptographie> und als Download *Video-Einleitung-Kryptographie.mp4*
- Verschlüsselungsarten (Video **V 2**/mp4 H5P): <https://raabe.click/Video-Verschluesselungsarten> und als Download *Video-Verschlüsselungsarten.mp4*
- Einleitung Kryptographie (Präsentation zu **V 1**/PPT): *Einleitung-Kryptographie.pptx*
- Verschlüsselungsarten (Präsentation zu **V 2**/PPT): *Verschluesselungsarten.pptx*

Ergänzendes Material

- ggf. Selbstlerneinheit (Präsentation/PPT):
Selbstlerneinheit_Daten-und-Codierung_Einführung.pptx

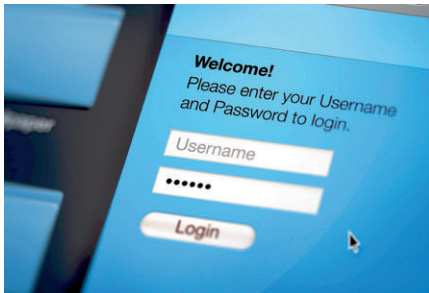
Erklärung zu den Symbolen

	Dieses Symbol markiert differenziertes Material. Wenn nicht anders ausgewiesen, befinden sich die Materialien auf mittlerem Niveau.				
	einfaches Niveau		mittleres Niveau		schwieriges Niveau

Verschlüsselung oder Kryptographie – Was ist das?

M 1

Schlösser und Schlüssel im Internet: Wozu braucht man so etwas?



© Spiffy/J/E+

Überall, wo wir hingehen, hinterlassen wir Spuren. Das ist nicht nur im „echten Leben“ so. Auch im virtuellen Raum des Internets dürfen wir nicht vergessen, dass wir Teil eines großen Netzwerkes sind. Dadurch machen wir uns gläsern. Wir hinterlassen überall Datenspuren: Welche Websites wir besuchen, wer wir sind, wo wir wohnen, welche Bankdaten wir besitzen usw. Und natürlich will niemand, dass all dies in falsche Hände gerät. Deshalb verstecken wir unsere Daten gerne hinter

verschlossenen Türen: Um an unsere Benutzerkonten zu kommen, braucht man einen Schlüssel – das Passwort. Hat man den passenden Schlüssel nicht, kommt man nicht hinein. In diesem Zusammenhang der Datenverschlüsselung spricht man auch von *Kryptographie*.

Definition: Der Begriff *Kryptographie* ist eine Kombination der altgriechischen Wörter *kryptós* (deutsch: verborgen) und *gráphein* (deutsch: schreiben). Zunächst als Wissenschaft der analogen Verschlüsselung bekannt, ist sie heute vor allem im Bereich der digitalen Informationssicherheit zu finden.

Kriterien für ein gutes Passwort

Ein Passwort stellt im virtuellen Raum des Internets also einen guten Schlüssel zur Verschlüsselung von Daten dar. Doch wie sieht ein *sicheres Passwort* aus?

Tausche dich mit deinem Partner/deiner Partnerin über deine Ideen zu dieser Frage aus. Erstellt gemeinsam eine Checkliste mit den drei wichtigsten Kriterien für ein sicheres Passwort.

- ✓ _____
- ✓ _____
- ✓ _____

Herkunft: Vor der Informatik

Kryptographie ist allerdings nichts, was in der Informatik mit Computern angefangen hat. Der Begriff wurde dadurch nur bekannter. Einige Verschlüsselungen basieren auf historischen Ideen, da man schon früh Nachrichten für Fremde unzugänglich machen wollte. Teilweise konnten sie von Menschen geknackt werden, teilweise mussten Maschinen ran. Lasst uns deshalb selbst zu Kryptographen, Detektiven und Sicherheitsexperten werden und entdecken, welche Ideen dieser historischen Verschlüsselungsmethoden wir am Computer gebrauchen können.



M 4

Freimaurer-Alphabet – Verschlüsseln durch Ersetzen



Wenn man Buchstaben verstecken will, warum nicht einfach gegen etwas anderes tauschen? Wir trauen uns an ein Krypto-Alphabet – wir ersetzen die Buchstaben durch etwas Neues. Das kann man nicht nur mit Signalen – wie z. B. beim Morse-Code – umsetzen, sondern natürlich auch mit anderen Symbolen, Buchstaben oder Bildern. Im Altertum gab es das schon einmal in Form des Freimaurer-Alphabets, auch „Freimaurer-Quadrat“ genannt. Dort sahen Botschaften wie folgt aus:



Aufgabe

Doch was soll das da oben bedeuten? Hier siehst du den Schlüssel und ein Beispiel. Finde heraus, wie der Code funktioniert, und gib an, was die obige Geheimnachricht bedeutet.

Schau dir bei Bedarf das Video (Minute 1:54 bis 4:17) noch einmal an, indem du den Link/ QR-Code aufrufst: <https://raabe.click/Video-Verschlueselungsarten>



Der Schlüssel

A	B	C	J	K	L
D	E	F	M	N	O
G	H	I	P	Q	R
T	S	U	X	Y	Z

Ein Beispiel

□ □ >
□ J L □ >
□ F C F □ □ □ F F V L □ .

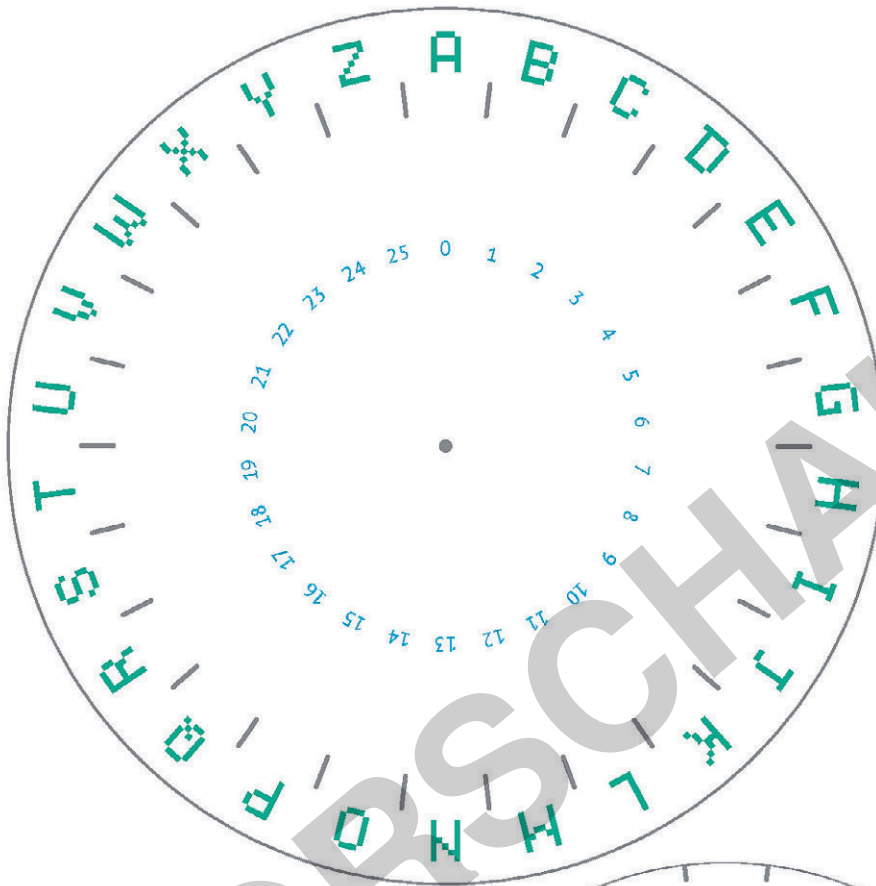
Übersetzung: *Not macht erfinderisch.*

Was bedeutet also die Nachricht oben in der Box?

© RAABE 2022

M 5b

Caesar-Chiffre – Basteln einer Caesar-Scheibe

**Aufgaben**

1. Schneide beide Scheiben aus.
2. Schneide das kleine Fenster bei der kleineren Scheibe aus.
3. Steche mit einer Schere ein Loch in die Mitte von beiden Scheiben.
4. Verbinde die Scheiben mit einer Muserbeutelklammer.
5. Los geht's mit dem Verschlüsseln!

