GI-Fachgruppe
Informatische Bildung in NRW

Informatische Bildung in NRW

Unterrichtsmaterialien für die Sekundarstufe I

Johannes Pieper

Codierung und Kryptologie

Verschlüsseln, Entschlüsseln und Knacken von Nachrichten

Autoren

Dieses Dokument ist ein sogenanntes Modul der Materialsammlung, die von der Fachgruppe Informatische Bildung in NRW der Gesellschaft für Informatik heraus gegeben wird. Verantwortliche Autoren für dieses Dokument: Johannes Pieper

Lizenz

Dieses Dokument steht unter der Creative Commons by-nc-sa-Lizenz. Folglich darf es beliebig kopiert und bearbeitet werden, sofern das Folgeprodukt wiederum unter dieser Lizenz vertrieben wird. Eine kommerzielle Nutzung ist nicht erlaubt. https://creativecommons.org/licenses/by-nc-sa/4.0/deed.de

Verweise auf Material

Dieses Modul enthält Hinweise und Verweise (Links) auf Material.Wird eine Seite des Bezugsmaterials dargestellt, ist dieses immer die erste, auch wenn das entsprechende Material aus mehreren besteht. Die Weltkugel verweist dabei auf die entsprechende Webseite und das Dokumentensymbol hat einen relativen Pfad hinterlegt, der die Nutzung der Verzeichnisstruktur der Materialsammlung voraussetzt.

Kontakt

Ihre Ansprechpartner für die vorliegenden Materialien sind Daniel Losch daniel.losch@gi.de und Johannes Pieper pieper@informatiktag-nrw.de

codierung_kryptologie.tex

git
Version: dd1fc2
Stand: 26. Juni 2026 18:18
Zuletzt bearbeitet von: Johannes Pieper

1 Beschreibung

Ein mögliches Thema in der Mittelstufe ist die Codierung und Kryptologie, also die Beschäftigung mit der Verschlüsselung von Nachrichten. Ziel dieses Moduls ist es, dass die Schülerinnen und Schüler neben der Codierung auch verschiedene Arten der Verschlüsselung kennen und anwenden lernen. Dabei liegt der Schwerpunkt auf den klassischen Verfahren, die man auch per Hand anwenden kann.

Der zweite Teil des Moduls vertieft einige dieser Verfahren und zeigt ihre Schwächen auf, indem die Lernenden dazu animiert werden, verschlüsselte Texte zu knacken. Dabei lernen sie auch z. B. die Möglichkeiten der Häufigkeitsanalyse kennen.

Den Abschluss dieses Moduls bildet die Thematisierung von asymmetrischen Verfahren. Hierbei wird eine Möglichkeit des Schlüsseltausch besprochen, sowie die Bildung von Hash-Werten.

Der hier vorgestellte Ablauf wurde bereits mehrere Male in der Jahrgangsstufe 9 im Wahlpflichtbereich durchgeführt. Er umfasst ungefähr 13 Unterrichtsstunden von je 45 Minuten.

2 Ablauf und Material

Der Ablauf ist in die drei Teile des Moduls unterteilt. Das entsprechende Material ist direkt damit verlinkt, bzw. eingebunden.

2.1 Verschiedene Verschlüsselungsverfahren in Eigenarbeit

Den Einstieg in den Themenbereich der Codierung und Verschlüsselung bildet das Spioncamp, dass unter der Adresse https://ddi.uni-wuppertal.de/de/downloads/lern-lehrmaterialien/spioncamp/ zu finden ist. Dabei erarbeiten sich die Schülerinnen und Schüler die verschiedenen Verfahren selbstständig. Dabei erhalten sie zusätzlich folgende Arbeitsaufträge:

- Kurzdokumentation der Verfahren in eigenen Worten (Was wird wie gemacht).
- Einsortierung der Verfahren in verschiedene Kategorien.
- Erklären der verschiedenen Kategorien.

Zum Abschluss werden ausgewählte Verfahren im Plenum von einzelnen Schülerinnen und Schülern vorgestellt. Dazu gehören unter anderem: Caesar, Vigenère, Skytale, Steganographie (Mit weiteren Beispielen wie Schreiben mit Zitronensaft und den Text verstecken hinter dem Wachs einer Wachstafel) und Morse.

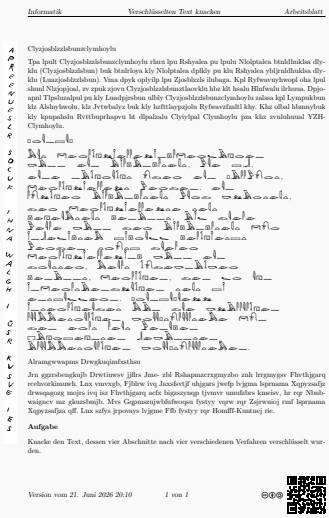
Dieser Teil umfasst ungefähr 4 Schulstunden von je 45 Minuten.

2.2 Knacken von verschlüsselten Texten

Zu Beginn des zweiten Teils erhalten die Schülerinnen und Schüler das Arbeitsblatt mit einem Text der in vier verschiedene Teile aufgeteilt wurde, die unterschiedlich verschlüsselt wurden. Ohne weitere Kommentierung erhalten sie den Auftrag, diesen Text zu lesen, so dass sie sich erst an die Aufgabe machen müssen, ihn zu knacken. Dieses kann in Gruppen erfolgen.

Material

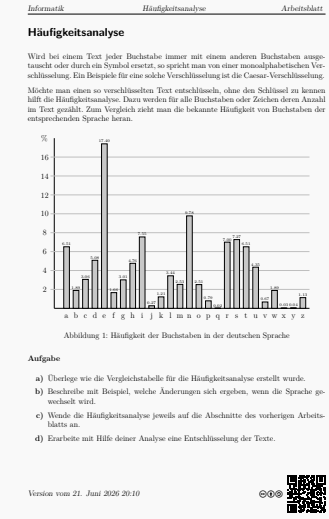
- ab_verschluesselter_text.pdf



Während der Bearbeitung des ersten Arbeitsblatts erhalten die Schülerinnen und Schüler das zweite Arbeitsblatt zur Häufigkeitsanalyse. Dieses dient als Hilfsmittel um zwei der vier Abschnitte knacken zu können.

Material

- ab_haeufigkeitsanalyse.pdf



Die anschließenden Besprechung erfolgt auch, wenn der vierte Teil, der mit Vigenère verschlüsselt wurde, von keinem geknackt wurde. Eine Häufigkeitsanalyse sollte aber von einigen Gruppen für diesen Text bereits angefertigt worden sein, so dass das Ergebnis vorgestellt werden kann. Im Plenum können dann Auffälligkeiten am Text besprochen werden, wie z. B. die Wiederholung einiger Wörter. Daran lässt sich die Schlüssellänge bestimmen, da die Abstände dieser Wiederholungen einem Vielfachen der Schlüssellänge

entsprechen. Mit der bekannten Länge des Schlüssels kann dann eine Häufigkeitsanalyse über jeden x-ten Buchstaben durchgeführt werden.

Ausgehend von diesen Erfahrungen können allgemeine Strategien zum Knacken verschlüsselter Nachrichten erarbeitet werden, wie es im Unterrichtsentwurf beschrieben ist. Die Texte sind dabei mit Verfahren aus dem Spioncamp verschlüsselt worden und können teilweise nur mit diesen Materialien auch nur geknackt werden.

Material

- ub_strategien_codeknacken.pdf



Unterrichtsentwurf

(Unterrichtsbesuch im Fach Informatik)

Entwicklung verschiedener Strategien zum Knacken von Texten, die mit verschiedenen Techniken verschlüsselt wurden

Lehrer: -, StR
Schulform: Gymnasium
Lerngruppe: Differenzierungskurs Informatik 9
(18 Schülerinnen und Schüler, 1 weiblich und 17 männlich)
Zeit: 10.30 Uhr – 11.15 Uhr (4. Stunde)

- ab_verschluesselte_texte_fuer_strategie.pdf



Informatik *Verschlüsselter Text* *Arbeitsblatt*

1. Verschlüsselter Text

Der folgende Text ist mit einem dir bekannten Verfahren verschlüsselt worden.

D	G	L	T	S	I	H
E	I	E	N	K		I
E	N	H	U	S	H	R
I	E	S	N	S		N
I	E	B		E	E	T
R	M	R	N	A	M	C
X	D	L		T	O	
S	S	S		T	N	U
E	H		W	N	S	
		S		N	E	H
T		U	I		D	G
T	H	E	L		I	G
S	E	V	E		E	S
T	U	C	D	N	T	E
	D	E	H	I	E	E
	A	L	E	D	C	

Aufgabe

1. Finde heraus, wie der Text verschlüsselt wurde und übersetze ihn in Klartext.
2. Notiere dir deine Vorgehensweise. Lasse dabei auch Dinge nicht aus, die in eine Sackgasse geführt haben. Übertrage die Vorgehensweise deiner Gruppe auf eine Folie, sodass du sie vorstellen kannst.

Hinweise

- Du darfst jederzeit auf die Materialien aus dem Spioncamp zurückgreifen, wenn es dir beim Entschlüsseln hilfreich ist.
- Bei dem Text sind die Satzzeichen (Punkte, Komma etc.) entfernt worden. Leerzeichen sind aber immer an der entsprechenden Stelle vorhanden.

Version vom 21. Juni 2026 20:10

Dieser Teil umfasst ungefähr 6 Schulstunden von je 45 Minuten.

2.3 Asymmetrische Verfahren

Der Tausch der Schlüssel bei der Verschlüsselung ist eines der schwierigsten Probleme. Diese können entweder im Plenum oder mit noch zu erstellenden Arbeitsanweisungen in kleinen Gruppen durchgespielt werden. Dabei wird folgendes benötigt:

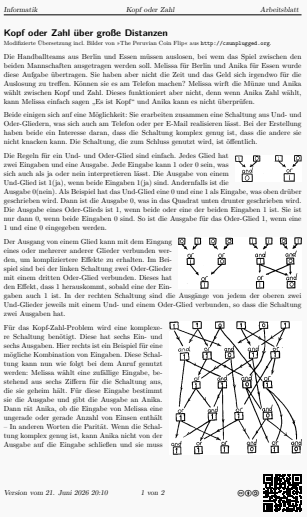
- Eine Box, die sich mit zwei Vorhängeschlössern verschließen lässt.
- Mindestens drei Vorhängeschlösser mit unterschiedlichen Schlüsseln. Diese müssen ohne Schlüssel zuschnappen.
- Eine zu übermittelnde Nachricht.

Schülerinnen und Schüler können dann die Rollen von Alice, Bob und Eve einnehmen und die Nachricht untereinander versuchen auszutauschen. Dieses wird sowohl ohne Schloss (unverschlüsselt), als auch mit zwei Schlössern und dem mehrere Male hin- und hergeben der Box durchgeführt. Auch das Prinzip des öffentlichen Schlosses lässt sich so demonstrieren. Mit dem dritten Schloss für Eve lassen sich auch Schwachstellen des Systems aufzeigen und mögliche Lösungen besprechen.

Festigen lässt sich das Prinzip der asymmetrischen mit dem Kopf oder Zahl Beispiel aus CS-unplugged, für dass hier eine deutsche Übersetzung vorliegt. Dieses zeigt ein Beispiel für die Bildung von Hash-Werten, die sich anschließenden noch bei anderen Anwendungsbeispielen wie der Bildung von Checksummen oder dem Speichern von Passwörtern vertiefen lassen.

Material

- ab_kopf_oder_zahl.pdf



Informatik *Kopf oder Zahl* *Arbeitsblatt*

Kopf oder Zahl über große Distanzen

Modifizierte Übersetzung incl. Bilder von »The Peruvian Coin Flip« von http://csunplugged.org

Die Handballteams aus Berlin und Essen müssen auslosen, bei wem das Spiel zwischen den beiden Mannschaften ausgetragen werden soll. Melissa für Berlin und Anika für Essen wurde diese Aufgabe übertragen. Sie haben aber nicht die Zeit und das Geld sich irgendwo für die Auslosung zu treffen. Können sie es am Telefon machen? Melissa wirft die Münze und Anika wählt zwischen Kopf und Zahl. Dieses funktioniert aber nicht, denn wenn Anika Zahl wählt, kann Melissa einfach sagen „Es ist Kopf" und Anika kann es nicht überprüfen.

Beide einigen sich auf eine Möglichkeit: Sie erarbeiten zusammen eine Schaltung aus Und- und Oder-Gliedern, was sich auch am Telefon oder per E-Mail realisieren lässt. Bei der Erstellung haben beide ein Interesse daran, dass die Schaltung komplex genug ist, dass die andere sie nicht knacken kann. Die Schaltung, die zum Schluss genutzt wird, ist öffentlich.

Die Regeln für ein Und- und Oder-Glied sind einfach. Jedes Glied hat zwei Eingaben und eine Ausgabe. Jede Eingabe kann 1 oder 0 sein, was sich auch als ja oder nein interpretieren lässt. Die Ausgabe von einem Und-Glied ist 1(ja), wenn beide Eingaben 1(ja) sind. Andernfalls ist die Ausgabe 0(nein). Als Beispiel hat das Und-Glied eine 0 und eine 1 als Eingabe, was oben drüber geschrieben wird. Dann ist die Ausgabe 0, was in das Quadrat unten drunter geschrieben wird. Die Ausgabe eines Oder-Glieds ist 1, wenn beide oder eine der beiden Eingaben 1 ist. Sie ist nur dann 0, wenn beide Eingaben 0 sind. So ist die Ausgabe für das Oder-Glied 1, wenn eine 1 und eine 0 eingegeben werden.

Der Ausgang von einem Glied kann mit dem Eingang eines oder mehrerer anderer Glieder verbunden werden, um kompliziertere Effekte zu erhalten. Im Beispiel sind bei der linken Schaltung zwei Oder-Glieder mit einem dritten Oder-Glied verbunden. Dieses hat den Effekt, dass 1 herauskommt, sobald eine der Eingaben auch 1 ist. In der rechten Schaltung sind die Ausgänge von jedem der oberen zwei Und-Glieder jeweils mit einem Und- und einem Oder-Glied verbunden, so dass die Schaltung zwei Ausgaben hat.

Für das Kopf-Zahl-Problem wird eine komplexere Schaltung benötigt. Diese hat sechs Ein- und sechs Ausgaben. Hier rechts ist ein Beispiel für eine mögliche Kombination von Eingaben. Diese Schaltung kann nun wie folgt bei dem Auruf genutzt werden: Melissa wählt eine zufällige Eingabe, bestehend aus sechs Ziffern für die Schaltung aus, die sie geheim hält. Für diese Eingabe bestimmt sie die Ausgabe und gibt die Ausgabe an Anika. Dann rät Anika, ob die Eingabe von Melissa eine ungerade oder gerade Anzahl von Einsen enthält – In anderen Worten die Parität. Wenn die Schaltung komplex genug ist, kann Anika nicht von der Ausgabe auf die Eingabe schließen und sie muss

Version vom 21. Juni 2026 20:10 *1 von 2*

Dieser Teil umfasst ungefähr 3 Schulstunden von je 45 Minuten.