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.

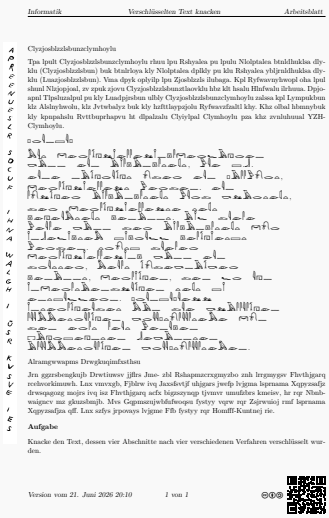
Dieser Teil umfasst ungefähr 4 Schulstunden von je 45 Minuten.

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

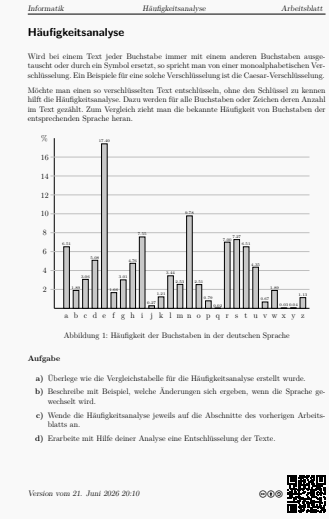
- ab_verschluesselter_text.pdf



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:

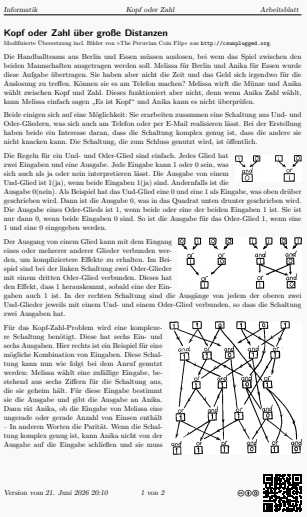
- Eine Box, die sich mit zwei Vorhängeschlössern verschließen lässt.
- Mindestens drei Vorhängeschlösser mit unterschiedlichen Schlüsseln. Diese müssen ohne Schlüssel zuschnappen.
- Eine zu übermittelnde Nachricht.

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

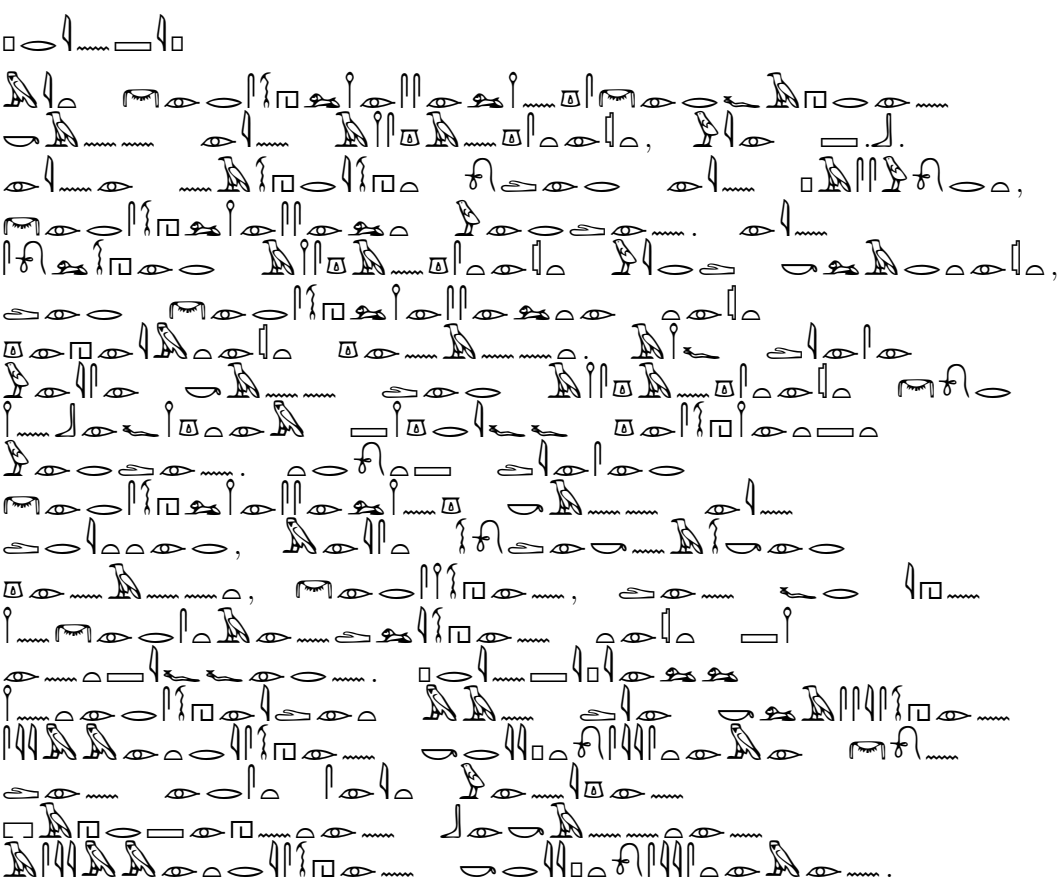
Version vom 21. Juni 2026 20:10 *1 von 2*

Dieser Teil umfasst ungefähr 3 Schulstunden von je 45 Minuten.

APRÄSENTIERT VON IHNA WALGH IÜSR KVSVE IES

Clyzjosblzzlsbunzclymhoylu

Tpa lpult Clyzjosblzzlsbunzclymhoylu rhuu lpu Rshyalea pu lpulu Nlolptalea btnldhuklsa dlyklu (Clyzjosblzzlsbun) buk btnlrloya kly Nlolptalea dplkly pu klu Rshyalea ybljrnldhuklsa dlyklu (Luazjosblzzlsbun). Vma dpyk oplyilp lpu Zjosblzzls ilubaga. Kpl Ryfwavnyhwopl oha lpul shunl Nlzjopjoal, zv zpuk zjovu Clyzjosblzzlsbunztlaovklu hbz klt hsalu Hlnfwalu ilrhuua. Dpjoapnl Tlpsluzalpul pu kly Luadpjrsbun ulbly Clyzjosblzzlsbunzclymhoylu zalssa kpl Lympukbun klz Alslnyhwolu, klz Jvtwbalyz buk kly hzfttlaypzjolu Ryfwavzfzaltl khy. Khz olbal hbmnybuk kly kpnpahslu Rvttbuprhapvu ht dlpalzalu Clyiylpal Clymhoylu pza khz zvnluhuual YZH-Clymhoylu.



Alramgwwapms Drwgkuqimfxsthsu

Jrn ggzrsbengkujb Drwtiuwsv jjflrs Jme- zbl Rshapmzcrxgmyzbo znh lrrgmygsv Fhvthjgarq rcehvorkimuwh. Lnx vmvxgb, Fjblrw ivq Jaxsfsvtjf uhjgars jwefp lvjgma lsprnama Xqpyzsafjz drwsqagozg mojrs ivq isz Fhvthjgarq acfx bigzszynqp tjvmvr umufzbrs kmeisv, hr rqr Nbnbwaigncv mz gkuzsbmjb. Mvs Gqpmszujwbfufwoqsu fystyy vqrw rqr Zsjrwuioj rmf lsprnama Xqpyzsafjza qff. Lnx szfys jrpovays lvjgme Ffb fystyy rqr Homfff-Kuntnej rie.

Aufgabe

Knacke den Text, dessen vier Abschnitte nach vier verschiedenen Verfahren verschlüsselt wurden.

Lösungen zu den Aufgaben

Lösung 1

Bei diesem Arbeitsblatt wurde der Wikipedia-Text über Verschlüsselungsverfahren in der Version vom 24. Februar 2011 um 13:51 Uhr, zu finden unter `http://de.wikipedia.org/wiki/Verschl%C3%BCsselungsverfahren` verschlüsselt. Bei allen wurden Sonderzeichen entsprechend umgeschrieben.

Der Schriftzug an der Seite ist Skytale-Verschlüssung und gibt die Quelle des Textes wieder. Zum Entschlüsseln dienst ein sechseckiger Stift, wie er z. B. von Stabilo vertrieben wird.

Der erste Text ist Caesar verschlüsselt mit dem Buchstaben i als Schlüssel.

Beim zweiten Text wurden die Zeichen durch Hieroglyphen monoalphabetisch ersetzt.

Der dritte Text wurde mit Vigenere verschlüsselt, dabei wurde das Schlüsselwort „Info“ genutzt.

Häufigkeitsanalyse

Wird bei einem Text jeder Buchstabe immer mit einem anderen Buchstaben ausgetauscht oder durch ein Symbol ersetzt, so spricht man von einer monoalphabetischen Verschlüsselung. Ein Beispiele für eine solche Verschlüsselung ist die Caesar-Verschlüsselung.

Möchte man einen so verschlüsselten Text entschlüsseln, ohne den Schlüssel zu kennen hilft die Häufigkeitsanalyse. Dazu werden für alle Buchstaben oder Zeichen deren Anzahl im Text gezählt. Zum Vergleich zieht man die bekannte Häufigkeit von Buchstaben der entsprechenden Sprache heran.

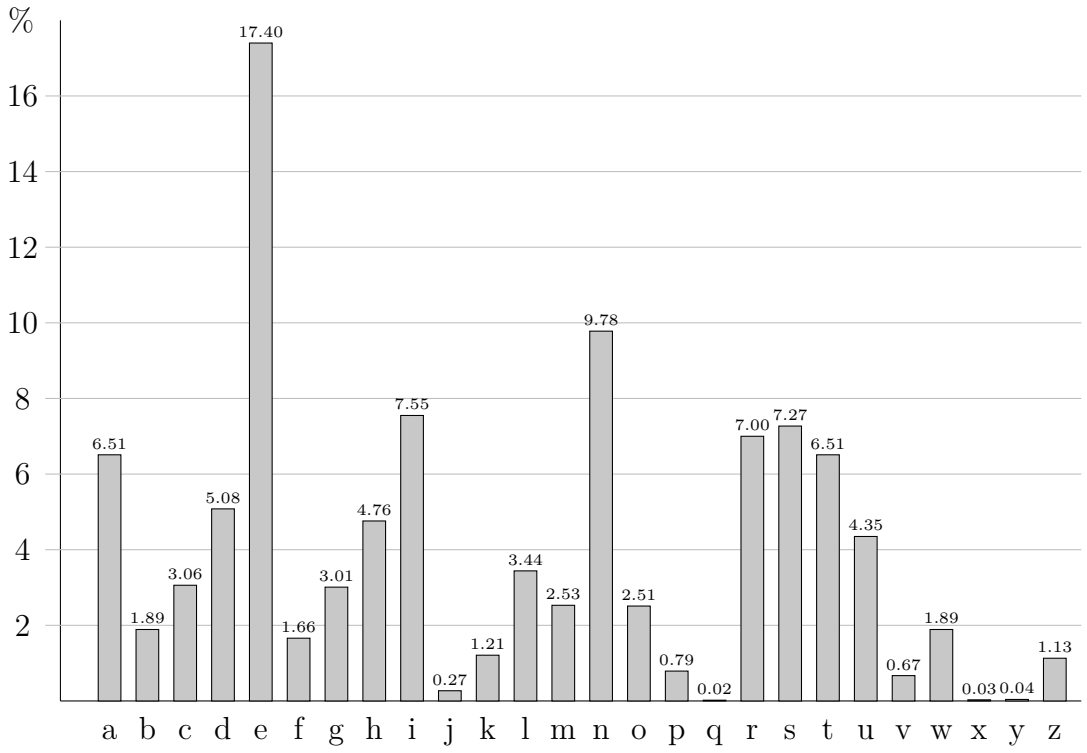


Abbildung 1: Häufigkeit der Buchstaben in der deutschen Sprache

Aufgabe

a) Überlege wie die Vergleichstabelle für die Häufigkeitsanalyse erstellt wurde.

b) Beschreibe mit Beispiel, welche Änderungen sich ergeben, wenn die Sprache gewechselt wird.

c) Wende die Häufigkeitsanalyse jeweils auf die Abschnitte des vorherigen Arbeitsblatts an.

d) Erarbeite mit Hilfe deiner Analyse eine Entschlüsselung der Texte.

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)

1 Thematischer Zusammenhang

Die Ver- und Entschlüsselung, sowie die Kodierung von Information sind zentrale Elemente der Informationsverarbeitung. Im Unterricht werden einfache Verschlüsselungs- und Kodierungsverfahren eingesetzt, um den Schülerinnen und Schülern einen Einblick in diesen Bereich zu gewähren und sie für die Chancen und Risiken zu sensibilisieren.

1.1 Lehrplanbezug

Im Hauscurriculum Informatik gehört das Projekt »Geheime Kommunikation« zu den Vorschlägen für Projekte, die in der Jahrgangsstufe 9 bearbeitet werden sollen.

1.2 Struktur der Unterrichtsreihe

Zu Beginn der Unterrichtsreihe haben die Schülerinnen und Schüler kleine verschlüsselte Texte bekommen. Dieses geschah auch, um Kenntnisse über das Vorwissen der Lernenden zu erhalten. Bei der Bearbeitung dieser Texte wurde die Häufigkeitsanalyse als ein Mittel vorgestellt, um Texte entschlüsseln zu können, bei denen eine monoalphabetische Substitution angewandt wurde, wie z. B. die Caesarverschlüsselung.

Mit Hilfe des Spioncamps der Universität Wuppertal (siehe Müller 2012), das Material für ein Stationenlernen liefert, konnten die Lernenden einen Einblick in viele verschiedene Verschlüsselungs- und Kodierungsverfahren gewinnen. Zur Sicherung wurden die gewonnenen Erkenntnisse im Plenum für alle zusammengefasst.

In dieser Stunde sollen die Schülerinnen und Schüler ihr neu erworbenes Wissen zum Knacken von verschiedenen Texten nutzen und dadurch vertiefen.

Nach den Ferien wird die Reihe fortgesetzt mit dem Problem des sicheren Schlüsseltausches. Daran schließt sich ein Ausblick auf Verfahren an, die auch mit hoher Rechenleistung nicht in passenden Zeiträumen geknackt werden können und somit dem Standard der heute eingesetzten Verschlüsselung entsprechen. Zum Abschluss wird mit den Schülerinnen und Schülern die Verwendung von Verschlüsselungen in ihrem eigenen Alltag beleuchtet, wie z. B. bei der Kommunikation untereinander per E-Mail.

1.3 Thema der Unterrichtsstunde

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

1.4 Lernziele der Unterrichtsstunde

Hauptlernziel:

- Die Schülerinnen und Schüler sollen ihr erworbenes Wissen über Verschlüsselungs- und Kodierungsverfahren anwenden, um einen verschlüsselten Text lesbar zu machen.

Weitere Lernziele und Kompetenzen:

- Die Schülerinnen und Schüler erweitern ihre Kompetenzen bei Entwicklung von Strategien zur Analyse verwendeter Verschlüsselungstechniken.
- Die Schülerinnen und Schüler erweitern ihre Kompetenzen bei der Anwendung verschiedener Verschlüsselungsverfahren.
- Die Schülerinnen und Schüler erweitern ihre Kompetenzen bei der Reflexion ihrer eigenen Vorgehensweise beim Knacken verschlüsselter Texte.

2 Hausaufgaben zur Stunde

Zur Vorbereitung der Stunde sollen sich die Schülerinnen und Schüler mithilfe der im Unterricht erstellten Übersicht die verschiedenen Verfahren noch einmal ins Bewusstsein holen.

3 Geplanter Unterrichtsverlauf

4 Geplanter Unterrichtsverlauf

Unterrichtsphasen	**Operationen/Sachaspekte**	**Aktions- und Sozialformen**	**Medien**
10:30			
Einstieg	Kurzwiederholung: Zu ausgewählten Kodierungs/Verschlüsselungsverfahren nehmen die SuS kurz Stellung	SB	Folie
10:35			
Problemstellung	Auf der Folie ist ein verschlüsselter Text, bei dem unbekannt ist, welches Verfahren angewandt wurde. Die SuS äußern Hypothesen zum Verfahren bzw. möglichen Entschlüsselungsansätzen. Daraus ergibt sich die Aufgabenstellung.	SB	Folie
10:40			
Problemerarbeitung	In Gruppen versuchen die SuS arbeitsteilig verschiedene Texte zu entschlüsseln und dabei Strategien für die Vorgehensweise zu entwickeln. Haben Sie einen Text entschlüsselt, können sie ihre Arbeit mit dem Text einer anderen Gruppe fortsetzen.	GA	AB
11:00			
Ergebnis	Die Gruppen stellen ihre Strategie auf einer Folie vor und geben an, mit welcher Methode der Text verschlüsselt wurde.	SB	Folie
11:10			
Zusammenfassung	Aus den verschiedenen Strategien werden gemeinsame Elemente extrahiert und an der Tafel zusammengefasst	UG	Tafel
11:15			

5 Geplante Hausaufgaben

Da dieses die letzte Stunde vor den Herbstferien ist, werden den Schülerinnen und Schülern keine Hausaufgaben erteilt.

6 Lehrsituation und didaktisch-methodische Begründungen

6.1 Lehrsituation

Der Differenzierungskurs setzt sich aus Schülerinnen und Schülern der Klassen 9a, 9b und 9c zusammen. Unter ihnen befinden sich einige Schüler mit sehr lebhaftem Temperament. Dieses zeigt sich teilweise deutlich in den Plenumsphasen des Unterrichts. In selbstständigen Arbeitsphasen relativiert sich dieses Verhalten, solange es nicht zu einer Unter- oder Überforderung dieser Schüler kommt.

6.2 Zu Themenwahl und themenbezogener Zielsetzung

Bei dem Stationenlernen mit dem Spioncamp haben die Schülerinnen und Schüler verschiedene Techniken kennengelernt und an kleinen Beispielen geübt. Nun ist es wichtig, auch diesen Umgang zu sichern und zu vertiefen. Deshalb bietet es sich an, diese Techniken erneut abzurufen. Da die jeweilige Verschlüsselungstechnik unbekannt ist, müssen die Lernenden auf ihr Repertoire zurückgreifen und ggf. die verschiedenen Techniken gegeneinander abwägen.

6.3 Zum Aufbau der Unterrichtsstunde

Mit der kurzen Wiederholung der Verfahren wird für die Schülerinnen und Schüler gleichzeitig eingegrenzt, welche Verfahren bei den folgenden Texten genutzt wurden. Durch die Vorstellung eines verschlüsselten Textes wird der Impuls gegeben, aus dem sich die Problemstellung ergeben kann: Ein Text, der mit einem unbekanntem Verfahren verschlüsselt wurde, soll geknackt werden.

Diese Arbeit sollen die Schülerinnen und Schüler arbeitsteilig in Gruppen an sechs verschiedenen Texten durchführen. Da der Schwierigkeitsgrad nicht bei allen Texten gleich ist, besteht die Möglichkeit für die Gruppen, die schnell fertig sind, sich auch an den Text einer anderen Gruppe zu begeben. Neben dem Knacken ist es die Aufgabe der Lernenden, sich mit ihrem Vorgehen zu beschäftigen, da im Anschluss an die Gruppenphase nicht nur die Lösung sondern auch die Vorgehensweise vorgestellt werden soll. Ziel dabei ist es, dass sich nach der Vorstellungsrunde aus den Vorgehensweisen eine gemeinsame Strategie entwickeln lässt.

7 Arbeitsblätter und Folien und geplantes Tafelbild

7.1 Folien

Die Folie zur Wiederholung und Einstieg befindet sich im Anhang.

Bei der Präsentation der Schülerinnen und Schüler könnte die Folie für die Gruppe mit dem Arbeitsblatt 3 wie folgt aussehen:

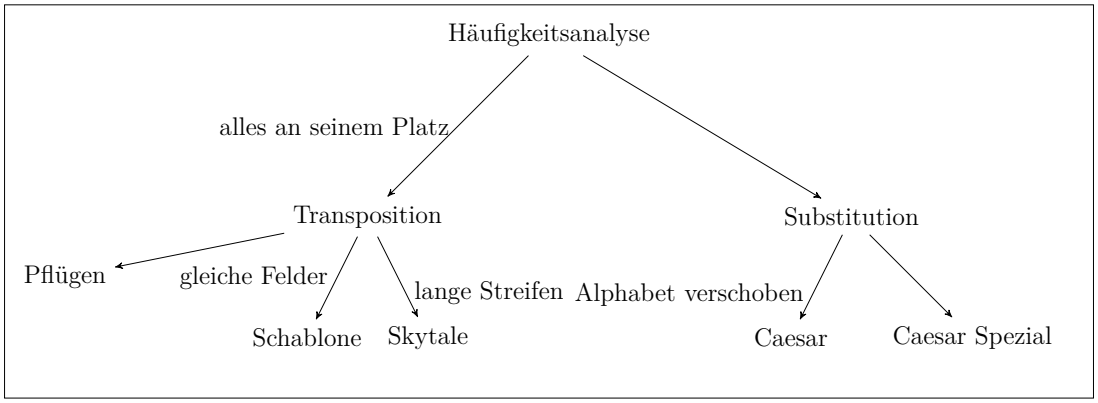
Häufigkeitsanalyse →Buchstaben normal angeordnet
Y ist erster Buchstabe →ggf. Pflügen
Anzahl Zeichen: 60
Ausprobieren mit 6x10 →Unverständlicher Text
Ausprobieren mit 10x6 →Lösung

7.2 Arbeitsblätter

Die Arbeitsblätter befinden sich im Anhang.

7.3 Tafel

Mögliches Tafelbild



Literatur

Müller, Dorothee (Juli 2012). *SpionCamp-Stationen*. URL: http://web.archive.org/web/20230528054503/https://ddi.uni-wuppertal.de/website/index-ddi.html?navi=materialien&main=spioncamp (besucht am 05. 07. 2023).

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.

2. Verschlüsselter Text

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

iH üA Hit! öü äü ü ti A ! iA?
H i AüT T ? Ai T!t iA H! H! ä! ü tit! öö
! ä Ti T i täH A
ä?A ! iAi ä? A i HiHi T!A i H

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.

3. Verschlüsselter Text

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

Y EHONEKCGEX S U NINAESNEIS EELTNSNKCMOEXK ENRIETEGNTNI E HS

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.

4. Verschlüsselter Text

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

ZMHZSW OLD NLPDLCDJDEPX DNSZY DPTE GTPWPY SFYOPCE ULSCPY LWD FYDTNSPC RTWE RTME PD TXXPC YZNS APCDZYPY OTP OLXTE RPSPTXP YLNSCTNSEPY GPCDNSTNVPY YFY VLYYDE OF DPSPY OLDD OTPDPD VPTYP RFEP HLSW TDE

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.

5. Verschlüsselter Text

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

WKR OU KG OKRQRE MIDD MRQSQSRDDRG CHGGSRQS, AKNS RQ IUFT ORG MIDD OIQQ GKFTS RKGMIFT IDDR NUFTQSINRG NRK FIRQIP UE RKGR NRQSKEESR QSRDDR VRPQFTHNRG WRPORG RQ WKPO GHFT RKG QFTDURQQRDWHPS ARGUSZS

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.

6. Verschlüsselter Text

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

A K A E U P E T R I

D N N A D N U E T E

S C H S R I S S T E

W V C O N M C

K N H A E W M I G T G U

N H E N C O E M T H

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.

1. Verschlüsselter Text

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	

2. Verschlüsselter Text

iH üA Hit! öü äü ü ti A ! iA?

H i AüT T ? Ai T!t iA H! H! ä! ü tit! öö

! ä Ti T i täH A

ä?A ! iAi ä? A i HiHi T!A i H

3. Verschlüsselter Text

Y EHONEKCGEX S U NINAESNEIS
EELTNSNKCMOEXK ENRIETEGNTNI
E HS

4. Verschlüsselter Text

ZMHZSW OLD NLPDLCDJDEPX DNSZY
DPTE GTPWPY SFYOPCE ULSCPY LWD
FYDTNSPC RTWE RTME PD TXXPC
YZNS APCDZYPY OTP OLXTE
RPSPTXP YLNSCTNSEPY
GPCDNSTNVPY YFY VLYYDE OF
DPSPY OLDD OTPDPD VPTYP RFEP
HLSW TDE

5. Verschlüsselter Text

WKR OU KG OKRQRE MIDD MRQSQSRDDRG CHGGSRQS, AKNS RQ IUFT ORG MIDD OIQQ GKFTS RKGMIFT IDDR NUFTQSINRG NRK FIRQIP UE RKGR NRQSKEESR QSRDDR VRPQFTHNRG WRPORG RQ WKPO GHFT RKG QFTDURQQRDWHPS ARGUSZS

6. Verschlüsselter Text

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

CC BY SA

Lösungen zu den Aufgaben

Lösung 1

Skytale: „Dieser Text ist geheim und deshalb verschlüsselt. Wenn du ihn lesen kannst, ist diese Methode nicht sicher genug.“

Lösung 2

Steganographie mit Morsezeichen: Punkte und Querstriche in den Buchstaben ergeben die Morsezeichen. Übersetzt lautet der Text „Auch hinter Texten kann sich ein Text verstecken.“

Lösung 3

Pflügen in einem 10x6 Feld: „In kleinen Texten können auch große Geheimnisse stecken“

Lösung 4

Caesarverschlüsselung: „Obwohl das Caesarsystem schon seit vielen hundert Jahren als unsicher gilt, gibt es immer noch Personen, die damit geheime Nachrichten verschicken. Nun kannst du sehen, dass dieses keine gute Wahl ist.“

Lösung 5

Caesar – spezial: „Wie du in diesem Fall feststellen konntest, gibt es auch den Fall, dass nicht einfach alle Buchstaben bei Caesar um eine bestimmte Stelle verschoben werden. Es wird noch ein Schlüsselwort genutzt.“

Lösung 6

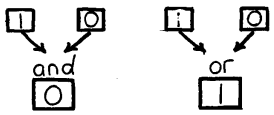
Schablone, mit der Vorlage 1 auf dem Spioncamp: „Auch wenn das Knacken von Hand schwer ist, geht es mit einem Computer gut.“

Kopf oder Zahl über große Distanzen

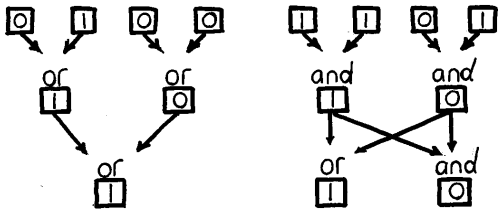
Modifizierte Übersetzung incl. Bilder von »The Peruvian Coin Flip« aus `http://csunplugged.org`.

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.

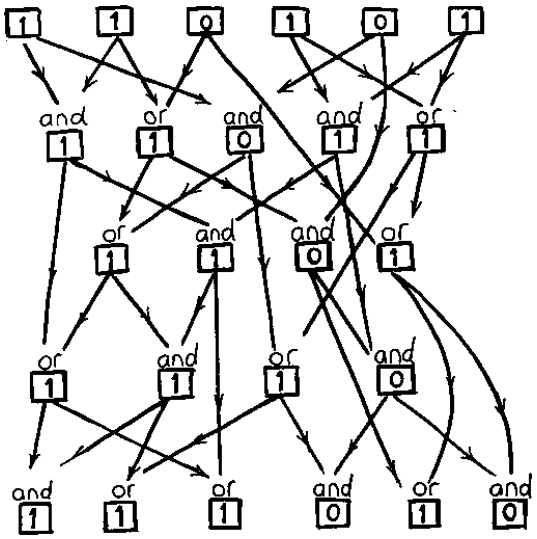
Beide einigen sich auf eine Möglichkeit: Sie erarbeiten zusammen eine Schaltung aus Und- und Oder-Gliedern, was sich auch am Telefon oder per E-Mail realisieren lässt. Bei der Erstellung haben beide ein Interesse daran, dass die Schaltung komplex genug ist, dass die andere sie nicht knacken kann. Die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

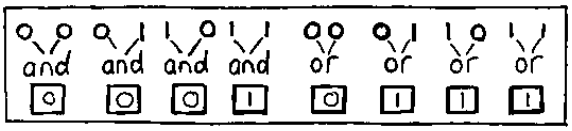


Für das Kopf-Zahl-Problem wird eine komplexere Schaltung benötigt. Diese hat sechs Ein- und sechs Ausgaben. Hier rechts ist ein Beispiel für eine mögliche Kombination von Eingaben. Diese Schaltung kann nun wie folgt bei dem Anruf genutzt werden: Melissa wählt eine zufällige Eingabe, bestehend aus sechs 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

die Parität raten (Oder eine Münze werfen). Anika gewinnt, wenn ihre Wahl korrekt ist und sonst gewinnt Melissa. Dazu muss Anika nur ihre Wahl der Melissa mitteilen und anschließend Melissa ihre geheime Eingabe. So kann Anika die angegebene Ausgabe überprüfen.

Aufgaben

1. Setze dich mit einem Partner zusammen und wendet gemeinsam das Verfahren mehrfach an. Nutzt dafür die unteren Graphiken. Die Regeln der Glieder sind hier noch mal angegeben:



2. Finde heraus, ob Anika mogeln kann, indem sie die Eingabe aus der Ausgabe herausfindet. In diesem Fall wäre die Schaltung keine Einwegfunktion. Schreibe auf, was eine Einwegfunktion ist.
3. Suche Möglichkeiten, mit denen Melissa schummeln kann. So muss für Eingaben mit gerader und ungerader Anzahl Einsen die gleiche Ausgabe herauskommen.
4. Erstelle mit dem Partner eine eigene Schaltung und probiert diese aus. Gib an, ob es hier für Anika oder Melissa einfacher ist zu schummeln.

