



Bergische Universität Wuppertal

Didaktik der Informatik

Thesis zur Erlangung des akademischen Grades
eines Master of Education (M.Ed.)

Lehramt an Gymnasien und Gesamtschulen

Aktuelle Verfahren der Kryptologie für den Informatikunterricht

Lernstationen zur Erweiterung des SpionCamps

vorgelegt von: Denise Schmitz
E-Mail: deniseschmitz.ddorf@gmail.com
Erstprüferin: Dr. Dorothee Müller
Zweitprüfer: Prof. Dr. Ludger Humbert

*Überarbeitete Version
Düsseldorf, den 08. Juli 2020*



Inhaltsverzeichnis

1	Einleitung	1
1.1	Grundbegriffe der Kryptologie	1
1.2	Motivation und Wahl des Themas	3
1.3	Aufbau der Arbeit	5
2	Kryptologie in den Bildungsdokumenten für Nordrhein-Westfalen	7
2.1	Bildungsstandards	8
2.2	Kernlehrpläne	10
2.3	Vorgaben für das Zentralabitur	12
2.4	Schulinterne Lehrpläne	13
3	Das SpionCamp	15
3.1	Stationenlernen	15
3.2	Die Unterthemen des SpionCamps	21
3.3	Weiteres Material der Bergischen Universität Wuppertal	28
3.3.1	MathePrisma	28
3.3.2	<i>Ich habe ein Geheimnis!</i>	30
3.3.3	Materialsammlung	33
4	Die neuen Stationen	34
4.1	Blockchiffren	34
4.1.1	Theoretische Grundlagen	35
4.1.2	Didaktische Analyse	38
4.1.3	Kompetenzen	45
4.2	Stromchiffren	45
4.2.1	Theoretische Grundlagen	46
4.2.2	Didaktische Analyse	49
4.2.3	Kompetenzen	55
5	Erprobungen im Unterricht	56
5.1	Durchführung des SpionCamps	56
5.1.1	Vorbereitung	56
5.1.2	Durchführung	58
5.1.3	Reflexion	60
5.2	Unterrichtserprobung mit neuem Material	64
5.2.1	Vorbereitung	65

5.2.2	Durchführung	65
5.2.3	Reflexion	67
5.3	Verbesserungen	73
6	Fazit	77
Anhang		I
	Station zur Blocktransposition	I
	Station zur Autokey-Chiffre	VII
	Fragebögen	XV
	Bibliographie	XIX
	Abbildungsverzeichnis	XXIV
	Erklärung über die Eigenständigkeit	

1 Einleitung

Der Schutz sensibler Information ist ein Anliegen, das bis in die Anfänge menschlicher Kultur reicht

Otto Horak, 1994 (zitiert nach F. L. Bauer, 1997, S. 1)

Im Leben eines jeden Menschen gibt es Daten, die privat und schützenswert sind. Dies war schon früher der Fall und ist zu Zeiten des allwissenden und nicht vergessenden Internets umso wichtiger. Bereits Kinder sollten lernen, mit sensiblen Daten vorsichtig umzugehen und zu wissen, welche Daten geteilt und welche eher geheim gehalten werden sollten. Dafür müssen sie verstehen, wie wichtig diese Daten sind und wie sie geschützt werden können. Dies kann jedoch nicht immer zu Hause vermittelt werden, da das informatische Allgemeinwissen in vielen Haushalten nicht vorhanden ist. Deswegen sollte die Schule eine Instanz sein, die Schülerinnen und Schülern Datensicherheit lehrt. In kein anderes Fach passt dabei diese Sensibilisierung hinsichtlich des Schutzes privater Daten besser als in die Informatik.

1.1 Grundbegriffe der Kryptologie

Die Geheimhaltung von sensiblen Daten wird in der Informatik mittels der *Kryptologie* bewerkstelligt. Die Kryptologie besteht aus zwei Disziplinen – der *Kryptographie* und der *Kryptoanalyse*. Während die erste die Ver- und Entschlüsselung von Nachrichten bezeichnet, beschäftigt sich die zweite mit dem »Knacken« von verschlüsselten Nachrichten ohne zugehörigen Schlüssel. In der Informatik ist eine *Nachricht* eine Datenmenge, die zwischen zwei Instanzen ausgetauscht wird. Der *Klartext* entspricht der Nachricht vor und der *Geheimtext* nach einer Verschlüsselung. Eine Verschlüsselung wird auch als *Chiffre* bezeichnet. Die formale Definition eines *Kryptosystems* lässt sich als Fünftupel $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ schreiben, mit den folgenden Eigenschaften (vgl. Buchmann, 2010, S. 59):

- Die Menge $\mathcal{P}$ ist der Klartextrraum. Ihre Elemente heißen Klartexte.
- Die Menge $\mathcal{C}$ ist der Geheimtextraum. Ihre Elemente heißen Geheimtexte.
- Die Menge $\mathcal{K}$ ist der Schlüsselraum. Ihre Elemente heißen Schlüssel.
- $\mathcal{E} = \{E_e : \mathcal{P} \rightarrow \mathcal{C}; e \in \mathcal{K}\}$ ist eine Familie von Verschlüsselungsfunktionen.
- $\mathcal{D} = \{D_d : \mathcal{C} \rightarrow \mathcal{P}; d \in \mathcal{K}\}$ ist eine Familie von Entschlüsselungsfunktionen.
- Für jedes $e \in \mathcal{K}$ existiert ein $d \in \mathcal{K}$, so dass für alle $p \in \mathcal{P}$ die Gleichung $D_d(E_e(p)) = p$ gilt.

In der Kryptologie geht man davon aus, dass ein Verschlüsselungsverfahren bekannt ist und nur der *Schlüssel* zwischen den Instanzen geheim gehalten werden muss. Dies nennt

man das *Kerckhoffs'sche Prinzip*. Der Kryptoanalytiker SHANNON hielt dies als die berühmte Maxime fest: „The enemy knows the system“ (vgl. Schmeh, 2013, S. 40).

Neben den Verschlüsselungsverfahren werden auch die *Steganographie* und die *Codierung* häufig zur Kryptologie gezählt. Bei der *Steganographie* handelt es sich um Methoden der Geheimhaltung durch Verbergen. Dies ist beispielsweise durch geheime Orte sowie versteckte Daten in Bildern oder Texten möglich. Ein *Code* wird in der Literatur unterschiedlich definiert. Teilweise wird er als Synonym zu *Geheimtextvokabular* (vgl. F. L. Bauer, 1997, S. 34) oder als Verfahren zur Verschleierung bezeichnet, „bei dem die Wörter oder Sätze des Klartexts durch andere Wörter oder Buchstabenfolgen ersetzt werden“ (Singh, 2000, S. 455). Diese Ersetzungen können in einem Codebuch oder einer Codetabelle festgehalten werden. In dieser Arbeit wird der Begriff *Code* verwendet, wenn die Nachricht für jede Person nachschlagbar ist. Dies ist beispielsweise beim Morsealphabet oder der Blindenschrift der Fall.

Die Verschlüsselungsverfahren werden in verschiedene Arten untergliedert, die *symmetrischen*, *asymmetrischen* und *hybriden* Verfahren. Symmetrische Verfahren nutzen zum Ver- und Entschlüsseln denselben Schlüssel. Die historischen symmetrischen Verfahren werden in zwei Verschlüsselungsklassen eingeteilt, der *Transposition* und der *Substitution*. Bei einer Transposition bleiben die Buchstaben einer Nachricht, „was sie sind, aber nicht, wo sie sind“ (D. Müller, 2012). Die Buchstaben vertauschen somit ihre Plätze, wie es beispielsweise bei Anagrammen der Fall ist. Bei einer Substitution hingegen bleiben die Buchstaben „wo sie sind, aber nicht, was sie sind“ (ebd.). Dadurch werden Buchstaben oder Buchstabenpaare durch andere ersetzt. Die Substitutionen können noch in weitere Arten unterteilt werden, die in Kapitel 3.2 erläutert werden. Die moderneren symmetrischen Verschlüsselungsverfahren werden in zwei weitere Verschlüsselungsklassen unterteilt, der *Blockchiffre* und der *Stromchiffre*. Beide werden in Kapitel 4 genauer erläutert. Während bei den klassischen symmetrischen Verschlüsselungsverfahren mit Buchstaben gearbeitet wird, wird bei den modernen Verfahren mit der Binärdarstellung oder den Ordinalzahlen der Buchstaben gerechnet. Die klassischen und die modernen Verfahren können dabei nicht klar voneinander abgegrenzt werden, da viele modernere Verfahren klassische Verfahren nutzen. Ein asymmetrisches Verschlüsselungsverfahren nutzt für die Ver- und Entschlüsselung verschiedene Schlüssel. Dies wird beispielsweise bei Public-Key-Verfahren angewandt. Hybride Verfahren verknüpfen die Vorteile von symmetrischen und asymmetrischen Verfahren, indem sie beide nutzen. So können beispielsweise Nachrichten mit den einfachen und schnellen symmetrischen Verschlüsselungsverfahren verschickt werden, aber der Schlüssel mit einem sicheren und langsamen asymmetrischen Verschlüsselungsverfahren.

Die Kryptologie erfüllt bestimmte Sicherheitsziele u. a. die *Vertraulichkeit*, *Authentizität*, *Integrität* sowie die *Verfügbarkeit*. Diese Sicherheitsziele ermöglichen einen sicheren Austausch von Daten. Die *Vertraulichkeit* stellt sicher, dass eine Nachricht nur von den Personen gelesen werden kann, für die sie auch bestimmt ist. Dies wird mittels Verschlüsselungsverfahren bewerkstelligt, die vor ungewolltem Mitlesen schützen. Kryptographische Techniken, beispielsweise elektronische Signaturen, geben Aufschluss über Echtheit der Daten sowie die Identität des Absenders einer Nachricht. Dadurch garantieren sie die *Authentizität* der Daten. Die *Integrität* soll sicherstellen, dass Daten vollständig und unverändert bleiben, was durch kryptographische Verfahren bewiesen werden kann. Daten sollen zusätzlich *verfügbar* sein, wenn sie benötigt werden. Dies schließt auch die korrekte Verarbeitung mit ein (vgl. Buchmann, 2010, 1 f.).

1.2 Motivation und Wahl des Themas

Die Kryptologie ist ein Teilgebiet der theoretischen Informatik und muss gemäß der Bildungsdokumente in Nordrhein-Westfalen im Schulfach Informatik unterrichtet werden (siehe Kapitel 2). Sie lässt sich fachdidaktisch auch auf den Grundlagen der fundamentalen Ideen legitimieren und gehört somit zu den „grundlegenden Prinzipien, Denkweisen und Methoden“ (Schwill, 1993, S. 1) der Informatik.

Horizontalkriterium Die Kryptologie zählt zur theoretischen Informatik, wird jedoch auch in anderen Fachgebieten verwendet und besitzt somit eine umfassende Anwendbarkeit. Durch ihren Einsatz in der Vergangenheit wurden Kriege gewonnen sowie die Gesellschaft geformt und auch zur heutigen Zeit sollen Daten geheim gehalten werden. Dies wird immer häufiger mit digitalen Technologien bewerkstelligt. Deswegen trägt die Kryptologie zu den Themengebieten *Informatik*, *Mensch und Gesellschaft*, *Angewandte Informatik* sowie *Praktische Informatik* bei.

Vertikalkriterium Die in der Kryptologie verwendete Mathematik ist Schülerinnen und Schülern der Oberstufe bekannt (vgl. F. L. Bauer, 1997, S. VI). Sie kann ebenfalls auf andere Entwicklungsstufen heruntergebrochen werden, um einfache Verschlüsselungsverfahren verständlich zu machen. So können bereits Kinder in der Grundschule erste Verfahren kennenlernen und ihren Einsatz im Alltag besprechen. Die Entwicklung und Analyse neuer Verschlüsselungsverfahren ist hochkomplex und wird von Wissenschaftlern der ganzen Welt durchgeführt. Deswegen kann die Kryptologie auf allen intellektuellen Niveaus erarbeitet werden.

Zeitkriterium Die Kryptologie wurde bereits vor vielen Jahrtausenden verwendet, um Geheimbotschaften zu übermitteln. Bis zur heutigen Zeit wurden zahlreiche Ver-

schlüsselungen entwickelt und »geknackt«. In der Zukunft werden vorhandene Verschlüsselungsverfahren verbessert oder neue erfunden, um Daten und Nachrichten so gut wie möglich zu schützen. Dieser Wettlauf zwischen der Kryptographie und der Kryptoanalyse formt die Kryptologie und wird vermutlich niemals ein Ende finden.

Sinnkriterium Für Schülerinnen und Schüler ist die Kryptologie relevant, da sie sensible Daten besitzen, die geschützt werden müssen. Bereits Schülerinnen und Schüler in der Grundschule wollen Geheimnisse verwahren und finden Spaß daran, sich gegenseitig verschlüsselte Nachrichten zu schicken. Dafür verwenden sie beispielsweise Geheimsprachen oder -schriften. Dies ist in weiterführenden Schulen nicht anders. Neben Geheimschriften und Zettelchen kommen dort auch elektronische Geräte zum Einsatz. Diese Informatiksysteme hüten Geheimnisse und Nachrichten jedoch nicht so sicher, wie die meisten denken. Deswegen müssen das Wissen über diese Sicherheitsmängel und die Verbesserung zum Schutz von Daten an die Schülerinnen und Schüler weitergereicht werden.

Zielkriterium Das Ziel der Kryptologie ist, den Schülerinnen und Schülern den Umgang mit sensiblen Daten und Verschlüsselungen aufzuzeigen, um ihre Privatsphäre zu schützen.

Es ist unter verschiedenen Blickwinkeln sinnvoll und notwendig, den Umgang mit sensiblen Daten zu lernen. Neben dem praktischen Einsatz, der durch den Schutz von Daten erreicht wird, und dem theoretischen Wissen über Kryptosysteme zählen auch die Hintergründe der Kryptologie zum Pflichtlehrstoff. Dazu gehören beispielsweise ihren historischen Einsatz: „Kryptosysteme sind Waffen – sowohl Verteidigungswaffen wie auch Angriffswaffen. Wem das nicht klar ist, der hat aus dem Verlauf des 2. Weltkriegs nichts gelernt“ (F. L. Bauer, 1997, S. 6). Informatikerinnen und Informatiker müssen sich ihrer moralischen, politischen und rechtlichen Verantwortung bewusst sein. Sie können ihr Wissen nicht nur für die Gesellschaft, sondern auch gegen diese verwenden. Deswegen gibt es in den Bildungsdokumenten einen eigenen Inhaltsbereich *Informatik, Mensch und Gesellschaft*, in dem u. a. diese Dinge angesprochen werden.

Im Unterricht werden eine Vielzahl von Methoden verwendet, um die Lernergebnisse zu verbessern sowie das Vergnügen am Inhalt zu vergrößern. Dabei sollen nicht die Lehrkräfte, sondern die Schülerinnen und Schüler im Vordergrund stehen. Dies kann beispielsweise durch ein Thema geschehen, das selbst bearbeitet und gelernt werden kann. Dadurch erhöht sich die Eigenverantwortung und das Selbstbild der Schülerinnen und Schüler.

Die Kryptologie bietet sich für einen selbstlernenden Zugang an, da die Verschlüsselungsverfahren von den Schülerinnen und Schülern selbstständig durchgeführt und analysiert werden können. Außerdem sind die Verfahren unabhängig voneinander, weswegen die Reihenfolge der Bearbeitung keinen Einfluss auf das Lernergebnis hat. Deswegen hat die Bergische Universität Wuppertal ein Stationenlernen mit verschiedenen historischen und modernen Verschlüsselungsverfahren entwickelt, das im Unterricht frei genutzt werden kann. Das *SpionCamp* umfasst die Steganographie, die Codierung und symmetrische Verschlüsselungsverfahren sowie das Problem des Schlüsselaustausches.

Das SpionCamp wird bereits heute an vielen Schulen genutzt und bekommt von den Lehrkräften positives Feedback. Die Schülerinnen und Schüler lernen selbstständig auf verschiedene Arten und können sich gegenseitig Nachrichten schreiben. Dadurch ist ihre Motivation sehr hoch und das Interesse an der Kryptologie und der Informatik steigt. Die meisten Stationen sind für die Sekundarstufe I erstellt worden, weswegen sie dort auch häufig eingesetzt werden. Die Kryptologie ist jedoch auch im Kernlehrplan der Sekundarstufe II zu finden. Für den Einsatz in dieser fehlen allerdings schwierigere Verfahren, die aktuell genutzt werden und somit einen stärkeren Bezug zum Alltag der Schülerinnen und Schüler aufweisen.

Diese Arbeit analysiert das SpionCamp hinsichtlich der Kompetenzen, die in den Bildungsdokumenten des Landes Nordrhein-Westfalen zu finden sind, und zeigt die Erstellung zweier neuer Stationen für die Sekundarstufe II auf. Diese Stationen werden dann hinsichtlich ihrer Verständlichkeit und Durchführbarkeit evaluiert.

Die Idee, zwei neue Stationen zu entwickeln, kam mir während der Überarbeitung des SpionCamps bei meiner Tätigkeit als wissenschaftliche Hilfskraft der Didaktik der Informatik an der Bergischen Universität Wuppertal. Bei dieser Überarbeitung wurden einige Stationen erweitert oder verbessert. Außerdem entstanden dabei zwei weitere Stationen, die zusammen mit den bereits verfügbaren in Kapitel 3.2 vorgestellt werden.

1.3 Aufbau der Arbeit

In dieser wissenschaftlichen Arbeit werden neue anspruchsvolle Themen für das Stationenlernen zur Kryptologie entwickelt und getestet. In Kapitel 2 wird zunächst erläutert, was die Bildungsdokumente des Landes Nordrhein-Westfalen für die Kryptologie in den verschiedenen Schulstufen vorsehen und welche Kompetenzen die Schülerinnen und Schüler entwickeln sollen. Dafür werden die Bildungsstandards der Gesellschaft für Informatik, die Kernlehrpläne des Ministeriums für Schule und Bildung des Landes Nordrhein-Westfalen, die Vorgaben für das Zentralabitur sowie ein Beispiel für schulinterne Lehrpläne betrachtet. Danach wird in Kapitel 3 das SpionCamp vorgestellt, das Verfahren des

Stationenlernens aufgezeigt und die einzelnen Unterthemen des SpionCamps erläutert. Dies wird zeigen, wie die neuen Stationen eingegliedert und verknüpft werden können. Darauf folgend werden in Kapitel 3.3 einige weitere Unterrichtsmaterialien der Bergischen Universität Wuppertal vorgestellt, die sich mit der Kryptologie beschäftigen. Neben dem Materialangebot der Bergischen Universität Wuppertal gibt es natürlich zahlreiche weitere Institutionen, die Unterrichtsmaterial zur Kryptologie anbieten. In dieser Arbeit wird jedoch nur das mit dem SpionCamp in Verbindung stehende Material aufgezeigt. Einige weitere Beispiele werden in Kapitel 6 angesprochen.

In Kapitel 4 werden die beiden neuen Stationen schrittweise erläutert. Bei jeder von ihnen wird zuerst erklärt, wie es zur Wahl des jeweiligen Verfahrens gekommen ist. Es folgt der theoretische Hintergrund, der auch in den Stationen ansatzweise an die Schülerinnen und Schüler herangebracht werden soll. Der Aufbau und die Entscheidungen zur Realisierung werden in der didaktische Analyse aufgezeigt und am Ende werden die Kompetenzen genannt, die durch die neuen Stationen erworben werden. Kapitel 5 beschäftigt sich mit der Evaluation der neuen Stationen an zwei verschiedenen Schulen. Die Kommentare und Verbesserungsvorschläge der Lernenden und Lehrkräfte werden erläutert und in Kapitel 5.3 in die Stationen eingearbeitet. In Kapitel 6 wird ein Fazit hinsichtlich der neuen Stationen gezogen. Außerdem werden mögliche Erweiterungen für die Erfüllung der Kompetenzen aus den Bildungsdokumenten aufgezeigt.

Im Anhang befinden sich die aktuellen Versionen der neuen Arbeitsmaterialien und die in Kapitel 5 verwendeten Fragebögen. Wenn vorherige Versionen der Arbeitsmaterialien angesprochen werden, befindet sich der angesprochene Teil im Text. Wird im Text von Materialien des SpionCamps gesprochen, handelt es sich immer um die frei verfügbaren Materialien auf der Internetseite der Didaktik der Informatik an der Bergischen Universität Wuppertal (D. Müller, 2012). Dies wird zwar immer eindeutig genannt, jedoch aufgrund der hohen Verwendung nicht immer zitiert. Die neuen Materialien werden dort ebenfalls zur Verfügung gestellt.

2 Kryptologie in den Bildungsdokumenten für Nordrhein-Westfalen

In Nordrhein-Westfalen gibt es vier verschiedene Bildungsdokumentarten für das Fach Informatik. Zum einen veröffentlichte die *Gesellschaft für Informatik (GI)* Bildungsstandards für den Informatikunterricht, die jeweils von der Fachzeitschrift *LOG IN* als Beilage veröffentlicht wurden. Dabei handelt es sich um Kompetenzen, die aus Sicht der GI im Informatikunterricht erreicht werden sollen. Sie stellen „ein Minimum an Kompetenzen [dar], das jede Schülerin und jeder Schüler [...] aufweisen sollte“ (GI, 2008, S. 2).

Das *Ministerium für Schule und Bildung des Landes Nordrhein-Westfalen (MSB-NW)* (früher *Ministerium für Schule und Weiterbildung des Landes Nordrhein-Westfalen (MSW-NW)*) stellt die Kernlehrpläne bereit, an die sich die Schulen halten müssen. Für die Sekundarstufe I wird in dieser Arbeit der Kernlehrplan für das Wahlpflichtfach in Gymnasien betrachtet. Die Lehrpläne für Real- und Gesamtschulen unterscheiden sich nur wenig voneinander (vgl. MSW-NW, 2013, 2015a). Für die Hauptschulen wurde kein aktueller Kernlehrplan für Informatik veröffentlicht. Außerdem werden von der MSB-NW jährlich Vorgaben für das Zentralabitur mit inhaltlichen Schwerpunkten publiziert, um die Themenauswahl einzuschränken.

Bei den letzten zum aktuellen Zeitpunkt geltenden Vorgaben für das Fach Informatik handelt es sich um die schulinternen Lehrpläne. In ihnen halten die Schulen fest, was sie die Schülerinnen und Schülern in den verschiedenen Jahrgangsstufen lehren wollen. Da diese Lehrpläne für jede Schule unterschiedlich aufgestellt sind, werden in diesem Kapitel die Beispiele der *Qualitäts- und UnterstützungsAgentur – Landesinstitut für Schule (QUA-LiS NRW)* für eine fiktive Schule betrachtet. Die Primarstufe wird dabei ausgelassen, weil kein Beispiel eines schulinternen Lehrplans für den Sachunterricht existiert und Informatik dort nicht als eigenes Fach unterrichtet wird. Außerdem muss für die Informatik in der Sekundarstufe I der schulinterne Lehrplan für das Wahlpflichtfach an der Gesamtschule betrachtet werden, da ein solcher bislang für Gymnasien noch nicht veröffentlicht wurde. Das Beispiel für die Realschule entspricht diesem (vgl. QUA-LiS NRW, 2016b).

Im Unterschied zu den Bildungsstandards, die bereits Kompetenzen für die fünfte bis siebte Jahrgangsstufe festsetzen, werden diese Jahrgänge in den aktuellen G8-Kernlehrplänen und somit in den schulinternen Lehrplänen nicht beachtet, da Wahlpflichtfächer erst für die achte Klasse gewählt werden. Diese Jahrgänge werden somit noch nicht für die informatische Bildung eingeplant. In der 2018 veröffentlichten Stundentafel für G9 sind jedoch für alle Schülerinnen und Schüler der Sekundarstufe I zwei Wochenstunden „explizit für die Stärkung der informatischen Bildung vorgesehen“ (MSB-NW, 2018a, S. 3).

2.1 Bildungsstandards

Die Bildungsstandards der GI untergliedern die Kompetenzen des Informatikunterrichts in fünf Inhalts- und fünf Prozessbereiche (siehe Abbildung 1). Diese sind untrennbar miteinander verzahnt, da die Inhalte mittels Prozessen erschlossen werden. Die Kryptologie wird je nach Schulstufe in den Inhaltsbereichen *Information und Daten* und *Informatik, Mensch und Gesellschaft* angesiedelt. Während die jüngeren Schülerinnen und Schüler vor allem verstehen sollen, dass zwischen Darstellungsform und Bedeutung aufgrund von Codierungen und Verschlüsselungen ein deutlicher Unterschied liegt, sollen die älteren Schülerinnen und Schüler auf die Risiken im Umgang mit Informatiksystemen eingehen und deswegen Verschlüsselungsverfahren nutzen, um sicherer zu kommunizieren.

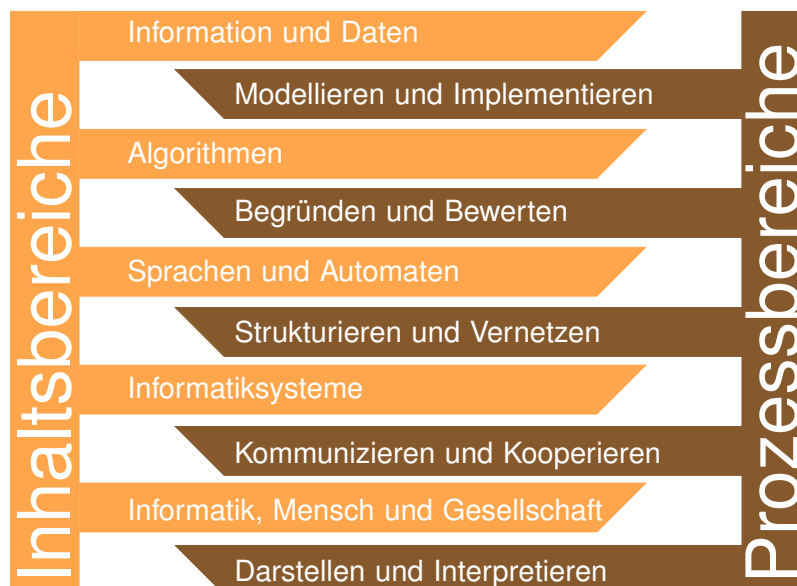


Abbildung 1: Prozess- und Inhaltsbereiche des Informatikunterrichts in den Bildungsstandards (GI, 2019, S. 7)

Die GI veröffentlichte 2019 die „Kompetenzen für informatische Bildung im Primarbereich“ (GI, 2019). Dort steht für den Inhaltsbereich *Information und Daten* geschrieben, dass Kryptologie zum Lebensweltbezug der Schülerinnen und Schüler gehört, da sich „vor allem bei persönlichen Daten [...] Fragen zur Sicherheit vor Verfälschung und geschützter Übertragung [stellen], die bereits für Kinder erfahrbar sind“ (ebd., S. 9). Deswegen sollte die Kryptologie bereits in der Grundschule unterrichtet werden. Dabei ist es wichtig, die Begriffe und Verfahren auf das Wissen der Schülerinnen und Schüler anzupassen. Die GI stellt in den Kompetenzerwartungen des Inhaltsbereichs sicher, dass „[der Begriff *Verschlüsselung*] frühzeitig von dem Begriff *Codierung* unterschieden werden [sollte], um beide Aspekte getrennt thematisieren zu können“ (ebd., S. 12, Hervorh. im Orig.). Dazu „bietet sich eine historisch orientierte Thematisierung einfacher Verschlüs-

selungsverfahren und deren Analyse an“ (GI, 2019, S. 12).

Die zu erwerbenden Kompetenzen der Schülerinnen und Schüler sind in Tabelle 1 dargestellt. Während am Ende der zweiten Klasse nur binäre Codierungen angewandt und begründet werden, wird am Ende der vierten Klasse von den Schülerinnen und Schüler erwartet, dass sie Verschlüsselungsverfahren anwenden und eigene Verfahren entwickeln.

Ende Klasse 2	Ende Klasse 4
Die Schülerinnen und Schüler ► erläutern, dass Dokumente aus Daten bestehen ► stellen Information mithilfe von Daten dar ► interpretieren Daten, um Information zu gewinnen ► geben an, dass Vereinbarungen notwendig sind, um Daten zu codieren und zu decodieren ► codieren Daten in eine binäre Darstellung und interpretieren binär dargestellte Elemente als Daten	Die Schülerinnen und Schüler ► entwerfen für eine kleine Anzahl verschiedener Elemente eine eigene binäre Codierung ► stellen Information in unterschiedlichen Repräsentationsformen (Text, Bild, Audio, Video) dar ► nutzen und entwickeln Vereinbarungen, um Daten zu verschlüsseln und zu entschlüsseln ► nutzen und entwickeln Vereinbarungen zur Übermittlung von Nachrichten

Tabelle 1: Kompetenzen im Inhaltsbereich *Information und Daten* für den Primarbereich (GI, 2019, S. 13)

Für die Sekundarstufe I verabschiedete die GI 2008 die „Grundsätze und Standards für die Informatik in der Schule“ (GI, 2008). Von der fünften bis siebten Jahrgangsstufe lernen die Schülerinnen und Schüler Bedeutung und Darstellungsform einer Nachricht zu unterscheiden (vgl. ebd., S. 24). Sie sollen mittels Beispielen (z. B. Codierungen oder selbsterfundenen „Geheimschriften“) unterschiedliche Darstellungsformen einer Nachricht kennenlernen und sich gegenseitig „geheime“ Nachrichten schicken oder „Rätsel“ lösen (vgl. ebd., S. 25). Alle Jahrgangsstufen sollen zusätzlich im Inhaltsbereich *Informatik, Mensch und Gesellschaft* „angemessen auf Risiken bei der Nutzung von Informatiksystemen [reagieren]“ (ebd., S. 18). Dafür werden die Schülerinnen und Schüler der achten bis zehnten Jahrgangsstufe dahingehend sensibilisiert, dass einige Daten sehr persönlich und deswegen schützenswert sind, und stellen sich dann die Frage, wie sie geschützt werden können (vgl. ebd., S. 44). Sie sollen mindestens ein einfaches Verfahren im Unterricht behandeln, damit sie „die Unsicherheiten einfacher Verschlüsselungsverfahren [erkennen]“ (ebd., S. 41).

Die „Bildungsstandards Informatik für die Sekundarstufe II“ (GI, 2016) wurden 2016 von der GI publiziert und ordnen die Kryptologie dem Inhaltsbereich *Informatik, Mensch und Gesellschaft* zu. In diesem werden „Entscheidungsfreiheiten im Umgang mit Infor-

matiksystemen, Handeln in Übereinstimmung mit gesellschaftlichen Normen und angemessenes Reagieren auf Risiken bei der Nutzung von Informatiksystemen [...] reflektiert“ (GI, 2016, S. 12). Dafür sollen die Schülerinnen und Schüler auf dem grundlegenden und erhöhten Anforderungsniveau unter anderem „Verfahren zur Sicherung von Vertraulichkeit, Authentizität und Integrität von Daten [verwenden und beschreiben]“ (ebd., S. 12). Auf dem erhöhten Anforderungsniveau sollen sie zusätzlich die Verfahren „in konkreten aktuellen Anwendungskontexten [analysieren und beurteilen]“ und „Maßnahmen zur Realisierung von Datensicherheit für konkrete Anwendungsfälle, insbesondere Zugriffskontrolle [konzipieren]“ (ebd., S. 12).

2.2 Kernlehrpläne

Das MSB-NW veröffentlicht in Anlehnung an die Bildungsstandards der GI die Kernlehrpläne für das Unterrichtsfach Informatik. Aus ihnen werden die schulinternen Lehrpläne der einzelnen Schulen abgeleitet. Sie bilden somit das rechtlich aussagekräftigste Bildungsdokument. Der Kernlehrplan der Sekundarstufe II unterteilt die zu erwerbenden Kompetenzen der Schülerinnen und Schüler in fünf Kompetenzbereiche und fünf Inhaltsfelder (zu sehen in Abbildung 3 auf Seite 12). Während die Inhaltsfelder den Inhaltsbereichen der Bildungsstandards entsprechen, unterscheiden sich die Kompetenzbereiche von den Prozessbereichen an mehreren Stellen. Der Prozessbereich *Modellieren und Implementieren* wurde in zwei Kompetenzbereiche aufgeteilt, dafür fehlt der Prozessbereich *Strukturieren und Vernetzen*. Die Kompetenzbereiche und Inhaltsfelder wurden im 2019 erschienen Kernlehrplan der Sekundarstufe I für das Wahlpflichtfach Informatik angepasst (zu sehen in Abbildung 2 auf Seite 11). Nun sind die Kompetenzbereiche *Modellieren* und *Implementieren* wieder ein gemeinsamer Kompetenzbereich, es fehlt jedoch immer noch der Bereich *Strukturieren und Vernetzen*.

Während die GI Informatik bereits fest in der Grundschule verankert sehen möchte, ist der Begriff *Informatik* kein einziges Mal in den Kernlehrplänen des Landes Nordrhein-Westfalen für die Primarstufe zu finden (vgl. MSW-NW, 2008). Die MSB-NW hat allerdings 2015 das Projekt *Informatik an Grundschulen* in die Wege geleitet und es an einigen Grundschulen im Sachunterricht getestet. Dieses Projekt wird in Kapitel 3.3.2 näher betrachtet.

Der Kernlehrplan für das Wahlpflichtfach Informatik in der Sekundarstufe I an Gymnasien wurde im Juli 2019 veröffentlicht und gilt gleichermaßen für den verkürzten (G8) und den neunjährigen Bildungsgang (G9) (MSB-NW, 2019a). Dies hängt damit zusammen,

dass zukünftig ein Wahlpflichtfach Informatik (oder eine Fächerkombination mit Informatik) an jedem Gymnasium angeboten werden muss (vgl. MSB-NW, 2018b, S. 3). Zwischen den Kompetenzen der Kryptologie in den Empfehlungen der GI und dem gymnasialen Kernlehrplan für das Wahlpflichtfach Informatik gibt es nur wenige Unterschiede. Laut dem Kernlehrplan unterscheiden die Schülerinnen und Schüler im Inhaltsfeld *Information und Daten* ebenfalls zwischen diesen beiden Elementen (vgl. MSB-NW, 2019a, 14 f.). Dafür „codieren [sie] Daten für die Verarbeitung mit einem Informatiksystem“ (vgl. ebd., S. 18). Außerdem ist die Kryptologie wieder im Inhaltsfeld *Informatik, Mensch und Gesellschaft* untergebracht, in dem steht, dass die Schülerinnen und Schüler „die Gefährdung von Daten durch Defekte und Schadsoftware [beschreiben] und [...] Maßnahmen zum Schutz von Daten [benennen]“, „Maßnahmen zur sicheren Kommunikation in Netzwerken [nennen] und [...] diese [anwenden]“ und „die Unsicherheit eines einfachen Verschlüsselungsverfahrens [erläutern]“ (ebd., S. 21).

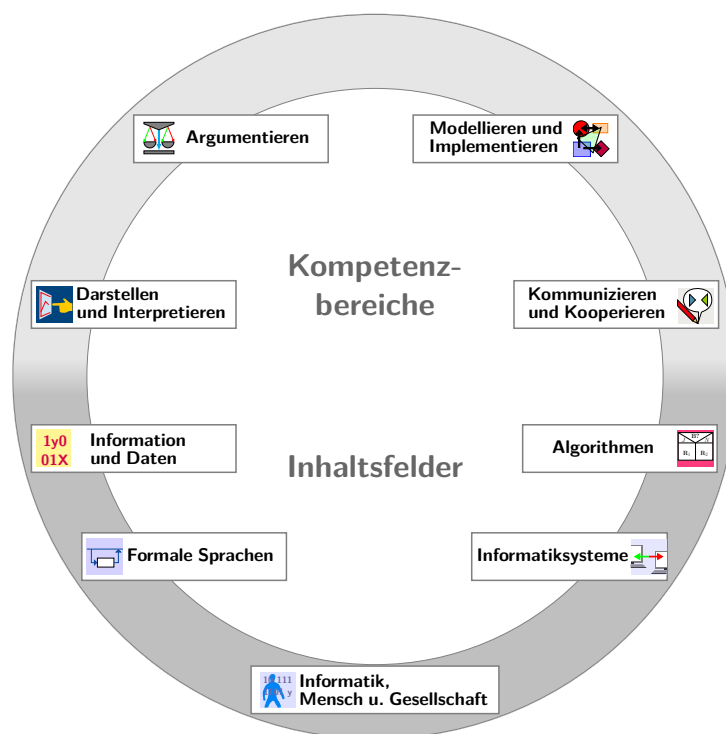


Abbildung 2: Kompetenzbereiche und Inhaltsfelder im Kernlehrplan des Wahlpflichtfaches Informatik an Gymnasien (nach MSB-NW, 2019a, S. 18)

Für die gymnasiale Oberstufe wurde 2014 der Kernlehrplan für Informatik von der MSB-NW herausgegeben. In ihm werden Verschlüsselungen im Inhaltsfeld *Informatiksysteme* unter dem inhaltlichen Schwerpunkt *Sicherheit* angesiedelt. Die Schülerinnen und Schüler, die einen Grundkurs besuchen, sollen „Eigenschaften und Einsatzbereiche sym-

metrischer und asymmetrischer Verschlüsselungsverfahren [analysieren und erläutern]“ (MSW-NW, 2013, S. 32). Im Leistungskurs kommt zusätzlich die Funktionsweisen der Verschlüsselungsverfahren hinzu (vgl. ebd., S. 38). Weitere Hinweise oder zu erwerbende Kompetenzen sind nicht angegeben.

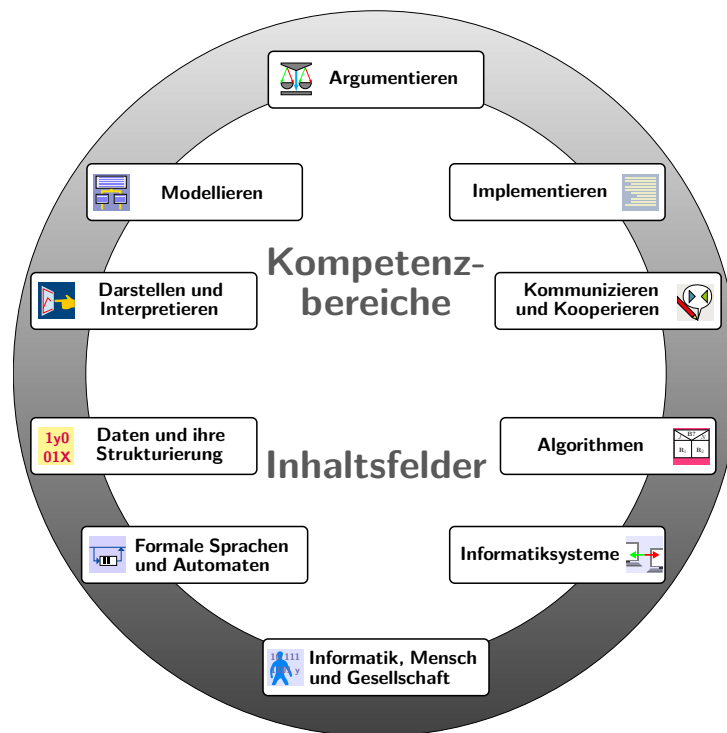


Abbildung 3: Kompetenzbereiche und Inhaltsfelder im Kernlehrplan Informatik für die gymnasiale Oberstufe (nach MSW-NW, 2013, S. 19)

2.3 Vorgaben für das Zentralabitur

Über den Kernlehrplan der Sekundarstufe II hinaus, werden von der MSB-NW jährlich Vorgaben für das Zentralabitur in den einzelnen Fächern veröffentlicht. Diese orientieren sich an dem jeweiligen Kernlehrplan und fokussieren die Themenbereiche, „damit alle Schülerinnen und Schüler, die im Jahr 2019 das Abitur ablegen, gleichermaßen über die notwendigen inhaltlichen Voraussetzungen für eine angemessene Anwendung der Kompetenzen bei der Bearbeitung der zentral gestellten Aufgaben verfügen“ (MSB-NW, 2018c, S. 1). Dabei schränkt die Fokussierung jedoch nicht die Pflichtthemen für die gesamte Oberstufe ein, da deren Realisierung in der Verantwortung der Lehrkräfte liegt (vgl. ebd., S. 1). „In der Abiturprüfung werden daher grundsätzlich **alle** Kompetenzerwartungen vorausgesetzt, die der Lehrplan für das Ende der Qualifikationsphase der gymnasialen Oberstufe vorsieht“ (ebd., S. 1, Hervorh. im Orig.). Im vergangenen Zentralabitur 2019 und den zwei kommenden Abiturjahrgängen 2020 und 2021 sind die Themen des in-

haltlichen Schwerpunktes *Sicherheit* und auch des Inhaltsfeldes *Informatiksysteme* nicht fokussiert.

Die Auswahl der Abituraufgaben wird aus den fünf Inhaltsfeldern getroffen. Die Lehrkräfte der Grund- und Leistungskurse dürfen aus jeweils vier zentral gestellten Aufgaben zwei bzw. drei Aufgaben wählen. Dabei muss eins der Inhaltsfelder *Daten und ihre Strukturierung* oder *Algorithmen* vorkommen. Die Kryptologie kann, muss aber nicht, in Abituraufgaben angesprochen werden (vgl. MSB-NW, 2018c,d, 2019b).

2.4 Schulinterne Lehrpläne

Im „Beispiel für einen schulinternen Lehrplan zum Kernlehrplan der Gesamtschule im Wahlpflichtfach Informatik“ (QUA-LiS NRW, 2016a) wird die Kryptologie in der Jahrgangsstufe 9 im Unterrichtsvorhaben *Geheim ist geheim? Sichere Kommunikation mit Kryptographie* mit 15 Stunden eingeplant (ebd., S. 14). Die inhaltlichen Schwerpunkte für dieses Unterrichtsvorhaben sind (ebd., S. 14):

- Daten und ihre Codierung
- Erfassung, Verarbeitung und Verwaltung von Daten
- Algorithmen zum Lösen von Aufgaben und Problemen aus verschiedenen Anwendungsgebieten
- Formale Sprachen und einfache Automaten
- Anwendung verschiedener Informatiksysteme
- Informatiksysteme im Kontext gesellschaftlicher und rechtlicher Normen
- Chancen und Risiken bei der Nutzung von Informatiksystemen

Dabei sollen die Schülerinnen und Schüler zunächst dafür sensibilisiert werden, dass einige ihrer Daten privat sind und deswegen geschützt werden sollten. Sie diskutieren die Notwendigkeit von Geheimhaltung und beurteilen das Problem fehlender Anonymität in Netzwerken. Daraufhin lernen sie unterschiedliche steganographische Verfahren des Altertums sowie der Neuzeit kennen und entdecken den Bedarf von kryptographischen Verfahren. Anhand von Beispielen wird die Ver- und Entschlüsselung eingeübt sowie die Kryptoanalyse besprochen. Die Schülerinnen und Schüler lernen außerdem ein modernes Verfahren der asymmetrischen Verschlüsselung kennen und führen die Verschlüsselung von Mails beispielhaft durch (vgl. ebd., S. 60-62).

Im „Beispiel für einen schulinternen Lehrplan zum Kernlehrplan für die gymnasiale Oberstufe“ (QUA-LiS NRW, 2014) soll die Kryptologie für den Grundkurs im Unterrichtsvorhaben der Qualifikationsphase 1 *Sicherheit und Datenschutz in Netzstrukturen* im Umfang von zehn Stunden bearbeitet werden (ebd., S. 13). Als inhaltliche Schwerpunkte werden ausgewiesen (ebd., S. 13):

- Einzelrechner und Rechnernetzwerke
- Sicherheit
- Nutzung von Informatiksystemen, Wirkungen der Automatisierung

An das Thema *Datenbanken* anschließend lernen die Schülerinnen und Schüler Sicherheitsaspekte beim Zugriff auf Datenbanken und verschiedene symmetrische sowie asymmetrische kryptographische Verfahren kennen. Sie sehen außerdem Beispiele zur Datenschutzproblematik und zum Urheberrecht (ebd., 51 f.).

Im Leistungskurs wird die Kryptologie in der Qualifikationsphase 2 in dem Unterrichtsvorhaben *Sicherheit und Datenschutz in Informatiksystemen sowie Grenzen und Auswirkungen der Automatisierung* in 20 Stunden erarbeitet. Dabei werden die folgenden inhaltlichen Schwerpunkte gesetzt (ebd., S. 19):

- Nutzung von Informatiksystemen
- Sicherheit
- Wirkungen der Automatisierung
- Grenzen der Automatisierung

In diesem Vorhaben sollen die Schülerinnen und Schüler die moralische und rechtliche Verantwortung von Informatikerinnen und Informatikern sowie die Notwendigkeit zum Schutz von sensiblen Daten erkennen. Dafür werden die grundlegenden Sicherheitsziele *Vertraulichkeit*, *Integrität* und *Verfügbarkeit* definiert und sowohl symmetrische als auch asymmetrische Verschlüsselungsverfahren zur Umsetzung der Ziele eingeführt. Dabei sollen auch der Angriff auf die Verschlüsselungsverfahren, das Problem des Schlüsselaustausches und das Prinzip des Signierens besprochen werden (ebd., S. 90-94).

3 Das SpionCamp

Durch das *MathePrisma* (Fachbereich C / Mathematik der Bergischen Universität Wuppertal, 2001), das in Kapitel 3.3.1 vorgestellt wird, inspiriert, wurde ab 2004 unter der Leitung von GABRIEL und SCHÄFER die *Spionschule* an der Bergischen Universität Wuppertal erstellt. Im Jahr 2011 wurden die Lernstationen zur Kryptologie aufgrund von Lizenzproblemen bei der Verwendung einiger Abbildungen unter der Leitung von D. MÜLLER sowohl in einer Examens- als auch in einer Forschungsarbeit überarbeitet und dann öffentlich zur Verfügung gestellt. Dabei wurde der negativ behaftete Begriff *Schule in Camp* geändert. Durch die Überarbeitung entstanden auch Anleitungen zur Erstellung und Handhabung der Stationen sowie anspruchsvollere Stationen für die Sekundarstufe II. Die Stationen beziehen sich dabei nicht nur auf die Kryptographie, sondern auch auf die Kryptoanalyse und umfassen somit die gesamte Kryptologie (Aust, D. Müller und Gabriel, 2011, S. 3).

Das Entdecken verschiedener Verschlüsselungsverfahren steht an den Lernstationen im Vordergrund. Die Schülerinnen und Schüler werden in die Rolle eines Angreifers versetzt und entwickeln Möglichkeiten zum »Knacken« der Verfahren. Von den frühen Verschlüsselungsverfahren, die lediglich einen sicheren Umgang mit Alphabeten erfordern, bis hin zu modernen Verfahren, die in höherem Maße mathematische Grundlagen verwenden, bieten die Stationen verschiedene Schwierigkeitsstufen.

Aust, D. Müller und Gabriel, 2011, S. 236

3.1 Stationenlernen

Das *Stationenlernen*, bzw. alternativ als *Lernen an Stationen* bezeichnet, ist eine Methode für den Unterricht, bei der die Schülerinnen und Schüler selbstständig Aufgaben wählen und bearbeiten. Dafür werden unterschiedliche Arbeitsaufträge zu einem oder mehreren zueinander passenden Themen im Raum verteilt. Dadurch haben die Schülerinnen und Schüler mehr Entscheidungsfreiraum und können ihren eigenen Lernweg selbst gestalten. R. BAUER geht davon aus, man müsse die Stationen nicht nacheinander, sondern könnte sie in einer beliebigen Reihenfolge erledigen (vgl. R. Bauer, 1997, S. 59).

Die Grundidee kommt aus dem Zirkeltraining, das ursprünglich dem Sportunterricht entstammt. Bei diesem werden verschiedene Übungsstationen zur Verfügung gestellt, die zwischen zwei bis fünf Minuten dauern. Diese Idee wurde auf Übungen und Lernaufgaben aus anderen Fächern übertragen (vgl. ebd., S. 57-61).

Im ersten Schritt wird nun theoretisch begründet, wieso Stationenlernen sinnvoll ist. Dafür werden einige Erkenntnisse der Bildungswissenschaften genauer betrachtet.

Die konstruktivistische Didaktik sieht das Lernen als interaktiven Prozess, „bei dem Lehrer und Lerner am selben Vorgang teilhaben, aber aus unterschiedlichen Perspektiven beobachten, teilnehmen und agieren“ (Kontschinsky, 2003, S. 4). Die Schülerinnen und Schüler sind also am Lernvorgang aktiv beteiligt und sollen Wissen konstruieren, rekonstruieren und dekonstruieren. Die Lehrkraft soll dabei als Hilfestellung und Ratgeber gelten. Durch die „ungewohnte Entscheidungsfreiheit“ erhalten auch die Erfolgserlebnisse mehr Bedeutung und „hemmende Selbstvergleiche“ mit anderen Lernenden werden vermieden. Das Stationenlernen erfüllt die Forderungen der konstruktivistischen Methoden, da die Eigenständigkeit der Schülerinnen und Schüler bei dieser Methode im Vordergrund steht. Sie planen und bearbeiten das Lernen an den einzelnen Stationen und hinterfragen Gegenstände, um Wissen zu erlangen. Außerdem entsteht durch das Lernen an Stationen eine Methodenvielfalt und verschiedene Sozialformen können angewandt werden, wodurch das kooperative Arbeiten unterstützt wird (vgl. ebd., S. 4-6).

Das Stationenlernen geht individuell auf die Entwicklung der Schülerinnen und Schüler ein, da jede und jeder von ihnen in ihrem oder seinem eigenen Lerntempo lernen kann. Dies ist sehr wichtig, da „sich in jeder Klasse mindestens drei Entwicklungsjahrgänge befinden“ (vgl. R. Bauer, 1997, S. 34). Eine Ausrichtung am Durchschnittstempo über- oder unterfordert somit den Großteil der Klasse. Auch der Wechsel der Repräsentationsebenen kann im Stationenlernen gut realisiert werden. Von der handelnden *enaktiven* Ebene über die bildliche *ikonische* Ebene bis hin zur Darstellung mithilfe von Symbolen, also der *symbolischen* Ebene, kann alles im Stationenlernen realisiert werden. Dies spricht verschiedene Lerntypen an und steigert die Lernmotivation (vgl. ebd., S. 106-110).

Neuere Erkenntnisse beziehen sogar die Beteiligung möglichst vieler Sinnesorgane und den Wechsel der Eingangskanäle in eine positive Beeinflussung des Lernens ein. Auch dies kann in verschiedenen Stationen realisiert werden. Durch diese vielseitige Darbietung wird der Lerninhalt für die Schülerinnen und Schüler interessanter und bei Lernschwierigkeiten auf einem Lernkanal, kann auf einen anderen gewechselt werden. Auch der positive Einfluss von Bewegung auf den Wissenserwerb kann durch die Bewegung im Raum erfüllt werden (vgl. Kontschinsky, 2003, S. 5).

Kommen wir nun zu den Eigenschaften von Stationenlernen. Das Stationenlernen besteht aus den folgenden Elementen, wobei die grau geschriebenen Elemente von KONTSCHINSKY als optional angesehen werden (vgl. ebd., S. 7-10):

Thema Besonders geeignet sind Themen oder Themengebiete, die Raum für Erfahrungslernen bieten. Außerdem sollten sie über vielfältige Zugänge erschlossen, in tendenziell unabhängige Lernabschnitte unterteilt und alleine erarbeitet werden können.

Lernraum Der Raum, in dem das Stationenlernen stattfinden soll, sollte genug Platz für die Stationen und ausreichend Arbeitsplätze bieten. Dafür kann die Durchführung auch außerhalb des Klassenraums stattfinden oder in verschiedene Räume aufgeteilt werden.

Lernstationen An festgesetzten Orten im Lernraum liegen Arbeitsaufträge aus, die einen thematischen oder didaktischen Schwerpunkt setzen. Dabei ist es sinnvoll, einige Stationen als Pflicht- und andere als Wahlstationen zu kennzeichnen, um mehr Wahlmöglichkeiten zu geben. Manchmal werden auch Zeitangaben für die Stationen festgesetzt, um den Zeitdruck zu erhöhen.

Arbeitsaufträge Die Aufgaben an den einzelnen Stationen sollten von überschaubarem Umfang sein, da es sich beim Stationenlernen um kleinschrittiges Lernen handelt. Jeder Arbeitsauftrag präsentiert einen Abschnitt des Themas und sollte in seiner Lösbarkeit einsehbar sein. Die Reihenfolge der Bearbeitung der Arbeitsaufträge sollte möglichst frei wählbar sein, um den Lernweg der Schülerinnen und Schüler nicht einzuschränken. Die Arbeitsaufträge müssen in einer ausreichenden Zahl an der Station vorhanden sein, damit es nicht zu einem »Stau« kommen kann. Außerdem sollte in den Arbeitsaufträgen ersichtlich werden, ob die Stationen in Einzel-, Partner- oder Gruppenarbeit geleistet werden sollen.

Arbeitsmaterial Im Stationenlernen ist keine Materialform ausgeschlossen. Zu jeder Station gehört eine schriftliche Anweisung, welche Aufgaben zu lösen sind, welche Hilfsmittel verwendet werden können und was mit dem Ergebnis geschehen soll.

Arbeitsplatz Jeder Lernende benötigt zur Bearbeitung ausreichend Platz. Dieser kann sich am angestammten Platz in der Klasse oder an der Station befinden. Die Arbeitsplätze müssen in die Organisation des Stationenlernens eingeplant werden.

Lehrender Das Stationenlernen ist nicht von der Präsenz der Lehrperson abhängig. Sie kann sogar zeitweise ohne Lehrperson funktionieren. Die Lehrperson sollte jedoch die Vorbereitung und Durchführung anleiten und das Lernen auswerten.

Laufzettel Teilweise kann es nützlich sein, wenn die Schülerinnen und Schüler auf einem Zettel vermerken können, welche Stationen sie bereits bearbeitet haben, um

mehr Orientierung auf dem Lernweg zu haben. Dabei kann ein gemeinsamer Zettel im Klassenraum ausgehängt werden oder jeder Lernende führt ihn mit sich.

Auf- und Abbau, Vorbereitung, Auswertung Alle Teilnehmer des Stationenlernens sind auch an diesen Phasen beteiligt. Häufig ist es vorteilhaft, wenn die Schülerinnen und Schüler bereits bei der Vorbereitung mit dem Material in Kontakt treten, da ihr Interesse früher geweckt wird und sie mehr Verantwortung übernehmen. Auch Pausen sollten beim Lernen eingeplant werden, was durch eine Entspannungsstation geschehen kann.

Arbeitsjournal In einem Arbeitsjournal kann festgehalten werden, was die Lernenden erarbeitet haben und was sie daraus ableiten. Außerdem kann es als Selbstüberprüfung oder zur Überprüfung durch die Lehrperson genutzt werden.

Dokumentenmappe Alle Materialien können in einer Dokumentenmappe gesammelt werden. Sie kann bei der Auswertung der Lernphasen helfen.

Hilfesystem Durch ein Hilfesystem können Schülerinnen und Schüler Hilfe einfordern. Dies kann beispielsweise durch „Patenschaften“ von Schülerinnen und Schülern für bestimmte Lernstationen realisiert werden.

Das Stationenlernen kann in sechs Arbeitsphasen eingeteilt werden, die von der Planung bis zur Auswertung reichen. Dieser Ablauf ist in Abbildung 4 auf Seite 19 skizziert.

Die *Planung und Konzeption* eines Stationenlernens sind sehr zeitaufwendig, da der Erfolg von der Qualität der Vorbereitung abhängt. Die Lehrperson muss das Thema, den Lernzweck, die Leitstruktur und die Teilziele unter Berücksichtigung der Voraussetzungen der Lernenden festlegen und sich überlegen, wie sie das Lernen beurteilen will. Außerdem muss die Zeit- und Raumplanung beachtet werden. In diese Phase kann man die Lernenden miteinbeziehen, beispielsweise in die Themenwahl, die Leistungskriterien oder die Erstellung der Stationen.

Bei der *praktischen Vorbereitung und Bereitstellung* wird das Konzept in Lernaufträge übersetzt und im Lernraum positioniert. Dafür muss das Material und die Arbeitsmittel zusammengestellt und die Aufträge formuliert werden. Sind Hilfen gewünscht, werden diese zusätzlich eingeplant. Auch in dieser Phase können die Lernenden einbezogen werden, wodurch sich die folgende *Einführungsphase* erübrigt.

In der *Einführungsphase* sollen alle Beteiligten erfahren, wie das Stationenlernen funktioniert. Dafür müssen das Thema, die Lernziele und die Arbeitsregeln erläutert sowie die Arbeitsmittel und Hilfen kennengelernt werden. Außerdem sollen die Schülerinnen und Schüler die Stationen betrachten, um ihren Lernweg vor auszuplanen.

Während der *Durchführung* arbeiten die Schülerinnen und Schüler an den Stationen und tragen die erledigten Aufgaben auf dem Laufzettel ein. Diese Phase kann sich von ein bis zwei bis hin zu vielen Unterrichtseinheiten erstrecken. Im *Offenen Unterricht* ist eine längere Durchführungsphase typisch. Bei einer Bearbeitung in Gruppen bietet sich auch ein Rotationsverfahren an, bei dem die Gruppen nach einer festen Zeit die Station wechseln. Dabei ist es jedoch umso wichtiger, dass es keine festgelegte Reihenfolge gibt.

Das Überprüfen der Ergebnisse wird in der *Ergebniskontrolle und Präsentation* durchgeführt. Der (zeitliche) Rahmen ist dabei nicht festgesetzt. Ergebniskontrollen können am Ende jedes Arbeitsauftrags oder am Ende des Stationenlernens geschehen. Dies hängt von der gewollten Korrekturmöglichkeit und Leistungsbeurteilung ab. Die Leistungskontrolle kann auf verschiedene Arten realisiert werden.

Die *Auswertung* geschieht im Idealfall zwischen allen Beteiligten. Dabei sollen gelungene und nicht gelungene Situationen des Stationenlernens berücksichtigt werden, damit die Ergebnisse der Auswertung allen zugutekommt (vgl. Kontschinsky, 2003, S. 10-13).

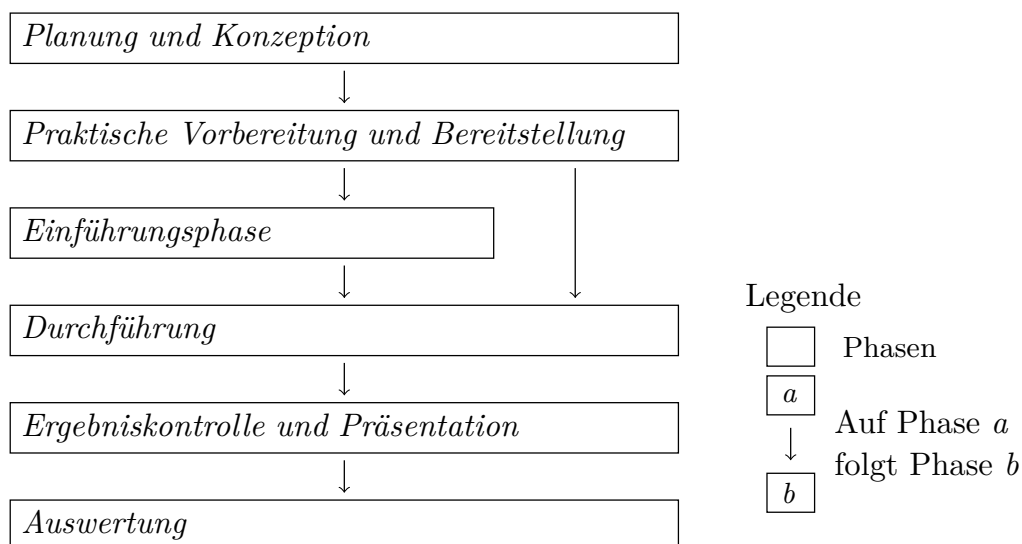


Abbildung 4: Phasen des Stationenlernens (vgl. Kontschinsky, 2003, S. 10-13)

Durch das Lernen an Stationen lernen die Schülerinnen und Schüler (Kontschinsky, 2003, S. 15)

- Aufgaben gezielt und in [gewisser] Reihenfolge zu bearbeiten,
- dabei Zeitregelungen einzuhalten,
- sich neugierig und experimentell zu verhalten (forschende Einstellung),
- eigene Entscheidungen zu begründen und zu treffen,

- Lösungen zu dokumentieren und zu präsentieren.

Außerdem kann in Partner- und Gruppenarbeit gelernt werden

- miteinander zu kooperieren,
- sich auf bestimmte Entscheidungen mehrheitlich zu einigen,
- abweichende Meinungen einzubeziehen [sowie]
- arbeitsgleiches und arbeitsteiliges Vorgehen zu praktizieren.

Nach KONTSCHINSKY würden sich die Schülerinnen und Schüler durch das Stationenlernen über Sinn und Verwendbarkeit des Lernstoffes klar und entwickeln eigenes Interesse daran. Die Vorbereitung und Durchführung sei zeitaufwendig, ermögliche jedoch positive Lernerfahrungen auf der Inhalts- und der Beziehungsebene (Kontschinsky, 2003, S. 15).

Neben den positiven Effekten des Stationenlernens gibt es jedoch auch problematische Seiten, die abgewogen werden müssen. Nicht jedes Thema bietet sich für ein Stationenlernen an, da zwischen den Stationen schlecht Verbindungen und Zusammenhänge hergestellt werden können. Dies liegt zum einen am kleinschrittigen Lernen und zum anderen an der möglichst beliebigen Reihenfolge der Bearbeitung. Auch der Zeitrahmen stellt ein Hindernis dar. Lässt man Schülerinnen und Schüler vollkommen frei arbeiten, benötigen sie viel Zeit. Einigen von ihnen fehlt es möglicherweise an Motivation, worauf die Lehrkraft schlecht Einfluss nehmen kann. Dadurch werden viele Unterrichtsstunden für ein Lernen an Stationen benötigt. Neben der zeitaufwendigen Vorbereitung und Durchführung ist auch die Auswertung und Leistungsbeurteilung schwierig, da sie individuell gestaltet sein muss.

Das SpionCamp stellt kein komplett fertig ausgearbeitetes Stationenlernen dar. Die Entscheidungen über den Lernraum, die Positionierung der Lernstationen und die Arbeitsplätze sind den ausführenden Lehrkräften überlassen. Sie können auch einzelne Stationen auslassen oder bearbeiten, weswegen es keinen vorgeschriebenen Laufzettel gibt. Eine Übersicht der Stationen kann von der Lehrkraft gestaltet werden und beispielsweise, wie in Abbildung 5 auf Seite 22 gezeigt, aussehen. Die Lehrkräfte müssen auch überlegen, wie sie die Schülerinnen und Schüler in die Vorbereitung einplanen und ob ein Arbeitsjournal, eine Dokumentenmappe oder ein Hilfesystem benötigt wird. Dies hängt von angestrebten Detailkompetenzen und pädagogisch-didaktischen Entscheidungen der Lehrkraft ab

und kann deswegen nicht vorgegeben werden. Außerdem muss sich die Lehrkraft Gedanken zur Leistungsbeurteilung bzw. Auswertung machen. Die Stationen sind unterschiedlich schwierig und beziehen sich teilweise aufeinander. Dadurch ist die Reihenfolge nicht vollkommen beliebig, was den Schülerinnen und Schülern mitgeteilt werden muss.

3.2 Die Unterthemen des SpionCamps

Die Materialien des SpionCamps können nicht nur als Stationenlernen, sondern auch in anderen Kontexten im Unterricht eingebaut werden. Dabei ist es teilweise sinnvoll, die Schülerinnen und Schüler die Stationen und Materialien innerhalb von Expertengruppen selbst erstellen zu lassen. Dadurch kann man den „kooperative[n] Aspekt des Lernens in den Vordergrund [stellen] und reziprokes Lernen [erproben]“ (Aust, D. Müller und Gabriel, 2011, S. 2).

Die Stationen des SpionCamps sind zurzeit in acht Unterthemen gegliedert. Diese Unterthemen stellen dabei unterschiedliche Verschlüsselungsarten und die Stationen unterschiedliche Verschlüsselungsverfahren dar. Die Stationen können verschiedenen Schwierigkeitsstufen zugeordnet werden, wobei diese vom Jahrgang abhängig sind, in dem das SpionCamp durchgeführt wird. Dabei sind beispielsweise die Stationen zu den Codierungen leichter und die Station zum Diffie-Hellmann-Algorithmus sowie zur Playfair-Verschlüsselung schwieriger. Wie bereits angesprochen, sind zwei Stationen während der Überarbeitung entstanden. Ihre Entwicklung ist noch nicht vollkommen abgeschlossen. Alle Stationen bestehen jeweils aus einem Stations-, einem Arbeits- und einem Lösungsblatt. Bei bestimmten Stationen entfällt eins der Blätter oder es gibt mehrere von ihnen. Auf dem Stationsblatt einer jeden Station ist zuerst ein Informationskasten zum Unterthema angegeben, worauf möglichst eine historische Eingliederung des Verfahrens folgt. Durch Beispiele wird dann die Ausführung des Verschlüsselungsverfahrens erläutert, wohingegen die Entschlüsselungsverfahren meist von den Schülerinnen und Schülern gefunden werden sollen. Zu mehreren Themen gibt es zusätzliches Material, das Unterstützung zur erfolgreichen Bearbeitung der Aufgaben bietet. Dazu gehört beispielsweise die Caesar-Scheibe oder die Rotoren.

Einige Schulen besitzen bereits einen Spionkoffer (zu sehen in Abbildung 6 auf Seite 23), bei dem es sich um einen Metallkoffer mit Fächeraufteilung und Spion-Logo handelt, der von der Bergischen Universität Wuppertal bei besonderen Anlässen verschenkt wird. In diesem Koffer befinden sich alle benötigten Materialien für das SpionCamp und zusätzlich Fähnchen in drei verschiedenen Farben sowie Fähnchenhalter zur Markierung der Schwierigkeitsstufen der Stationen. Die Stationsblätter und einige Hilfsblätter (z. B. ein separates Morsealphabet) sind laminiert, um die Stabilität zu gewähren. Dieser Koffer

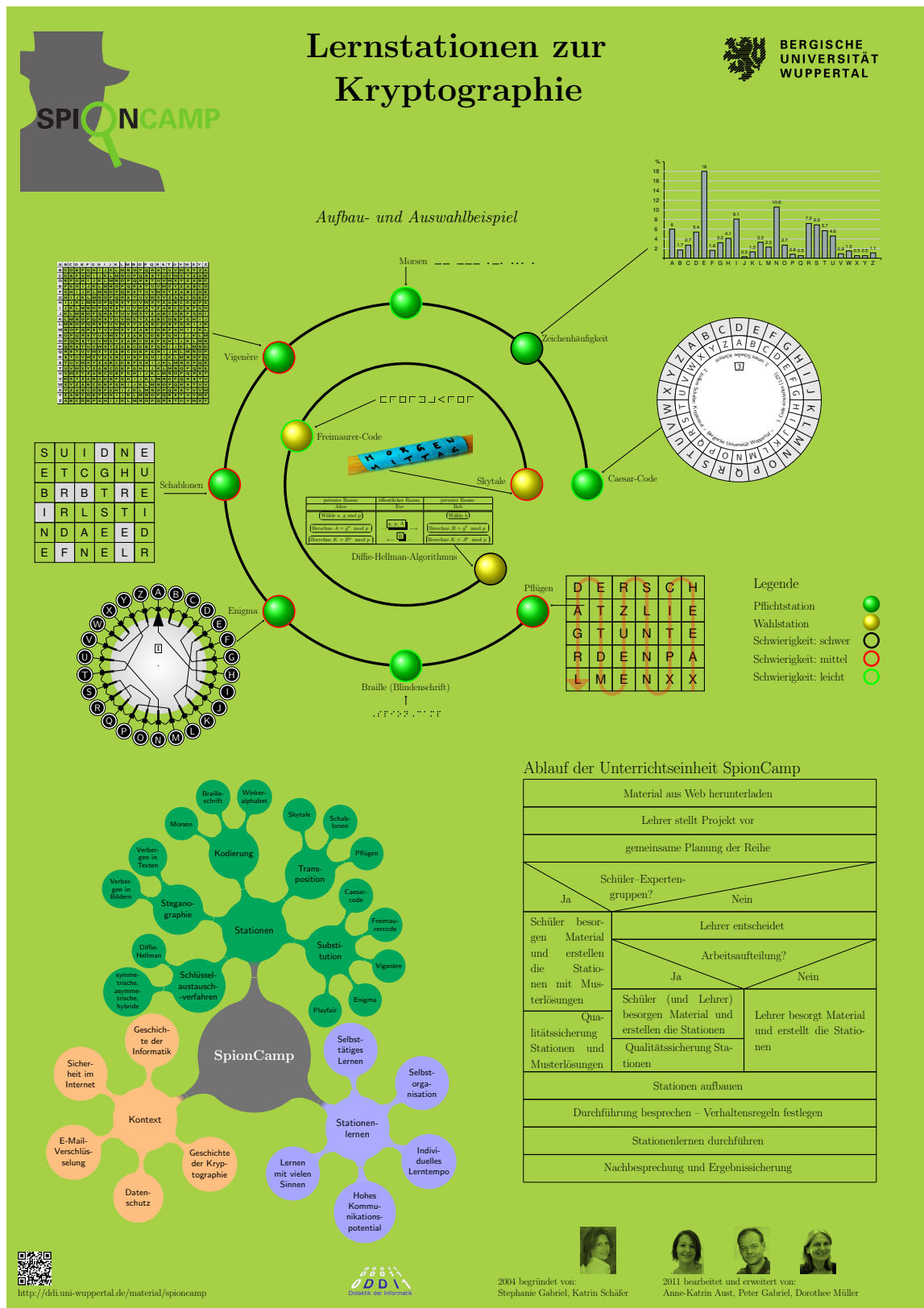


Abbildung 5: Überblick zum SpionCamp (D. Müller, 2012)

minimiert die Vorbereitungszeit für Lehrkräfte. Das SpionCamp kann jedoch auch ohne ihn durchgeführt werden. Die neuen Stationen aus Kapitel 4 sollen ebenfalls in diesen Koffer integriert werden.



Abbildung 6: Spionkoffer

Die folgenden Unterthemen und Stationen sind im SpionCamp zu finden (vgl. D. Müller, 2012). Die farblich hervorgehobenen Informationskästen sind wörtlich übernommen.

Codierung



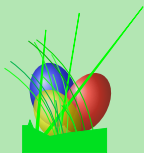
Die Buchstaben bleiben, **wo** sie sind, aber nicht, **was** sie sind. (Aber jeder kann nachschlagen, was sie bedeuten!) Man nennt so etwas einen **Code**. Mit einem Code soll nichts geheim gehalten werden.

Morsealphabet Mit dem Morsetelegraphen wurden früher Nachrichten mithilfe von kurzen und langen elektrischen Impulsen übermittelt. Die Schülerinnen und Schüler morsen sich gegenseitig Nachrichten mit einer Taschenlampe und sollen sich überlegen, wie das Morsealphabet aufgebaut ist.

Braille-Schrift Die Blindenschrift besteht aus erhöhten Punkten, die mit den Fingern ertastet werden können. Durch Stecknadeln und eine Hartschaumplatte können die Schülerinnen und Schüler Texte codieren und ertasten.

Winkeralphabet In der Seefahrt wurde das Winkeralphabet verwendet, um Nachrichten über eine kurze Distanz zu übermitteln. Mithilfe von Flaggen sollen die Schülerinnen und Schüler Nachrichten übertragen.

Steganographie



Die Buchstaben bleiben, **was** sie sind, aber man erkennt nicht, **wo** die Nachricht ist. Das ist eigentlich gar keine Verschlüsselung, man nennt das **Steganographie**. (Das Wort Steganographie ist abgeleitet von den griechischen Wörtern *steganos* = bedeckt und *graphein* = schreiben.)

Bild Nachrichten werden in Bildern versteckt, sodass sie auf den ersten Blick nicht gesehen werden. Diese Station besteht aus einem Bild, in dem eine codierte Nachricht versteckt wurde.

Text (in Entwicklung) Nachrichten können ebenfalls in Texten versteckt werden, indem sie als unverfängliche und offene Texte erscheinen oder durch kaum sichtbare graphische Details vom restlichen Text abgegrenzt werden. Die Aufgaben bestehen aus solchen versteckten Nachrichten.

Transposition



Die Buchstaben bleiben, **was** sie sind, aber nicht, **wo** sie sind. Solche Verschlüsselungen heißen **Transposition**. (Das Wort *Transposition* ist abgeleitet vom lateinischen Wort *transponere* = verschieben.)

Skytale Papierstreifen werden um einen Zylinder, genannt Skytale, mit bestimmter Dicke gewickelt und mit einer Nachricht beschrieben. Beim Abwickeln wird die Nachricht unleserlich. Die Schülerinnen und Schüler entschlüsseln gegebene Geheimtexte durch verschiedene Skytalen, schicken sich gegenseitig Nachrichten und »Knacken« eine Nachricht ohne passende Skytale.

Schablone Die Schablonen bestehen aus einem Quadrat, das in 25 gleichgroße, quadratische Felder unterteilt ist. Fünf ausgewählte Felder sind dabei ausgeschnitten. Um eine Nachricht zu verschlüsseln, legt man die Schablone auf ein leeres Papier und trägt in jedes der Felder einen Buchstaben ein. Danach wird die Schablone mehrmals gedreht und die

nächsten Buchstaben werden eingetragen. Um die Nachricht zu lesen, muss die richtige Schablone vorhanden sein. An der Station ver- und entschlüsseln die Schülerinnen und Schüler Nachrichten und entwerfen eigene Schablonen.

Pflügen Beim Verschlüsseln durch Pflügen wird eine Nachricht von oben links bis unten rechts zeilenweise in ein Rechteck mit Feldern eingetragen. Danach werden die Buchstaben von unten rechts ausgehend abwechselnd von unten und oben spaltenweise abgelesen. Um die Nachricht entschlüsseln zu können benötigt man die Länge des Rechtecks, also die Buchstabenanzahl einer Zeile. Es sollen Nachrichten ver- und entschlüsselt und ein Geheimtext »geknackt« werden.

Blocktransposition (neue Station) Wie diese Station gestaltet ist, wird in Kapitel 4.1 erläutert.

Substitution (monoalphabetisch)



Die Buchstaben bleiben, **wo** sie sind, aber nicht, **was** sie sind. Solche Verschlüsselungen heißen **Substitution**. (Das Wort *Substitution* ist abgeleitet vom lateinischen Wort *substituere* = ersetzen.)

Freimaurer Der Geheimbund der Freimaurer verwendete eine Verschlüsselung, in der die Buchstaben des Alphabets in einer beliebigen Reihenfolge in ein Muster eingetragen werden. Zum Verschlüsseln einer Nachricht werden die Buchstaben durch die Linien und Punkte ersetzt, die ihn im Muster umgeben. An dieser Station ver- und entschlüsseln die Schülerinnen und Schüler Nachrichten durch ein Muster mit festgelegter Reihenfolge. Außerdem überlegen sie, wie man eine Nachricht ohne Schlüssel entziffern kann.

Caesar Caesar verschlüsselte seine Nachrichten, indem er das Alphabet um drei Stellen verschob. Aber auch andere Schlüssel, also Anzahl von Stellen, um die verschoben wird, sind möglich. Die Caesar-Chiffre kann mit einem Schlüsselwort kombiniert werden, indem dieses ohne doppelte Buchstaben unter das normale Alphabet geschrieben wird und alle übrigen Buchstaben in Alphabetreihenfolge angehängt werden. Die Schülerinnen und Schüler benutzen eine Chiffrierscheibe, um Nachrichten

zu ver- und entschlüsseln und überlegen, wie die Verschlüsselung »geknackt« werden kann.

Substitution (bigraphisch)



Die Buchstaben bleiben, **wo** sie sind, aber nicht, **was** sie sind. Es werden nicht einzelne Buchstaben, sondern Buchstaben**paare** verschlüsselt. Solche Verschlüsselungen heißen **bigraphische Substitution**. (Das Wort *Substitution* ist abgeleitet vom lateinischen Wort *substituere* = ersetzen. *Bi* heißt *zwei* und *graphisch* kommt vom griechischen *graphein* = schreiben.)

Playfair Bei dieser Verschlüsselung wird ein Schlüsselwort in ein Quadrat mit 25 gleichgroßen, quadratischen Feldern zeilenweise ohne doppelte Buchstaben eingetragen. Danach werden alle übrigen Buchstaben in die weiteren Felder geschrieben, wobei *i* und *j* in ein Feld gehören. Nun werden die Buchstaben der Nachricht in Zweiergruppen eingeteilt, wobei Paare mit zwei gleichen Buchstaben durch ein eingeschobenes *x* getrennt werden. Die Paare werden gemeinsam verschlüsselt, indem sie im Quadrat ihre Spalten, aber nicht die Zeilen tauschen beziehungsweise durch ihre rechten bzw. unteren Nachfolger ersetzt werden, wenn sie in der gleichen Zeile bzw. Spalte stehen. Diese Station ist als schwierig eingestuft und die Schülerinnen und Schüler sollen verschiedene Nachrichten ver- und entschlüsseln.

Substitution (polyalphabetisch)



Die Buchstaben bleiben, **wo** sie sind, aber nicht, **was** sie sind. **Was** sie sind, ist immer wieder verschieden. Solche Verschlüsselungen heißen **polyalphabetische Substitution**. (Das Wort *Substitution* ist abgeleitet vom lateinischen Wort *substituere* = ersetzen. *Poly* heißt *viel*.)

Rotoren Die Rotor-Maschine Enigma wurde im Zweiten Weltkrieg verwendet um Nachrichten mithilfe von mehreren drehbaren Scheiben zu ver- und entschlüsseln. Dabei wurden die Rotoren nach jedem Buchstaben verschoben. Die Schülerinnen und Schüler üben dies mit einem Rotor und überlegen, wie man einen Geheimtext »knacken« könnte. Diese Station ist ebenfalls als schwer eingestuft.

Vigenère Dieses Verfahren verwendet das Vigenère-Quadrat, das aus allen möglichen verschobenen Alphabeten besteht, die untereinander geschrieben sind. Um eine Nachricht zu verschlüsseln, schreibt man ein Schlüsselwort mehrmals unter die Nachricht und ersetzt den Buchstaben des Klartextes mit dem Buchstaben im Vigenère-Quadrat, der in der Spalte des Klartextbuchstaben und der Zeile des Schlüsselbuchstaben liegt. Dies üben die Schülerinnen und Schüler mit vorgegebenen Schlüsselwörtern.

Autokey (neue Station) Funktion und Aufbau der Station wird in Kapitel 4.2 erläutert.

Kryptoanalyse (in Entwicklung)



Bei der **Kryptoanalyse** wird versucht, durch Eigenschaften des Geheimtextes den Schlüssel oder den Klartext herauszufinden.

Um einen Geheimtext, der durch eine monoalphabetische Substitution entstanden ist, ohne bekannten Schlüssel zu entschlüsseln, verwendet man die **Häufigkeitsanalyse**.

Buchstabenhäufigkeit (in Entwicklung) Die Buchstabenhäufigkeit wird benutzt, um Geheimtexte zu entschlüsseln. Die Schülerinnen und Schüler vergleichen die Häufigkeiten der einzelnen Buchstaben in einem Geheimtext mit den realen Häufigkeiten der deutschen Sprache. Außerdem nutzen sie Muster und Eigenschaften deutscher Wörter, um den Geheimtext zu »knacken«.

Schlüsselaustausch



Um einen Klartext zu verschlüsseln und auch anschließend zu entschlüsseln, brauchen Sender und Empfänger denselben Schlüssel. Dieser ist meist eine Zahl. Sender und Empfänger müssen den Schlüssel **geheim** austauschen können, das heißt, ohne dass ein Dritter ihn erfährt.

Modulo-Rechnung Modulo ist eine Rechenoperation, die u. a. für den Diffie-Hellman-Algorithmus benötigt wird. Sie entspricht dem Rest der ganzzahligen Division. Die Schülerinnen und Schüler sollen verschiedene Modulo-Aufgaben berechnen.

Diffie-Hellman-Algorithmus Um einen Schlüssel über eine unsichere Verbindung auszutauschen, verwendet man den Diffie-Hellman-Algorithmus. Dafür setzt man eine Primzahl und eine natürliche Zahl fest und jeder der beteiligten Personen wählt eine Geheimzahl, die kleiner ist, als die Primzahl. Mittels Potenzieren und der Modulo-Rechnung wird jeweils eine Zahl berechnet, die über die unsichere Verbindung ausgetauscht werden kann. Durch die erhaltene Zahl wird mittels Potenzieren und der Modulo-Rechnung der Schlüssel berechnet. Diesen kennen nur die Personen, die ihre Geheimzahl wissen. Die Schülerinnen und Schüler spielen diesen Algorithmus zu dritt mehrmals nach. Diese Station ist ebenfalls sehr schwierig.

3.3 Weiteres Material der Bergischen Universität Wuppertal

Das Vorbereiten von gutem Unterrichtsmaterial ist in allen Fächern mühsam. Äußerst auffällig ist dies beim Informatikunterricht, da das Fach noch nicht komplett ausgebaut ist. Noch wird Informatik nicht an jeder Schule angeboten und es gibt nur wenige Schulbücher, die zurate gezogen werden können. Deswegen hat die Fachgruppe Mathematik und Informatik der Bergischen Universität Wuppertal Material zusammengestellt, das für den Unterricht frei nutzbar ist. Das SpionCamp ist eines von ihnen und wurde – wie bereits oben erwähnt – durch das MathePrisma inspiriert. Außerdem wurde es als Grundlage für das Modul *Ich habe ein Geheimnis!* verwendet und wird an mehreren Stellen der Materialsammlung als Grundlage bzw. Wiederholung genannt.

3.3.1 MathePrisma

Das MathePrisma wurde 1999 als gemeinsames interaktives Multimedia-Projekt der Arbeitsgruppen Didaktik und Angewandte Informatik im Fachbereich C / Mathematik der Bergischen Universität Wuppertal ins Leben gerufen. Es enthält verschiedene Module zu mathematischen und informatischen Fragestellungen, anhand derer Methoden vorgestellt und angewandt werden können. Die Module sind dabei unterschiedlich schwierig, richten sich jedoch in erster Linie an Schülerinnen und Schüler ab der Jahrgangsstufe elf. Sie sollen die Faszination, Nützlichkeit und Attraktivität der Fächer entdecken. Dafür sind interaktive Elemente integriert, die eine spielerische und lockerere Lernatmosphäre schaffen. Dazu gehören intuitive Einstiege zur Problemerkennung und Entwicklung von Lösungsstrategien, Fragen zur Steuerung der Lernprozesse, individuelle Lösungswege sowie Lernzielkontrollen. Visualisierungen sind durch Filme, Bildfolgen und Animationen geschaffen. Die Module eignen sich durch ausführliche Lösungswege und Selbst-

überprüfungen zum Selbststudium, können jedoch auch durch Lehrkräfte betreut werden. Sie können sogar offline genutzt werden, um minimale Ressourcen vorauszusetzen (vgl. Fachbereich C / Mathematik der Bergischen Universität Wuppertal, 2001).

Folgende Zielsetzungen sind als Hintergründe für das MathePrisma angegeben (vgl. ebd.):

- Erfahren und Begreifen von Mathematik
- Probleme lösen / Spielen mit dem Problem
- Entwicklung und Vergleich von Lösungsstrategien
- problemorientierte mathematische Aufbereitung und Begriffsbildung
- Unabhängigkeit von Lehrplänen
- unterhaltsame Blicke über den mathematischen Tellerrand hinaus
- freie Verfügbarkeit
- Vorstellung mathematischer Werkzeuge und deren konkrete Anwendung

Für den kryptologischen Bereich gibt es Module zu der Caesar-Chiffre, dem DES-Algorithmus (Data Encryption Standard, wird in Kapitel 4.1 skizziert), der Enigma und der RSA-Verschlüsselung (RIVEST, SHAMIR, ADLEMAN). Das Modul zur Caesar-Chiffre war ausschlaggebend für die Inspiration zur Entwicklung des SpionCamps. Es wird außerdem zurzeit als Vorbild für eine Erweiterung des Moduls *Ich habe ein Geheimnis!* genutzt.

Das MathePrisma gewann bereits mehrere Auszeichnungen. Im Jahr 2001 wurden es von einer Jury zum Gewinner des Mediendidaktischen Hochschulpreises (MEDIDA-PRIX) gekürt (Gesellschaft für Medien in der Wissenschaft, 2001). Bei der Europäischen Fachtagung *Virtueller Campus* (Universität Hildesheim, 2001) der *Gesellschaft für Medien in der Wissenschaft* vom 19. bis 21. September 2001, bei der auch die Verleihung des MEDIDA-PRIX 2001 stattfand, wurde es zusätzlich mit dem Publikumspreis ausgezeichnet. Die Posterserie zum MathePrisma (Frommer, Krivsky und Zöllner, 2000) gewann beim Wettbewerb der *European Mathematical Society* den zweiten Preis (International Mathematical Union, 2000).

Die MathePrisma-Module und Modulelemente dürfen privat und in Bildungseinrichtungen frei genutzt werden, solange die Hinweise auf die Autoren, die Bergische Universität Wuppertal und das MathePrisma nicht entfernt werden. Für eine kommerzielle Nutzung wird eine schriftliche Zustimmung benötigt (vgl. Fachbereich C / Mathematik der Bergischen Universität Wuppertal, 2001).

3.3.2 Ich habe ein Geheimnis!

Wie bereits in Kapitel 2.1 analysiert, sollte die Informatik und insbesondere die Kryptologie bereits in der Grundschule gelehrt werden. Dafür rief das MSB-NW das 2019 abgeschlossene Projekt *Informatik an Grundschulen* (MSW-NW, 2016) ins Leben. Das Ziel dieses Projektes war es, „den Schülerinnen und Schülern der dritten und vierten Klassen Facetten der Informatik begreifbar zu machen, und sie so zu unterstützen, ein Verständnis für Informatiksysteme und die Bedeutung von Informatik im Alltag zu entwickeln“ (ebd.). Dafür stellten drei Standorte in Zusammenarbeit mit den dortigen Hochschulen und ausgewählten Grundschulen jeweils ein Modul für den Sachunterricht ohne den Einsatz von Informatiksystemen zusammen. Eine Erweiterung der Module um Informatiksysteme ist zurzeit in Arbeit. Jedes der drei Module durchschritzt die folgenden Phasen (vgl. ebd., Hervorh. im Orig.):

Phase 1 Die Unterrichtsmaterialien werden gemeinsam mit Grundschullehrkräften entwickelt. Mit den Materialien sensibilisieren sie die Schülerinnen und Schüler für informatische Aspekte aus der Erfahrungs- und Lebenswelt und greifen Vorkenntnisse auf. Die Ausgestaltung verfolgt dabei das Prinzip des *entdeckenden Lernens*, indem *kreative Gestaltungselemente* und *problemorientierte Lernsettings* verwendet werden, um das Konzept über die enaktive Ebene erfahrbar zu machen.

Phase 2 Die mitarbeitenden Lehrkräfte an den Pilotgrundschulen erproben und evaluieren die Materialien im Sachunterricht. Dabei sollte die Passung zur Zielgruppe und insbesondere zu den Eingangsvoraussetzungen der Schülerinnen und Schüler eruiert und die Modulmaterialien iterativ verbessert werden. Außerdem tauschen die drei Standorte die Materialien aus und entwickeln sie durch gegenseitiges Feedback weiter.

Phase 3 An weiteren Korrespondenzschulen werden Sachunterrichtslehrkräfte auf die Umsetzung der Module in ihrem Unterricht vorbereitet. Dazu werden für jedes Modul Veranstaltungen zur Schulung der Lehrkräfte geplant und durchgeführt.

Phase 4 Die vorbereitenden Veranstaltungen werden mit je zwei Grundschullehrkräften aus mehreren Korrespondenzschulen von den Universitäten mit Unterstützung der mitwirkenden Grundschullehrkräfte durchgeführt.

Phase 5 Die neu vorbereiteten Lehrkräfte setzen die Module in ihrem eigenen Unterricht um. Die Mitarbeiterinnen und Mitarbeiter der Universitäten stehen den teilnehmenden Lehrkräften der Korrespondenzschulen auch im weiteren Verlauf des Projekts als Ansprechpartner zur Verfügung.

Durch diese Phasierung entwickelte die Rheinisch-Westfälische Technische Hochschule Aachen das Modul *Digitale Welt* (Schülerlabor Informatik – InfoSphere, 2016) mit drei Doppelstunden zu Datenübertragung, Binärdarstellung und Fehlererkennung. Die Universität Paderborn realisierte *Wie funktioniert ein Roboter?* (Didaktik der Informatik an der Universität Paderborn, 2019), in dem erste Schritte der Programmierung erläutert und ausprobiert werden. Das dritte Modul der Bergischen Universität Wuppertal *Ich habe ein Geheimnis!* (Didaktik der Informatik an der Bergischen Universität Wuppertal, 2019) beschäftigt sich mit Kryptologie und wird nun detaillierter beschrieben.

Einige der Stationen des SpionCamps wurden als Grundlage für das Modul der Bergischen Universität Wuppertal genutzt. Das Modul bezieht sich ebenfalls auf historische kryptographische Verfahren der Codierung, der Transposition und Substitution. Allerdings wird hier die Freimaurer-Chiffre als Codierung bezeichnet. Dies ist damit begründet, dass jede monoalphabetische Substitution als eine Codierung angesehen werden kann, die aber immer individuell festgelegt wird (vgl. Humbert u. a., 2019, S. KR 11). Den Schülerinnen und Schülern wird die Freimaurer-Chiffre also als Codierung vorgestellt, bei der das Alphabet in einer festen Reihenfolge in das Muster eingetragen ist. Durch diese feste Reihenfolge kann jeder nachschlagen, was die Nachricht bedeutet.

Das Kryptologie-Modul beinhaltet Material für zehn Schulstunden und eine optionale Zusatzstunde. Die Schülerinnen und Schüler lernen mit den beiden Identifikationsfiguren der Kryptologie *Alice* und *Bob*, die sich Daten übermitteln, sowie der Angreiferin *Eve* die folgenden Unterthemen der Kryptologie kennen (ebd., S. KR 02, Hervorh. im Orig.):

Beispielhafter Einstieg – Informatik in der Lebenswirklichkeit Die Schülerinnen und Schüler besuchen einen nahe gelegenen Supermarkt und setzen die Informatikbrille auf – Welche informatischen Phänomene finden sich an diesem Lernort? Alternativ wird der Supermarkt mit Bildkarten besprochen.

Anschließend überlegen und verschriftlichen die Schülerinnen und Schüler, was sie mit dem Wortfeld Informatik assoziieren.

Steganographie Die Schülerinnen und Schüler finden verborgene Nachrichten und tauschen sich über den Grad der Sicherheit aus. Wenn alle Verstecke gefunden oder bekannt sind, ist die Steganographie wirkungslos.

Codierung Die Schülerinnen und Schüler nutzen z. B. die Freimaurer-Chiffre, indem sie mit einer Codetabelle selber codieren und decodieren. Eve als Angreiferin greift schnell die Nachricht ab, da sie auch die Codetabelle kennt – eine Verbesserung muss her.

Transposition Papierstreifen werden auf Holzstäbe gewickelt: die Skytale ist erfunden!

Die Schülerinnen und Schüler lernen Fachbegriffe wie *Algorithmus* und *Schlüssel* und werden selbst zum Angreifer auf die Nachrichten.

Substitution Mit Code-Scheibe und -Tabelle verschlüsseln die Schülerinnen und Schüler wie Caesar im alten Rom. Der Angreifer hat immer mehr Mühe, den Algorithmus zu knacken. Bei einigen Verfahren ist aber auch der Schlüsseltausch unter den Eingeweihten umständlich.

Verschlüsselung im Alltag Zurück zum Anfang: Wo begegnen uns die nun bekannten kryptologischen Phänomene im Alltag? Die Schülerinnen und Schüler diskutieren Angriffsszenarien auf Messenger und Co.

Bei der Bearbeitung dieser Unterthemen werden die folgenden Kompetenzen erworben (Humbert u. a., 2019, S. KR 07, Hervorh. im Orig.):

Kompetenzen zur Informatik in der Lebenswirklichkeit

Die Schülerinnen und Schüler ...

- beschreiben ihren persönlichen Umgang mit Informatiksystemen.
- beschreiben ihren persönlichen Umgang mit Diensten des Internets.
- beschreiben Analogien und Unterschiede zwischen der realen und der digitalen Welt.

Kompetenzen zur Kryptologie

Die Schülerinnen und Schüler ...

- charakterisieren den Begriff *Algorithmus*.
- erläutern gegebene Algorithmen.
- führen Algorithmen schrittweise aus.
- kennen ein Verfahren zur Transposition.
- analysieren den Algorithmus zur Verschlüsselung von Nachrichten (Daten).
- entwerfen einen Algorithmus zur Verschlüsselung von Nachrichten (Daten).
- »knacken« verschlüsselte Nachrichten mithilfe eines bekannten Verfahrens.
- erarbeiten eine Methode zur systematischen Entschlüsselung von verschlüsselten Nachrichten (Daten) und wenden diese an.

Mit dieser Aufteilung und diesen Kompetenzen wurden die Anforderungen der Bildungsstandards für den Primarbereich erfüllt. Es gibt eine klare Trennung der Begriffe *Verschlüsselung* und *Codierung* und es wurden historische kryptographische Verfahren genutzt, um den Schülerinnen und Schülern die Bandbreite der Kryptographie zu zeigen. Sie „knacken“ sogar verschlüsselte Nachrichten, wodurch zusätzlich die Kryptoanalyse angesprochen wird. Allerdings entwickeln sie keine eigenen Vereinbarungen für die Verschlüsselung und die Übermittlung von Daten, obwohl dies Kompetenzen im Inhaltsbereich *Information und Daten* sind, die zur Kryptologie gezählt werden können (siehe Tabelle 1 auf Seite 9).

3.3.3 Materialsammlung

Die Referendarinnen und Referendare der Informatikfachseminare Hamm und Arnsberg erstellten bei der Vorbereitung des bedarfsdeckenden Unterrichts Materialien für den Informatikunterricht. Diese Materialien wurden zusammen mit Lehrenden, Studierenden sowie Ehemaligen der Didaktik der Informatik an der Bergischen Universität Wuppertal und der Universität Dortmund aufgearbeitet sowie zusammengestellt. Bei den Materialien handelt es sich um Arbeitsblätter, Lernzielkontrollen, Kursarbeiten, Klausuren und Unterrichtsentwürfe, die nach Themen sortiert wurden. Sie liegen sowohl als PDF-Dateien als auch als LaTeX-Code vor, damit sie nicht nur einfach genutzt, sondern auch fortlaufend angepasst werden können. Sie unterliegen deswegen der LicenseCreative Commons by-nc-sa-Lizenz in der Version 4.0 und dürfen verändert sowie nicht kommerziell weiter verbreitet werden, solange die Autoren genannt werden (Pieper und D. Müller, 2013).

Die Materialien sind Themengebieten der Sekundarstufe I und II untergeordnet und für beide Schulstufen gibt es Material zur Kryptologie. Insgesamt gibt es für die Kryptologie Materialien zu den Unterthemen Verschlüsselungsverfahren, Codierungen, Kryptoanalyse, Signatur und zum Schlüsselaustausch. In der Sekundarstufe I wird die Codierung von der Kryptologie abgegrenzt und auf eine Sammlung von Informatiktricks (D. Müller, 2013) verwiesen, die zeigen, „wie aus einer geschickte[n] Kodierung ein Zaubertrick entstehen kann“ (Pieper und D. Müller, 2013). Für beide Stufen ist das SpionCamp als Empfehlung für die weitere Vertiefung bzw. als Wiederholung angegeben. Ein Modul zur Kryptologie für die Erprobungsstufe wird im Rahmen einer Masterarbeit zurzeit entwickelt und soll in die Materialsammlung integriert werden (Schmid, 2019).

4 Die neuen Stationen

Durch die Analyse der Bildungsdokumente wird ersichtlich, dass schwierigere Stationen das SpionCamp für die Sekundarstufe II relevanter machen würde. Diese sollten sich nahtlos an die bereits vorhandenen Stationen anpassen, um eine Bearbeitung als Stationenlernen nicht auszuschließen. Die zwei in diesem Kapitel erläuterten Verfahren erfüllen diese Anforderung und lassen sich gut als Stationen realisieren. Dabei wird jeweils nur ein Beispielfahrer der Block- und Stromverschlüsselungen in den Stationen erläutert, da sie einen Einblick in eine größere Menge von Verfahren darstellen. Die Block- und die Stromverschlüsselungen sind sehr gegenwartsrelevant, da sie die einzigen symmetrischen Verschlüsselungen sind, die zurzeit noch verwendet und teilweise auch in asymmetrischen sowie hybriden Verschlüsselungsverfahren angewandt werden. Die Relevanz der Verfahren wird auch anhand des folgenden Zitats deutlich.

Alle gängigen symmetrischen Verschlüsselungsverfahren gehören entweder zu den Block- oder zu den Stromchiffren.

Klaus Schmeh, 2013, S. 282

4.1 Blockchiffren

Der Begriff *Blockverschlüsselung* oder *Blockchiffre* bezeichnet eigentlich eine Oberkategorie von verschiedenen symmetrischen Verschlüsselungsverfahren, bei denen Klartexte in Blöcke einer festen Länge eingeteilt werden. Diese Verfahren stellen beispielsweise verschiedene Betriebsmodi des DES-Algorithmus (Data Encryption Standard) dar, der heutzutage in abgewandelter Form noch häufig verwendet wird. Auch Verschlüsselungsverfahren der Vergangenheit, wie etwa die Vigenère-Verschlüsselung, teilten die Klartexte in Blöcke. Diese Verbindung zwischen vergangenen und bestehenden Verschlüsselungsverfahren war einer der Gründe für die Realisierung einer Station zur Blockverschlüsselung. Außerdem wird ein weiterer sehr wichtiger Gegenstand der Informatik verwendet, der in jeder Transposition vorkommt. Es handelt sich dabei um Permutationen, die nicht nur in der Informatik sondern auch in der Mathematik eine wichtige Rolle spielen. Permutationen werden in der Schulmathematik im Themenfeld Kombinatorik (Wahrscheinlichkeitstheorie) benötigt und können leicht durch Beispiele erläutert werden. Diese Verknüpfung zur Mathematik und den anderen Transpositionsverfahren ist der zweite Grund für die Realisierung als Station. Der dritte Grund ist die enaktive Arbeit der Schülerinnen und Schüler in den Stationen des SpionCamps. Bei fast allen komplexeren Verschlüsselungsverfahren wird viel gerechnet, was für die meisten Schülerinnen und Schüler keinen großen Anreiz bietet. Deswegen wurde zu dieser Station Material ausgearbeitet, dass die

Permutation veranschaulicht. Die Schülerinnen und Schüler folgen Pfeilen, um die neuen Plätze der Buchstaben zu erfahren und können deswegen auch ohne mathematische Neugier das Prinzip verstehen.

4.1.1 Theoretische Grundlagen

Bei einer Blockverschlüsselung wird der Klartext, der aus Zeichen eines Alphabetes Σ besteht, in Blöcke einer bestimmten Länge eingeteilt. Diese Blocklänge n muss eine natürliche Zahl sein. Ist der Klartext zu kurz, wird er ergänzt, bis seine Länge durch n teilbar ist. Somit liegen die einzelnen Blöcke in der Menge Σ^n , also in den Wörtern der Länge n . Wörter beschreiben hierbei keine lesbaren Wörter, sondern Anordnungen von Zeichen aus dem Alphabet. Die Blöcke werden mithilfe von Permutationen verschlüsselt (vgl. Buchmann, 2010, S. 68).

Definition 4.1.1: Permutation (ebd., S. 66)

Sei X eine Menge. Eine Permutation von X ist eine bijektive Abbildung $f : X \rightarrow X$.

Die Menge aller Permutationen von X wird mit $S(X)$ bezeichnet.

Die Zeichen der Klartextblöcke werden also durch Permutationen vertauscht. Eine Permutation kann in der Zweizeilenform notiert werden, die von allen Notationen am verständlichsten ist. Bei dieser handelt es sich um eine Matrix mit zwei Zeilen und n Spalten, bei der die neuen Positionen der Zeichen unter den alten Positionen stehen.

Beispiel 4.1.2:

Sei $X = \{0, 1, 2, 3, 4\}$ und π eine Permutation aus $S(X)$, die jedes Zeichen um eine Stelle nach rechts verschiebt, dann ist

$$\pi = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \end{pmatrix}.$$

Aus dem Klartext **SPION** wird somit der Geheimtext **NSPIO**, da der Buchstabe an fünfter Stelle an die erste Stelle geschrieben wird und alle anderen Buchstaben eine Stelle aufrutschen.

Fixiert man die Blocklänge n sowie das Alphabet Σ und verwendet Σ^n als Klartext- und Geheimtextraum $\mathcal{P} = \mathcal{C} = \Sigma^n$ ist die Verschlüsselungsfunktion einer Blockchiffre definiert als

$$E_\pi : \Sigma^n \rightarrow \Sigma^n, v \mapsto \pi(v).$$

Die Entschlüsselungsfunktion ist

$$D_\pi : \Sigma^n \rightarrow \Sigma^n, v \mapsto \pi^{-1}(v).$$

Die Permutation wird bei der Entschlüsselungsfunktion umgekehrt angewendet, dabei wird die Zweizeilenform von unten nach oben gelesen. Der Schlüssel entspricht der Permutation, wodurch $n!$ viele Schlüssel für die Blocklänge n existieren (vgl. Buchmann, 2010, S. 68).

Blockchiffren werden beispielsweise im sehr bekannten DES-Algorithmus verwendet, der als eine Anpassung der Lucifer-Chiffre gilt und im Jahr 1977 als offizieller amerikanischer Verschlüsselungsstandard ausgezeichnet wurde (vgl. F. L. Bauer, 1997, S. 168). Die kurze Schlüssellänge des DES-Algorithmus stellt jedoch ein Problem dar, weswegen heutzutage häufig Erweiterungen des DES-Algorithmus, wie beispielsweise der Doppel-DES oder der Triple-DES, genutzt werden (vgl. Schmech, 2013, S. 89-91). Wir betrachten hier dennoch den normalen DES-Algorithmus, da dieser den Nutzen der Blockchiffre bereits aufzeigt und immer noch angewandt wird.

Beim einfachen DES-Algorithmus wird der Klartext, der in Binärdarstellung vorliegt, in 8-Byte-Klartextblöcke unterteilt und durch eine „Folge von festen Transpositionen und von schlüsselabhängigen, multipartiten, nichtlinearen Substitutionen“ (F. L. Bauer, 1997, S. 168) verschlüsselt. Der genaue Ablauf des DES-Algorithmus wird hier nur skizziert und kann in zahlreichen Werken nachgelesen werden (beispielsweise in Schmech, 2013, S. 81-92). Die Abfolge der Chiffrierschritte ist in Abbildung 7 auf Seite 38 abgebildet. Zunächst wird jeder der 8-Byte-Block einer Eingangspermutation π unterworfen. Danach wird er in zwei 4-Byte-Blöcke L_0 und R_0 unterteilt. Nun werden 16 mal die folgenden Schritte ausgeführt

$$L_i = R_{i-1} \text{ und } R_i = L_i \oplus f(R_{i-1}, K_i) \text{ für } i = 1, \dots, 16. \quad (1)$$

Dies bedeutet, dass wir unsere R_i in L_i speichern und beide auf bestimmte Weise verknüpfen, um die nächsten Blöcke R_i zu erhalten. K_i ist dabei ein 48-Bit-Schlüssel, der durch eine Auswahlfunktion aus dem vorgegebenen Schlüssel des Benutzers erzeugt wird. Die Auswahlfunktion entfernt die Paritätsbits (Sicherheitsbits), sortiert die verbleibenden 56 Bits nach einer festen Permutation um und unterteilt sie in 28-Bit-Blöcke. Diese Blöcke werden bei jeder Ausführung der in Gleichung 1 beschriebenen Schritte zyklisch nach links gedreht und durch ein vorgegebenes Verfahren in 48-Bit Teilschlüssel K_i eingeteilt. Dann werden bestimmte Bitstellen von R_i dupliziert und R_i wird mit K_i addiert und

modulo 2 gerechnet. Dies entspricht ebenfalls der Exklusiven-Oder-Verknüpfung, die als $\oplus$ dargestellt ist. Die Funktion f teilt das Ergebnis dieser Addition in acht 6-Bit-Gruppen und verwendet jeweils einen von acht Substitutionsboxen, die jeweils vier verschiedene nichtlineare Substitutionen realisieren. Diese Substitutionsboxen werden hier nicht weiter erläutert. Aus den acht Substitutionsboxen werden nachher acht 4-Bit-Ausgabeblocke erzeugt, die hintereinandergeschrieben und einer festen Permutation unterworfen werden. Aus den beiden 48-Bit Blöcken ist somit ein 32-Bit-Ausgabeblock entstanden. Dieser wird dann zum Schluss mit L_i durch $\oplus$ verknüpft, was wieder der Addition *modulo 2* oder der Exklusiven-Oder-Verknüpfung entspricht.

Nach 16 Durchgängen werden L_{16} und R_{16} aneinandergelassen und durch die inverse Permutation π^{-1} umgestellt. Die Ausgabe ist somit wieder ein 8-Byte-Klartextblock (vgl. F. L. Bauer, 1997, S. 168-169).

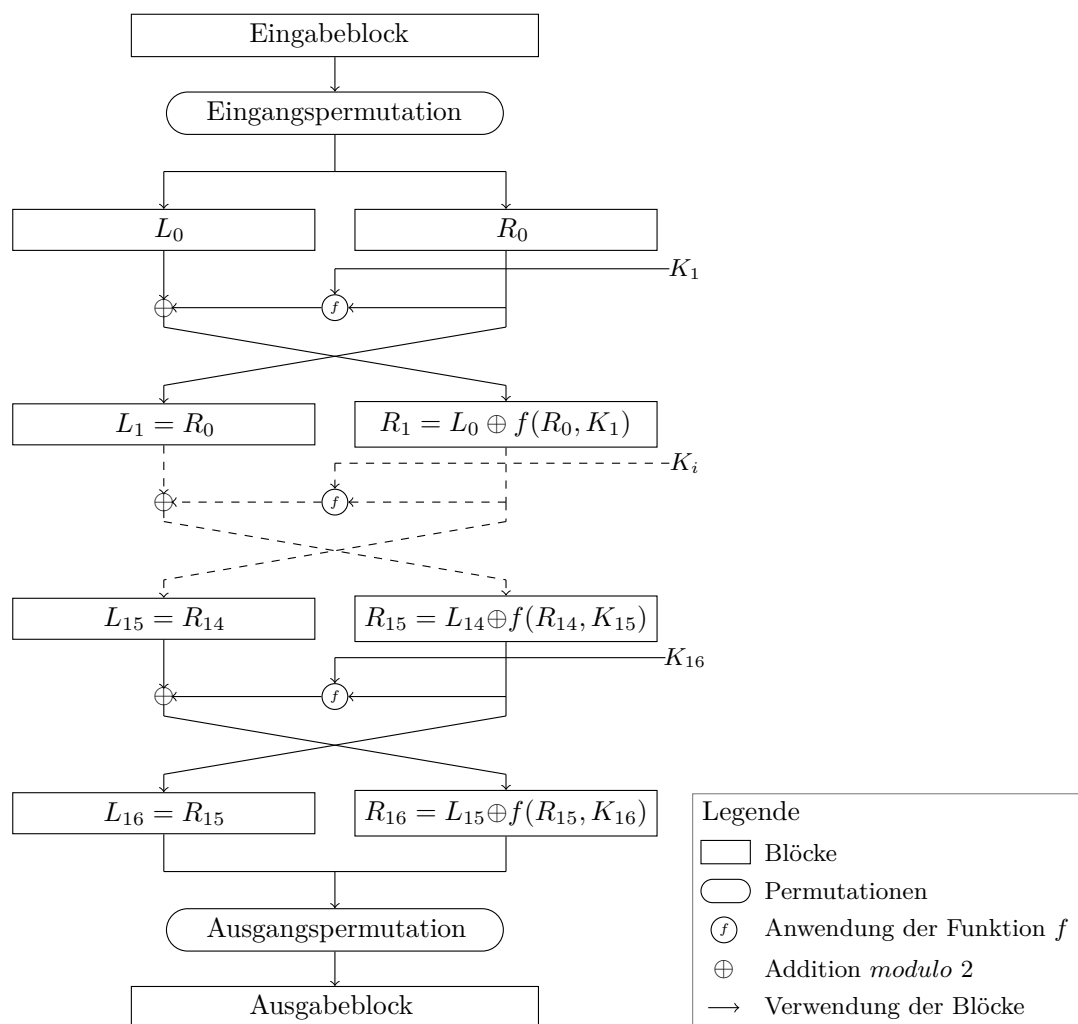


Abbildung 7: DES-Chiffrierschritte (nach F. L. Bauer, 1997, S. 169)

Der DES-Algorithmus besitzt verschiedene Betriebsmodi, „die sich in bezug [sic] auf die Chiffriergeschwindigkeit und Fehlerfortpflanzung wesentlich unterscheiden“ (F. L. Bauer, 1997, S. 171). Diese Betriebsmodi können auch für andere Verfahren eingesetzt werden, weswegen wir von einer allgemeinen Blocklänge n anstelle der im DES-Algorithmus festgelegten Blocklänge von 8-Byte und einer unbestimmten Verschlüsselung sprechen (vgl. J. Müller, 2018, S. 8-12):

Electronic Code Book Mode Beim ECB-Modus werden beliebig lange Texte in Blöcke der Länge n unterteilt. Die einzelnen Blöcke werden dann unabhängig voneinander unter Verwendung eines festen Schlüssels verschlüsselt. Der Geheimtext entspricht dann der Folge von Geheimtextblöcken. Die Entschlüsselung erfolgt analog für jeden einzelnen Block. Bei diesem Modus werden gleiche Klartextblöcke in gleiche Geheimtextblöcke verschlüsselt.

Cipher Block Chaining Mode Im CBC-Modus hängt die Verschlüsselung eines Klartextblockes zusätzlich von den vorhergegangenen Blöcken ab, wodurch sie kontextabhängig werden. Dadurch werden gleiche Klartextblöcke unterschiedlich verschlüsselt. Die Abhängigkeit der Blöcke wird durch die Verknüpfung der Addition *modulo 2* realisiert, indem die Klartextblöcke zuerst mit dem vorherigen Geheimtextblock verknüpft und danach verschlüsselt werden. Der erste Block wird dabei mithilfe eines Initialisierungsblockes verschlüsselt.

Output Feedback Mode Der OFB-Modus unterteilt den Klartext zuerst in Blöcke der Länge r mit $1 \leq r \leq n$. Der Initialisierungs- bzw. Schlüsselblock mit der Länge n wird zuerst verschlüsselt und dann werden seine ersten r Stellen mit dem Klartextblock verknüpft. Bei der Verknüpfung handelt es sich wieder um die Addition *modulo 2*. Die jeweils folgenden Klartextblöcke werden mit einem Schlüsselblock, der dem vorherigen bereits verschlüsselten Schlüsselblock entspricht, verknüpft.

Cipher Feedback Mode Der CFB-Modus ähnelt dem OFB-Modus stark, nur dass die Schlüsselblöcke anders gebildet werden. Der erste Schlüsselblock entspricht wieder dem Initialisierungsblock. Die darauf folgenden Schlüsselblöcke entstehen dadurch, dass die ersten r Stellen des letzten Schlüsselblockes gelöscht und mit dem letzten Geheimtextblock addiert werden.

4.1.2 Didaktische Analyse

Die Blockchiffren sind ein wichtiger Teil der modernen Kryptologie und werden an vielen Stellen als symmetrische Verschlüsselungen oder als Teil von hybriden Verschlüsselun-

gen verwendet. Das SpionCamp beinhaltet bereits eine Station, die ebenfalls als Blockverschlüsselung angesehen werden kann. Bei der Vigenère-Substitution wird der Klartext auch in Blöcke eingeteilt, die jeweils mit einem Schlüsselwort verschlüsselt werden. Bei dieser Verschlüsselung handelt es sich jedoch um eine Substitution. Dies lässt den wichtigen Aspekt der Transposition, die beispielsweise im DES-Algorithmus verwendet wird, außen vor.

Die neue Station arbeitet wie eine Blockchiffre, nur ohne Binärdarstellung der einzelnen Buchstaben. Die Binärdarstellung miteinzubeziehen, würde die Station unnötig kompliziert und ihre Bearbeitung zeitaufwendig machen, was bei einem Stationenlernen nicht gewünscht ist. Als Betriebsmodus wird der einfache jedoch nicht ganz so sichere ECB-Modus gewählt, da die anderen Modi die Bearbeitung der Station ebenfalls zu zeitaufwendig und kompliziert machen würden. Durch diese Festlegungen handelt es sich bei der Blockverschlüsselung um eine einfache Permutationsverschlüsselung, bei der die Buchstaben durch eine Permutation vertauscht werden. Diese Permutationsverschlüsselung gehört aufgrund der Verwendung von Buchstaben nicht zu den modernen, sondern zu den klassischen Verschlüsselungsverfahren. Teilweise wird diese Art der Permutationsverschlüsselung auch *Blocktransposition* (F. L. Bauer, 1997, S. 97) oder *Zeilentransposition* (Schmeh, 2013, 52 f.) genannt. Diese Blockverschlüsselung entspricht einer Transposition, die von Schülerinnen und Schülern verstanden werden kann und im folgenden Unterricht eine Grundlage für den DES-Algorithmus bildet.

Im Weiteren wird die neue Station zur Blockverschlüsselung fokussiert betrachtet. Der Aufbau der Arbeitsmaterialien (Stationsblatt, Arbeitsblatt, Lösungsblatt und Materialien) entspricht den anderen Stationen des SpionCamps. Dies beinhaltet den Stil der Blätter (Textart, Blöcke, Farben usw.), das Logo des SpionCamps, das Logo der Bergischen Universität Wuppertal sowie die Lizenz und Versionskennzeichnung. Diese Elemente sind vom SpionCamp ohne Anpassungen übernommen. Ebenso sind der Untertitel *Transposition* und der Informationstext bereits durch die anderen Stationen der Transposition festgelegt und bleiben deswegen unverändert. Der Aufbau der Blätter ist so nah wie möglich am Aufbau der bisherigen Stationen gehalten und wird im Folgenden erläutert.

Der Titel *Blocktransposition* wurde nach der Erprobung im Unterricht aus Kapitel 5 angepasst, damit die Chance besteht, weitere Blockchiffren im SpionCamp zu realisieren. Der vorherige Titel *Block-Chiffre* hätte diese Möglichkeit nicht zugelassen. Der neue Titel entspricht der Definition von F. L. BAUER. Dieser Titel doppelt sich zwar mit dem Untertitel der Station (*Transposition*), vereint jedoch den Aspekt der moderneren Blockchiffre und den Aspekt der klassischen Transposition.

Auf vielen der alten Stationsblätter befindet sich eine historische Einleitung über die Entwicklung oder die Verwendung der Verfahren. Dies ist bei der Blocktransposition nicht sinnvoll, da es keinen historisch spannenden Hintergrund mitzuteilen gibt und auch ein Bild der Entwicklergruppe als Bestandteil des Stationsblattes nicht mit den anderen Stationen zusammenpassen würde (s. Stationsblatt der Blocktransposition im Anhang).

Der kurze Erläuterungstext vor dem Beispiel soll den Schülerinnen und Schülern trotzdem einen kurzen theoretischen Hintergrund vermitteln. Deswegen war es wichtig, ihnen nahezubringen, dass es verschiedene Modi in der Blockverschlüsselung gibt. Wird der DES-Algorithmus im weiteren Unterricht besprochen, haben sie davon bereits gehört und wissen, wie der ECB-Modus funktioniert.

Auch die Einführung der Permutationen und ihrer Schreibweisen musste im Erklärungstext geschehen, um einen Mehrwert zu erschaffen und die Mathematik hinter dem Verfahren aufzuzeigen. Da eine Permutation jedoch durch die alleinige Definition schwer zu verstehen ist, bedarf es einem Beispiel. Dieses ist mit dem Beispiel des Verfahrens zusammengefasst, das auf fast jedem Stationsblatt zu finden ist. In diesem wird genau erklärt, wie die Permutation die Buchstaben umsortiert. Die Schülerinnen und Schüler können dadurch erkennen, dass die durch farbige Pfeile dargestellte Permutation ein Muster bildet. Wie dieses Muster genutzt werden kann, ist im nachfolgenden Text beschrieben. Dies ähnelt dem Aufbau der Caesar-Station, die das Verfahren zuerst anhand der Ersetzungstabelle erläutert und dann auf die Chiffrierscheibe verweist. Die Farben der Pfeile sind so ausgewählt, dass sie sich deutlich voneinander und dem grünen Hintergrund abheben. Außerdem sind die Pfeile von Buchstaben, die untereinander getauscht werden, in derselben Farbe. Dies wird auf dem Lösungsblatt beibehalten.

Die Permutationshilfen (s. Vorlage für Permutationshilfen im Anhang) sind eigentlich nur Darstellungshilfen für die Permutationen. Auf ihnen wird die Permutation aufgezeichnet, um die Buchstaben einfach und effizient umzusortieren, indem sie an die Stelle rücken, die der zugehörige Pfeil anzeigt. Die Funktionsweise ist im zweiten Erläuterungstext klar und einfach beschrieben, um Missverständnisse vorzubeugen. Die Permutationshilfen nützen den Schülerinnen und Schülern allerdings nur, wenn diese nicht zu klein und nicht zu groß schreiben. Deswegen gibt es eine Vorlage für Texte als Material, bei dem in jedes Kästchen genau ein Buchstabe geschrieben werden soll. Dies erinnert an die Vorlagen für Texte an der Station zu den Schablonen, bei der es ebenfalls für die Ver- und Entschlüsselung wichtig ist, wie die Buchstaben geschrieben werden. Sind diese zu groß oder liegen zu weit voneinander entfernt beziehungsweise zu nah aneinander, können die Schablonen nicht mehr genutzt werden. Eine solche Vorlage beugt somit Motivationssenkungen durch Misserfolge vor und soll die Lernenden bei der Bearbeitung der Aufgaben unterstützen.

Auf einem weiteren Materialblatt der Station sind vier Permutationshilfen abgedruckt. Die Längen sind unterschiedlich gewählt, um eine möglichst große Entscheidungsfreiheit bei der Auswahl eigener Permutationen zu gewährleisten. Zwei Blocklängen werden auf dem Arbeitsblatt benötigt. Zum einen wird die Permutationshilfe mit Blocklänge acht und dem vorgegebenen Schlüssel in Aufgabe 1 und 3 verwendet, um Nachrichten zu ver- und entschlüsseln. Zum anderen sollen die Schülerinnen und Schüler in Aufgabe 4 eine Permutation auf die Permutationshilfe mit Blocklänge sechs zeichnen. Alle Blocklängen sind so gewählt, dass sie nicht zu groß und nicht zu klein sind, wobei andere Blocklängen auch möglich gewesen wären. Die Blocklänge vier war die Kleinstmögliche, da die Blocklänge eins eine Nachricht nicht verschlüsselt und zwei und drei in Aufgabe 6 theoretisch betrachtet werden. Damit die Schülerinnen und Schüler nicht denken, dass Permutationen nur mit geraden Blocklängen funktionieren, ist zusätzlich noch eine ungerade Blocklänge gegeben.

Die Permutationshilfen sollen vor der Durchführung des SpionCamps oder in gemeinsamer Vorbereitung mit den Schülerinnen und Schülern gebastelt werden. Eine Möglichkeit ist, die Permutationshilfen und die dunklen Felder einfach nur auszuschneiden. Dann braucht man für jede Schülerin oder jeden Schüler mindestens zwei von ihnen, damit sie beschriftet werden können. Außerdem ist die Lebenszeit der Permutationshilfen auf die Bearbeitungszeit der Station beschränkt. Besser ist es, die Permutationshilfen zusätzlich zu laminieren. Dadurch können die Schülerinnen und Schüler Folienstifte nutzen, um Pfeile aufzuzeichnen und sie nach der Bearbeitung säubern. Dies spart Vorbereitungszeit und Papier. Eine kurze Bastelanleitung dazu findet sich ebenfalls auf dem Materialblatt der Permutationshilfen. Hierdurch ist diese Station jedoch die erste Station, die Folienstifte verwendet. Deswegen muss zusätzlich ein Folienstift in den Spionkoffer gelegt werden, damit dieser bei jeder Bearbeitung vorhanden ist.

Die Aufgaben zur Blocktransposition (s. Aufgabenblatt der Blocktransposition im Anhang) sind an die Aufgaben anderer Stationen angelehnt. Als Einstiegsaufgabe gibt es bei zwei Stationen eine Aufgabe zum Verschlüsseln des eigenen Namens. Da dieser jedoch häufig kürzer als acht Zeichen sein wird und daher nur ein Block verschlüsselt werden müsste, soll bei der Blockchiffre ein vorgegebener Satz verschlüsselt werden. Die Permutation ist dabei durch die Permutationshilfe mit Pfeilen vorgegeben, wodurch den Schülerinnen und Schülern der Einstieg in die Aufgaben erleichtert werden soll. Diese Aufgabe wurde nach der Erprobung im Unterricht aus Kapitel 5 verbessert. Dabei wurde die Aufgabenstellung präzisiert, um den Schülerinnen und Schülern die Bearbeitung zu erleichtern. In Kapitel 5.3 wird diese Verbesserung erläutert. Beide vorgegebenen Sätze, die auf dem Aufgabenblatt ver- und entschlüsselt werden sollen, sind so gewählt, dass

sie in eine Zeile der Textvorlage passen, wenn die Leerzeichen entfernt und benötigte Füllbuchstaben ans Ende geschrieben werden. Durch die Permutationshilfen müssen die Blöcke nicht voneinander getrennt werden, da die benachbarten Blöcke nicht zu sehen sind. Die vorgegebenen Sätze ergeben außerdem einen Treffpunkt, was zum Spionthema passt. Das Verschlüsseln in der Aufgabe 1 ist links in Abbildung 8 dargestellt.

An jeder Station (ausgenommen Buchstabenhäufigkeit, Modulo und Diffie-Hellman-Algorithmus) gibt es eine Aufgabe zum Entschlüsseln. Deswegen gibt es auch bei der Blocktransposition eine solche Aufgabe, bei der die Blocklänge und die Permutation festgelegt sind. Dabei müssen die Schülerinnen und Schüler die Permutationshilfen umgekehrt verwenden. Dies ist rechts in Abbildung 8 zu sehen. Im Weiteren gibt es bei den Stationen, an denen der Entschlüsselungsvorgang komplexer ist, also beim Pflügen, Playfair und Vigenère, Aufgaben, die lauten:

- „Beschreibe, wie du eine empfangene Nachricht mit bekanntem Schlüssel (= Anzahl Buchstaben pro Zeile) entschlüsseln kannst.“
- „Beschreibe das Verfahren für das Entschlüsseln der Nachricht. Was ist hier anders?“
- „Beschreibe ähnlich zum Verschlüsseln, wie das Entschlüsseln funktioniert.“

Das Entschlüsseln einer Nachricht, die mit der Blocktransposition verschlüsselt wurde, ist zwar vom Prinzip nicht schwierig. Es ist aber förderlich, sich über das Verfahren Gedanken zu machen und es einmal kurz aufzuschreiben. Dadurch schützt die Aufgabe vor Schwierigkeiten bei der Entschlüsselung, weswegen sie als zweite Aufgabe gestellt ist. Die Formulierung orientiert sich an der Pflügen-Station.

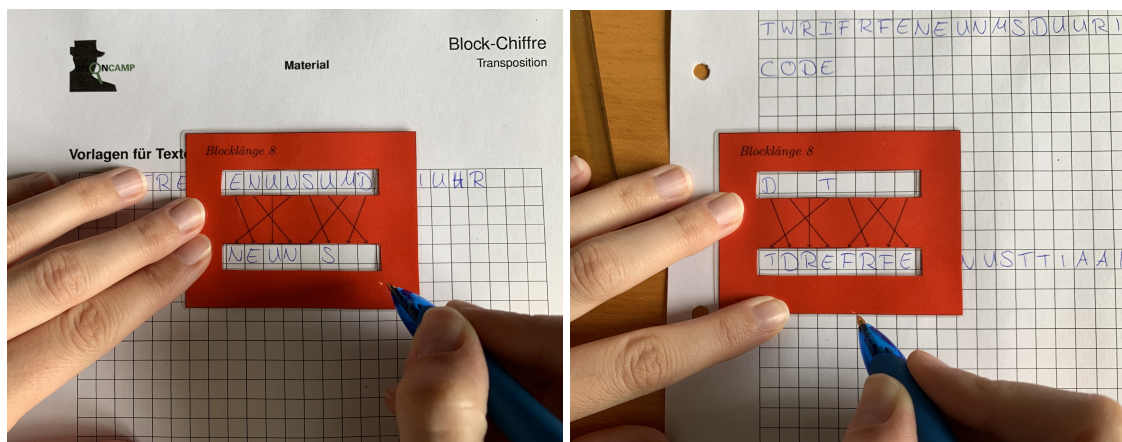


Abbildung 8: Ver- und Entschlüsseln mit der Permutationshilfe

An fast allen Stationen gibt es außerdem eine Aufgabe, bei der sich die Schülerinnen und Schüler gegenseitig eine Nachricht schreiben sollen. In einigen Fällen ist diese Aufgabe mit einem vorgegebenen Schlüssel formuliert und in den restlichen Fällen sollen die Schülerinnen und Schüler selbst einen Schlüssel wählen. Auf dem Aufgabenblatt der Schablonen-Station sind beide Varianten vorhanden. Damit nicht das gesamte Aufgabenblatt ohne die formale Schreibweise der Permutationen bearbeitet werden kann, soll es eine Aufgabe geben, in der die Schülerinnen und Schüler eine Permutation aufschreiben oder aufzeichnen. Dadurch liefert die Permutation einen Mehrwert und kann als zu entwickelnde Kompetenz für diese Station angegeben werden. Deswegen gibt es zwei Aufgaben, in denen sie sich gegenseitig eine Nachricht schicken. Eine davon mit vorgegebener Permutation und eine ohne. Die Permutationen werden dabei von den Schülerinnen und Schülern, wie in Abbildung 9 gezeigt, mit einem Folienstift auf die Permutationshilfen gezeichnet. Als Hilfestellung sollen sie die Vorlage für Texte nutzen, um die Pfeile ordentlich einzuzeichnen. Mit dieser Aufgabe gibt es somit drei Aufgaben, die auf das Verschlüsseln zielen, und ebenfalls drei Aufgaben, die das Entschlüsseln behandeln. Bei der Erprobung im Unterricht wurde darauf geachtet, ob die Bearbeitungszeit durch die Schülerinnen und Schüler bei dieser Station zu lang ist. Da dies nicht der Fall war, musste keine der Aufgaben wegfallen oder gekürzt werden.

Die letzte Aufgabe ist speziell für die Sekundarstufe II angelegt. Bei ihr muss das Wissen über die Kombinatorik genutzt werden. Sie soll auch helfen, ein Muster in den Möglichkeiten der Permutationen in Abhängigkeit der Blocklänge zu erkennen. Diese Mustererkennung wird auch in anderen Stationen durchgeführt. Beim Morsealphabet sollen die Schülerinnen und Schüler beispielsweise erkennen, dass die Anzahl der Zeichen mit den Häufigkeiten der Buchstaben zusammenhängt.

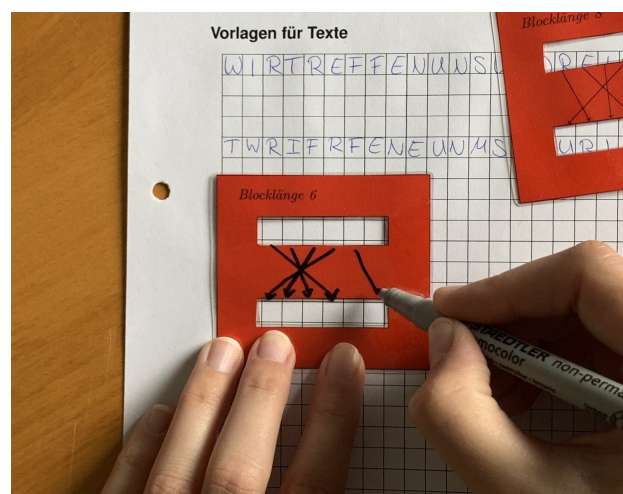


Abbildung 9: Beschriften der Permutationshilfe

Am Ende des Aufgabenblattes steht noch ein Hinweis, dass man die Permutationshilfen nach der Bearbeitung bitte sauber machen soll, damit die nächsten Schülerinnen und Schüler wieder mit Folienstiften auf sie zeichnen und somit alle Aufgaben alleine erledigen können. Das Säubern ist beispielsweise mit einem feuchten Lappen möglich. Die meisten Informatikkurse führen das SpionCamp jedoch im Informatikraum durch, in dem es keinen Wasseranschluss gibt. Deswegen sollte die Lehrkraft entweder einen Lappen vorbereiten oder mehrere Permutationshilfen einer jeden Sorte basteln, die nach der Durchführung des SpionCamps gesäubert werden können. Einige Folienstifte besitzen auch einen integrierten Radiergummi oder können mit einem solchen entfernt werden.

Der Aufbau des Lösungsblattes (s. Lösungsblatt der Blocktransposition im Anhang) hängt fast vollständig mit dem Aufgabenblatt zusammen. Die Ver- und Entschlüsselung der vorgegebenen Nachrichten wird wie auf dem Stationsblatt mit farbigen Pfeilen dargestellt, wodurch die Schülerinnen und Schüler das Muster der Permutation erkennen können. Die Wahl der Farben entspricht den Pfeilen auf dem Stationsblatt.

In der ersten Aufgabe kann sich die Lösung der Schülerinnen und Schüler aufgrund frei wählbarer Füllbuchstaben von der Musterlösung unterscheiden. Dies wird in der Lösung angesprochen und es wird nur ein Beispiel für die Lösung des letzten Blockes gegeben, der mit den Füllbuchstaben **AB** verschlüsselt ist.

In der zweiten Aufgabe sollen die Schülerinnen und Schüler beschreiben, wie sie eine Nachricht entschlüsseln können. Die Lösung erklärt dies nicht nur theoretisch, also dass die Permutation umgekehrt angewendet wird, sondern auch, wie dies praktisch mit den Permutationshilfen durchgeführt wird.

Zu den Aufgaben 4 und 5 gibt es aufgrund frei wählbarer Nachrichten keine allgemeine Lösung. Dies wird, wie im Rest des SpionCamps, durch den Satz „Zu dieser Aufgabe gibt es keine allgemeine Lösung.“ ausgedrückt.

Die Lösung der etwas schwierigeren Aufgabe 6 wird auf der zweiten Seite des Lösungsblattes erläutert. Eine zweite Lösungsseite gibt es zwar bei nur wenigen Stationen, durch sie konnte jedoch eine ausführliche Antwort gegeben werden. Es wäre auch denkbar gewesen, nur die Zahl der möglichen Permutationen anzugeben, wodurch die Schülerinnen und Schüler, die diese Aufgabe falsch oder nicht zu Ende gemacht haben, sie allerdings nicht verstehen können. Deswegen ist es sinnvoll, eine zweite Seite zu verwenden, um nicht nur die formale Schreibweise, sondern auch die graphische Darstellung abzubilden. Durch die graphische Darstellung können die Schülerinnen und Schüler eher einen Rückschluss darauf ziehen, was diese Aufgabe mit den anderen Aufgaben gemeinsam hat.

4.1.3 Kompetenzen

Durch die neue Station der Blocktransposition werden folgende Kompetenzen erlangt.
Die Schülerinnen und Schüler ...

- ... ordnen die Blockverschlüsselung der Transposition zu.
- ... kennen den heutzutage noch verwendeten *Electronic Code Book* Modus der Blockverschlüsselung, bei dem jeder Block einzeln verschlüsselt ist.
- ... schreiben Permutationen in Zweizeilenform auf.
- ... stellen Permutationen mithilfe von Pfeilen dar.
- ... schreiben Nachrichten in Blöcke einer bestimmten Länge.
- ... ver- und entschlüsseln Nachrichten mit der Blockverschlüsselung.
- ... nutzen Permutationshilfen zum Ver- und Entschlüsseln von Nachrichten.
- ... beschreiben die Ver- und Entschlüsselung von Nachrichten durch die Blockverschlüsselung.
- ... zeigen verschiedene Möglichkeiten für Permutationen einer festen Länge auf.

4.2 Stromchiffren

Der Begriff *Stromverschlüsselung* oder *Stromchiffre* bezeichnet ebenfalls eine Oberkategorie von verschiedenen symmetrischen Verschlüsselungsverfahren. Im Gegensatz zur Blockverschlüsselung hängt die Verschlüsselung jedoch nicht von der Länge des Geheimtextes ab. Mithilfe eines Startschlüssels wird durch die Nachricht ein Schlüsselstrom erzeugt. Deswegen sind Nachricht und Geheimtext eng miteinander verbunden.

Stromchiffren werden vor allem für Echtzeitübertragungen verwendet. Drei Beispiele dafür sind die Übertragungen von Mobiltelefonen zu Empfangsstationen, Bluetooth-Verbindungen und kontaktlosen Smartcards (vgl. Schmeh, 2013, S.289, 290 f., 295). Die gewählte Stromchiffre steht wieder in einer Verbindung zur Vigenère-Verschlüsselung und hat sogar einen gemeinsamen geschichtlichen Hintergrund, der auf dem Stationsblatt erläutert werden kann. Außerdem konnte eine enaktive Bearbeitung der Aufgaben durch einen selbstgebastelten Stromverschlüsseler, der an den Jefferson-Zylinder (vgl. F. L. Bauer, 1997, S.120) oder den Kryptex aus dem Film *Sakrileg* (Thomas Roth, 2016) erinnert, realisiert werden. Dieser zeigt das Prinzip der Stromverschlüsselung und lässt die Schülerinnen und Schüler auf eine innovative Art und Weise arbeiten.

4.2.1 Theoretische Grundlagen

Bei einer Stromverschlüsselung wird der Klartext mithilfe eines Schlüsselstroms verschlüsselt. Dafür werden wieder Zeichen eines Alphabetes Σ verwendet, die durch bestimmte andere Zeichen des Alphabets ausgetauscht werden. Es handelt sich somit um eine Substitution. Die Substitution wird durch einen Schlüsselstrom definiert, der mithilfe eines Startschlüssels $k_0 \in \mathcal{K}$ und eines Schlüsselstromgenerator $\mathcal{S} = \{S_i; i \in \mathbb{N}\}$ erzeugt wird. Dieser Schlüsselstrom wird verwendet, um alle Schlüssel für den Klartext zu ermitteln. Die Stromverschlüsselung wird *synchron* genannt, wenn der Schlüsselstrom unabhängig vom Klartext ist, und *asynchron*, wenn er von diesem abhängig ist. Im synchronen Fall gilt $k_i := S_i(k_0)$ für $i \in \mathbb{N}$, somit hängen einzelne Schlüssel nur vom Schlüsselstromgenerator und dem Startschlüssel ab. Ein Schlüsselstrom ist *periodisch*, wenn er sich nach einer bestimmten Zeit wiederholt, also wenn es ein $l \in \mathbb{N}$ gibt mit $k_{i+l} = k_i$. Die Vigenère-Verschlüsselung ist beispielsweise eine synchrone, periodische Stromverschlüsselung mit dem Startschlüssel, der durch das Schlüsselwort definiert ist, und einem Schlüsselstrom, der lediglich das Wort wiederholt (vgl. J. Müller, 2018, 19 f.).

Da die Verwendung von periodischen Schlüsselströmen aufgrund der einfachen Entzifferung durch eine Häufigkeitsanalyse jedoch nicht mehr verwendet wird, betrachten wir die asynchronen Stromchiffren.

Die wohl einfachste asynchrone Stromchiffre ist die sogenannte *Autokey-Verschlüsselung*, die bereits im 16. Jahrhundert verwendet wurde. Die erste Idee dazu entwickelte der Mathematiker CARDANO, der den Schlüsselstrom aus dem Klartext ableitete. Er benutzte für jedes Wort neu beginnend den Klartext als Schlüssel und verwendete das Vigenère-Quadrat bzw. zählte die Stellen des Buchstabens im Alphabet weiter. Was dies genau bedeutet und dass diese beiden Vorgehensweisen eigentlich dasselbe bewirken, wird im weiteren Verlauf noch ersichtlich. Das Vigenère-Quadrat ist in Abbildung 10 auf Seite 47 dargestellt und wird verwendet, wie in Kapitel 3.2 erläutert. Dies wird nun an einem Beispiel verdeutlicht:

Beispiel 4.2.1:

Klartext	D	I	E	N	E	U	E	S	T	A	T	I	O	N
Schlüssel	D	I	E	D	I	E	N	D	I	E	N	E	U	E
Geheimtext	G	Q	I	Q	M	Y	R	V	B	E	G	M	I	R

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

Abbildung 10: Vigenère-Quadrat (D. Müller, 2012)

Auf den ersten Blick wirkt diese Idee sinnvoll, würde man nun aber versuchen, den Geheimtext zu entschlüsseln, wäre dies äußerst schwierig. Das erste Wort wurde nämlich mit sich selber verschlüsselt, wodurch es keinen Ansatz gibt, wie der Schlüssel lautet. Die Verschlüsselung ist auch nicht eindeutig, da beispielsweise die Verschlüsselung von **D** durch **D** und die Verschlüsselung von **Q** durch **Q** jeweils den Geheimbuchstaben **G** ergeben. Dadurch ist das erste Wort des Klartextes nicht eindeutig und müsste geraten werden. Dies können ebenfalls Personen tun, an die der Text nicht gerichtet ist. Das Knacken und das Entschlüsseln ist somit der gleiche Vorgang.

VIGENÈRE machte aus der Idee von CARDANO eine neue Art der Verschlüsselung, indem er den ersten Buchstaben selbst wählte. Dieser wählbare Startschlüssel wird *Primary Key* genannt. Die darauf folgenden Schlüssel sind die Buchstaben des Klartextes oder des Geheimtextes. Für diese Verfahren werden also zwei Beispiele benötigt, eins, in dem die Klarbuchstaben genutzt werden und eins für die Geheimbuchstaben. Als Startschlüssel wurde in beiden Fällen das **E** gewählt.

Beispiel 4.2.2: (Schlüsselstrom entspricht Klartext)

Klartext	D	I	E	N	E	U	E	S	T	A	T	I	O	N
Schlüssel	E	D	I	E	N	E	U	E	S	T	A	T	I	O
Geheimtext	H	L	M	R	R	Y	Y	W	L	T	T	B	W	B

Beispiel 4.2.3: (Schlüsselstrom entspricht Geheimtext)

Klartext	D	I	E	N	E	U	E	S	T	A	T	I	O	N
Schlüssel	E	H	P	T	G	K	E	I	A	T	T	M	U	I
Geheimtext	H	P	T	G	K	E	I	A	T	T	M	U	I	V

Beide Verfahren wirken auf den ersten Blick wieder sinnvoll, allerdings kann die zweite Variante sofort geknackt werden, da der Schlüssel im Geheimtext offen liegt. Dadurch fehlt nur der erste Buchstabe im Klartext, der sich bei den meisten Nachrichten jedoch aus dem Kontext ergibt.

Allerdings ist auch das erste Verfahren nicht sicher, da es durch das Ausprobieren aller möglichen ersten Buchstaben gelöst werden kann. Dieses Verfahren wird trotz allem nun noch einmal detailliert betrachtet (vgl. F. L. Bauer, 1997, 144 f.).

Die formale Definition dieser Verschlüsselung ist, mit den oben verwendeten Notationen, durch die Verschlüsselungsfunktion

$$E_k : \Sigma^n \rightarrow \Sigma^n, v \mapsto v + k$$

und die Entschlüsselungsfunktion

$$D_k : \Sigma^n \rightarrow \Sigma^n, v \mapsto v - k$$

gegeben. Die Rechnungen $v + k$ und $v - k$ werden mithilfe der Identifizierung durch die Stellen (Ordinalzahlen) der Buchstaben im Alphabet realisiert, also ist A = 0, B = 1, usw. bis Z = 25. Dies entspricht auch der Verwendung des Vigenère-Quadrates, da die i -te Zeile der Verschiebung um i Stellen entspricht, also der Rechnung $+i$.

Sei $v = [v_0, v_1, \dots]$ der Klartext und $w = [w_0, w_1, \dots]$ der zugehörige Geheimtext, dann ist der Schlüsselstromgenerator definiert als $k_i = S_i(k_0, [w_0, \dots, w_{i-1}]) = D_{k_{i-1}}(w_{i-1}) = v_{i-1}$ für $i \in \mathbb{N}$. Damit ist der Schlüssel k_i äquivalent zum Klartext v_{i-1} (vgl. J. Müller, 2018, S. 20).

Wie bei der Caesar-Verschlüsselung gibt es auch hier eine Weiterentwicklung des Verfahrens, bei dem statt eines Startschlüssels aus einem Zeichen, ein Startschlüssel aus d Zeichen verwendet wird. Dabei handelt es sich bei d wieder um eine natürliche Zahl. Mit

dem gleichen Klartext wie in den anderen Beispielen und dem Startschlüssel **EFG** kann dies folgendermaßen dargestellt werden:

Beispiel 4.2.2:

Klartext	D	I	E	N	E	U	E	S	T	A	T	I	O	N
Schlüssel	E	F	G	D	I	E	N	E	U	E	S	T	A	T
Geheimtext	H	N	K	Q	M	Y	R	W	N	E	L	B	O	G

Diese Weiterentwicklung ist viel sicherer als die alte Variante, da das Durchprobieren der Anfangsschlüssel für sehr große d nicht mehr möglich ist. Die Entzifferung dieses Textes ist nur möglich, wenn ein Schlüssel oder ein Klartext mehrmals verwendet oder geschickt wird (vgl. F. L. Bauer, 1997, S. 145).

Auch hier können wir die formale Definition angeben. Die Ver- und Entschlüsselungsfunktionen bleiben gleich. Es ändert sich nur der Startschlüssel und Schlüsselstromgenerator. Sei $k = [k_0, \dots, k_{d-1}]$ der Startschlüssel, dann ist der Schlüsselstromgenerator definiert als $k_i = S_i(k, [w_0, \dots, w_{i-d}]) = D_{k_{i-d}}(w_{i-d}) = v_{i-d}$ für $i \in \mathbb{N}$. Damit ist der Schlüssel k_i äquivalent zum Klartext v_{i-d} .

Neben der Autokey-Verschlüsselung gibt es noch zahlreiche weitere Stromchiffren. Moderne Stromchiffren arbeiten meist nur mit der Binärdarstellung der Klartexte statt mit Buchstaben und generieren den eigentlichen Schlüsselstrom völlig unabhängig vom Klartext. Die Betriebsmodi der Blockverschlüsselung aus Kapitel 4.1.1 können ebenfalls realisiert werden, wobei die Blöcke der Länge 1 entsprechen. In einigen Varianten ist der Schlüsselstromgenerator ein Pseudozufallszahlgenerator (vgl. Schmech, 2013, S. 281-284). Es handelt sich dabei also um einen Einmalschlüssel, wie im One-Time-Pad. Dies ist ein einmal verwendbarer Schlüssel, der aus hunderten von Buchstaben oder Zeichen besteht (vgl. Singh, 2000, S. 151-156). Eine andere Möglichkeit, den Schlüsselstrom zu erzeugen, ist die Verwendung eines endlichen Automaten, wodurch die Chiffrierung jedoch periodisch wird (vgl. F. L. Bauer, 1997, S. 147).

4.2.2 Didaktische Analyse

Bei der neuen Station handelt es sich um die im Kapitel 4.2.1 beschriebene Autokey-Verschlüsselung, bei der die Schülerinnen und Schüler allerdings nicht das Vigenère-Quadrat verwenden, sondern die Identifizierung der Buchstaben durch die Stellen (Ordinalzahlen) im Alphabet, da die Arbeit mit dem Vigenère-Quadrat bereits an einer anderen Station geübt wird. Dies wird in der heutigen üblichen Kryptologie meistens so gemacht, da durch die Identifizierung einfacher gerechnet werden kann. Das »Rechnen

mit Buchstaben« ist für die Schülerinnen und Schüler neu und muss in der Station zunächst eingeführt werden. Diese einfachen Additions- und Subtraktionsaufgaben sollten von allen Schülerinnen und Schülern der Sekundarstufen I und II ausführbar sein. Der Stromverschlüsseler, der als Material verwendet wird, vereinfacht die Arbeit der Schülerinnen und Schüler sogar, da sie die Buchstabenbänder nur um eine bestimmte Anzahl weiter- oder zurückdrehen müssen.

Der Aufbau der Arbeitsmaterialien entspricht, wie bereits bei der Blockchiffre, den anderen Stationen des SpionCamps. Auf dem Stationsblatt befindet sich wieder ein Informationstext, der passend zum Untertitel und der Verschlüsselungskategorie *Substitution* festgelegt und unverändert ist.

Der Titel *Autokey-Chiffre* wurde ebenfalls nachträglich angepasst, da der vorherige Titel *Strom-Chiffre* wieder die Möglichkeit zur Erweiterung des SpionCamps um Stromchiffren genommen hätte. Der neue Titel entspricht der Schreibweise der Station zur Freimaurer-Chiffre. Diese gehört wie zuvor erwähnt zu den Substitutionen und ist eine Verschlüsselung, die von den Freimaurern entwickelt wurde, um sich auszutauschen. Der Begriff *Chiffre* wird in der Literatur unterschiedlich verwendet. SINGH bezeichnet als Chiffre „das Ergebnis einer Substitution, bei der jeder Buchstabe durch einen anderen Buchstaben oder ein Symbol ersetzt wird“ (Singh, 2000, S. 25). Andere Autoren verwenden *Chiffre* synonym zu *Verschlüsselungsverfahren* oder *Verschlüsselungsalgorithmus* (z. B. Schmeh, 2013, S. 39). Durch den Bindestrich zwischen den Wortteilen wird der Aspekt verstärkt, dass es sich bei beiden Chiffren (Freimaurer- und Autokey-Chiffre) um eine Verschlüsselung handelt, die sich jeweils durch einen bestimmten Aspekt auszeichnet. Bei der Freimaurer-Chiffre ist es die Entstehungsgeschichte und bei der Stromchiffre der Schlüsselstrom.

Im Erläuterungstext auf dem Stationsblatt (s. Stationsblatt der Autokey-Chiffre im Anhang) unter dem Informationskasten wird zuerst die allgemeine Stromverschlüsselung aufgezeigt, um den Schülerinnen und Schülern zu verdeutlichen, dass es eine Vielzahl verschiedener Stromverschlüsselungen gibt. Danach wird der spezielle Fall der Autokey-Verschlüsselung angesprochen und sein historischer Hintergrund dargestellt. Die Daten und das Bild von Vigenère sind von der Vigenère-Station übernommen.

Die Verbindung zur Vigenère-Station wird in einem Hinweis-Kasten aufgezeigt, dessen Stil vom Stationsblatt des Diffie-Hellman-Algorithmus übernommen ist. Das erste Beispiel erklärt, wie die Autokey-Verschlüsselung mithilfe des Vigenère-Quadrates gelöst werden kann. Eine weitere Station, die mit diesem Quadrat arbeitet, würde jedoch keinen

Mehrwert bringen. Deswegen wird im Erläuterungstext unter dem Beispiel darauf hingewiesen, dass sich die Station mit einer weiteren Möglichkeit zum Ver- und Entschlüsseln beschäftigt und die Wissenschaft häufig mit den Ordinalzahlen der Buchstaben und nicht mit den Buchstaben arbeitet. Da die Schülerinnen und Schüler noch an keiner Station mit der Ermittlung der Ordinalzahlen gearbeitet haben, wird dies ebenfalls aufgezeigt.

Im darauffolgenden Beispiel wird die Arbeit mit dem Stromverschlüsseler durch gebogene Pfeile verdeutlicht, welche die Drehung darstellen sollen. An den Pfeilen stehen die Schlüssel zum jeweiligen Klartextbuchstaben. Der Startschlüssel ist als **7** gewählt, wodurch der erste Buchstabe **G** um sieben Stellen weitergeschoben wird. Die Schülerinnen und Schüler drehen das Band des Stromverschlüsselers also sieben Stellen weiter und landen bei **N**. Als nächster Schlüssel im Schlüsselstrom wird nun der letzte Klartextbuchstabe gewählt, dies ist durch „G: 6“ gekennzeichnet. Die Verschlüsselung wird mit diesem Prinzip bis zum Ende des Klartextes vollzogen.

Wie auf dem Stationsblatt zur Caesar-Verschlüsselung folgt nun der angepasste Satz „Die »normale« Caesar-Verschlüsselung ist ziemlich leicht zu »knacken«. Etwas schwieriger wird es, wenn das Verfahren mit einem Schlüsselwort kombiniert wird.“ Der Startschlüssel wird nun als ein Schlüsselwort gewählt. Im dazugehörigen Beispiel wird das Schlüsselwort **CODE** zuerst in Zahlen umgewandelt und verschlüsselt dann denselben Klartext, wie im zweiten Beispiel. Dabei wird der erste Klartextbuchstabe nach den vier einzelnen Startschlüsseln bei der Verschlüsselung von **I** verwendet.

Alle Beispiele auf dem Stationsblatt wurden nach nach der Erprobung im Unterricht angepasst. Dazu zählt beispielsweise die farbliche Unterscheidung zwischen Startschlüssel und weiterem Schlüsselstrom sowie die genauere Erklärung des Vorgehens. Diese Verbesserungen werden ebenfalls in Kapitel 5.3 aufgezeigt.

Der Stromverschlüsseler (s. Stromverschlüsseler im Anhang) bestand vor der Erprobung im Unterricht aus zehn, nun nur noch aus sieben Buchstabenbändern, auf denen jeweils links und rechts der Buchstaben die Stellen im Alphabet stehen. So müssen sich die Schülerinnen und Schüler keine Stellen merken und können effektiver arbeiten. Hinter dem Buchstaben **Z** befand sich ein freies Feld, wodurch Leerzeichen dargestellt werden konnten. Dieses Feld wurde bei der Verbesserung entfernt. Die Anzahl der Buchstabenbänder ist so groß wie möglich gewählt, damit die Schülerinnen und Schüler beim Ver- und Entschlüsseln eines Klartextes möglichst selten bei den vorderen Bändern beginnen müssen. Zehn Bänder sind allerdings das Maximum, da die Bänder durch zwei Rechtecke, von dem eines Fenster zum Durchsehen besitzt, festgehalten werden und diese Rechtecke höchstens so lang sein können wie ein DIN-A4-Papier. Die Gründe für die Anpassung auf sieben Bänder sowie das Entfernen der Leerzeichen werden in Kapitel 5.3 erläutert.

Das Basteln des Stromverschlüssellers ist nicht intuitiv ersichtlich, weswegen eine Bastelanleitung als weiteres Material (s. Bastelanleitung im Anhang) hinzugefügt ist. Eine separate Bastelanleitung ist untypisch für das SpionCamp, da die meisten Bastelhinweise so kurz sind, dass sie auf das Blatt des Materials passen. Dies ist beim Stromverschlüsseler jedoch nicht möglich, weswegen die Bastelanleitung ausführlicher ausfallen konnte. Der Erläuterungstext und drei anschauliche Fotografien sollen den Lehrerinnen und Lehrern oder auch Schülerinnen und Schülern in der Vorbereitung beim Basteln helfen. Die Fotografien zeigen die neueste Version des Stromverschlüssellers.

Der Stromverschlüsseler ist so entwickelt, dass die Schülerinnen und Schüler den Klartext oder Geheimtext einstellen und dann die Bänder um die richtige Anzahl von Stellen weiter- oder zurückschieben können. Dabei sind im Rechteck, das die Buchstabenbänder hält, Fenster ausgeschnitten, in denen die aktuellen Buchstaben abgelesen werden können. Beim Verschlüsseln müssen sie sich die Schlüssel allerdings merken oder idealerweise notieren, weil der nächste Schlüssel nach der Verschlüsselung nicht mehr abgelesen werden kann. Dies sollte jedoch kein Problem darstellen, da sich die Schülerinnen und Schüler ohnehin Notizen zu den Aufgaben machen müssen. Beim Entschlüsseln sind die folgenden Schlüssel ganz einfach abzulesen, da sie in den Fenstern angezeigt werden. Die Arbeit mit dem alten Stromverschlüsseler ist in Abbildung 11 aufgezeigt. Das Prinzip ist bei der verbesserten Variante gleich geblieben.

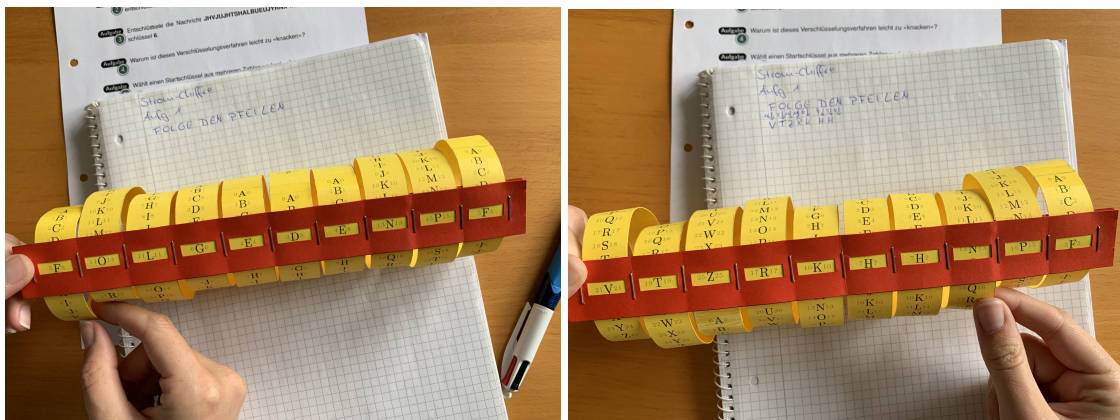


Abbildung 11: Verwendung des Stromverschlüssellers, links: Klartext vor dem Verschlüsseln, rechts: Verschlüsseln des achten Klartextbuchstabs

Ein Problem bei der Entwicklung des Stromverschlüssellers war die Stabilität. Sind die Buchstabenbänder zu schmal, verstellen sie sich, während die anderen Bänder eingestellt werden. Sind sie zu breit, drehen sie sich schlecht, was die Schülerinnen und Schüler demotivieren kann. Deswegen ist in der Bastelanleitung mehrfach darauf hingewiesen, die Drehbarkeit zu überprüfen und notfalls anzupassen.

Das zweite Problem war der Platzbedarf, da die fertig gebastelten Stromverschlüsseler

einem Zylinder mit einem Durchmesser von ca. sechs Zentimetern und einer Höhe von ca. 26 Zentimetern entsprechen. Der Spionkoffer ist auch ohne die neuen Stationen schon recht voll. Auch die Schulen, die das SpionCamp ohne Spionkoffer verwenden, haben vermutlich trotzdem eine entsprechende Aufbewahrung, bei der nicht davon ausgegangen werden kann, dass noch genug Platz vorhanden ist. Deswegen ist in der Bastelanleitung ebenfalls darauf hingewiesen, dass man den Stromverschlüsseler auch in flacher Ausführung verwenden kann. Das Drehen der Bänder kann zwar nicht mehr realisiert werden, aber durch das Schieben wird das Prinzip ebenfalls verdeutlicht. Möchte man den Stromverschlüsseler in den Spionkoffer integrieren, sollten die Skytalen in ihn hineingelegt werden. Dies wird in Abbildung 12 gezeigt. Schwieriger ist allerdings, weitere Fähnchen und Fähnchenhalter hinzuzufügen. Diese machen deutlich mehr Gesamtvolumen aus und müssen beim Schließen jedes Mal gezielt positioniert werden. Legt man einige von ihnen jedoch auf die CD-Hüllen in der Mitte, lässt sich der Koffer schließen.



Abbildung 12: Gepackter Spionkoffer mit den neuen Stationen

Das Arbeitsblatt zur Autokey-Verschlüsselung (s. Arbeitsblatt der Autokey-Chiffre im Anhang) ist analog zum Arbeitsblatt der Blocktransposition aufgebaut und auch die Aufgabenstellungen sind vereinheitlicht. Die einzigen Aufgaben, die sich unterscheiden, sind Aufgabe 4 und 6. Deswegen werden die Erläuterungen der anderen Aufgaben nur ganz kurz angesprochen, um nichts zu wiederholen.

In der ersten Aufgabe sollen die Schülerinnen und Schüler einen vorgegebenen Text mit einem festen Startschlüssel verschlüsseln. Danach sollen sie beschreiben, wie ein Geheimtext entschlüsselt werden kann und dies dann mit einem Startschlüssel und einer geheimen Nachricht in Aufgabe 3 durchführen. Auch das gegenseitige Schreiben von Nachrichten ist wieder in einer Aufgabe berücksichtigt. In Aufgabe 4 beschreiben die Schülerinnen und Schüler, wieso das Verfahren mit nur einem Startschlüssel leicht zu knacken ist. Diese Aufgabe orientiert sich dabei an dem anderen Verschlüsselungsverfahren, das leicht geknackt werden kann, wobei die Aufgabenstellung sogar wörtlich von der Station zur Caesar-Verschlüsselung übernommen ist. Daraufhin nutzen sie in Aufgabe 5 die erweiterte Autokey-Verschlüsselung, um sich gegenseitig Nachrichten zu schicken.

In der letzten Aufgabe dreht es sich wieder um die Mustererkennung. Die Schülerinnen und Schüler sollen über Fehlerfortpflanzung im Verfahren nachdenken und diese nicht nur auf die Verschlüsselung, sondern auch auf die Entschlüsselung beziehen. Diese Aufgabe ist wie auch die letzte Aufgabe bei der Blocktransposition speziell für die Sekundarstufe II entwickelt, kann aber auch schon von motivierten Schülerinnen und Schülern der Sekundarstufe I gelöst werden.

Nach der Erprobung im Unterricht wurde eine Tabelle mit den Stellen der Buchstaben auf dem Stationsblatt hinzugefügt. Der Grund dafür ist wieder in Kapitel 5.3 aufgezeigt.

Das Lösungsblatt (s. Lösungsblatt der Autokey-Chiffre im Anhang) ist wieder vom Arbeitsblatt der Station abhängig. Die Ver- und Entschlüsselung sind wie die Beispiele auf dem Stationsblatt durch Pfeile gekennzeichnet, an denen die Schlüssel stehen. Die Wörter sind dabei für die Übersichtlichkeit durch Leerzeichen voneinander getrennt. Weitere Aspekte der ersten und dritten Lösung müssen nicht aufgezeigt werden, da es sich einfach um die Ver- und Entschlüsselung gegebener Texte handelt.

Die Lösung der zweiten Aufgabe erläutert, wie eine Nachricht entschlüsselt werden kann. Dies wird wieder nicht nur theoretisch, sondern auch praktisch am Stromverschlüsseler aufgezeigt. Dabei wird auch darauf hingewiesen, dass der Schlüssel des nächsten Buchstabens direkt angezeigt wird.

Für Aufgabe 4 ist der Lösungssatz der analogen Aufgabe bei der Caesar-Station „Man muss höchstens 25 Schlüssel durchprobieren, um die Lösung zu erhalten.“ umformuliert, um einen besser klingenden Antwortsatz zu erhalten. Außerdem müssen im Gegensatz zur Caesar-Verschlüsselung alle 26 Schlüssel durchprobiert werden, da der Startschlüssel A nicht ausgeschlossen werden kann. Durch ihn würden trotzdem alle anderen Klartextbuchstaben mit dem jeweiligen vorherigen Klartextbuchstaben verschlüsselt werden. Der erste Buchstabe bliebe dabei erhalten. Die Lösung zu Aufgabe 5 entspricht wieder dem Satz „Zu dieser Aufgabe gibt es keine allgemeine Lösung.“.

In der Erläuterung zu Aufgabe 6 wird angesprochen, dass man es nicht merkt, wenn bei der Verschlüsselung ein Fehler passiert. Bei der Entschlüsselung zieht sich dieser Fehler jedoch durchgängig mit, wodurch jeder weitere Buchstabe falsch entziffert wird. Dies ist ein wichtiger Punkt, wieso bei dieser Verschlüsselungsart keine Fehler auftreten dürfen. Bei der Blockverschlüsselung hingegen wäre nur der Block beeinträchtigt, bei dem die Transposition falsch ausgeführt wird.

4.2.3 Kompetenzen

Die Bearbeitung der Station zur Autokey-Chiffre führt zu den folgenden Kompetenzen:
Die Schülerinnen und Schüler ...

- ... ordnen die Stromverschlüsselung der Substitution zu.
- ... kennen die *Autokey-Verschlüsselung* als ein Beispiel für eine Stromverschlüsselung.
- ... ver- und entschlüsseln Nachrichten mit der Stromverschlüsselung und einem Startschlüssel.
- ... ver- und entschlüsseln Nachrichten mit der Stromverschlüsselung und einem Schlüsselwort.
- ... nutzen ein zylinderförmiges Hilfsmittel mit Buchstabenbändern zum Ver- und Entschlüsseln von Nachrichten.
- ... beschreiben die Ver- und Entschlüsselung von Nachrichten durch die Stromverschlüsselung.
- ... erläutern, wieso die Stromverschlüsselung leicht geknackt werden kann.
- ... erklären, wie sich Fehler bei der Stromverschlüsselung fortpflanzen.

5 Erprobungen im Unterricht

Während der Erstellung der neuen Stationen aus Kapitel 4 floss viel theoretisches und praktisches Wissen mit ein. Trotzdem war es wichtig, die Stationen auch im Unterricht zu erproben, um Fehler zu identifizieren sowie zu entfernen, Hindernisse auszubessern und somit die Lernergebnisse zu maximieren. Die Stationen wurden in zwei Schulen in unterschiedlichen Jahrgangsstufen untersucht. In der ersten Schule wurde das gesamte SpionCamp mit einigen wenigen Pflichtstationen innerhalb von drei Unterrichtsstunden durchgeführt. Die andere Schule verwendet den Spionkoffer standardmäßig in den Differenzierungskursen der neunten Klassen, weswegen es sich anbot, die neuen Stationen nach der Bearbeitung innerhalb einer Doppelstunde auszuprobieren. Die Erprobungen fanden jeweils nach der letzten Klausur des Schuljahres kurz vor den Sommerferien statt.

5.1 Durchführung des SpionCamps

Die erste Erprobung der neuen Stationen fand in einem Informatikkurs der Einführungsphase statt und passte thematisch sehr gut in das Vorhaben der Lehrkraft. Sie ließ mir dabei freie Entfaltungs- und Entscheidungsräume, wodurch ich die Unterrichtsstunden passend gestalten konnte. Die Schülerinnen und Schüler hatten kein Vorwissen zur Kryptologie, weswegen das gesamte SpionCamp mit einigen ausgewählten Pflichtstationen durchgeführt wurde. Das SpionCamp wurde das erste Mal an der Schule umgesetzt, stieß jedoch bei den Informatik-Lehrkräften auf positives Feedback, sodass es in den nächsten Jahren vermutlich häufiger durchgeführt oder verwendet wird.

5.1.1 Vorbereitung

Die Erprobung sollte nach der letzten Klausur und vor Anfang der Sommerferien stattfinden. Die Lehrkraft hatte im Vorhinein bereits geplant, in den letzten Wochen des Unterrichts die Rolle von TURING im zweiten Weltkrieg zu behandeln, um damit Themen aus dem Inhaltsbereich *Informatik, Mensch und Gesellschaft* zu motivieren. Damit die Schülerinnen und Schüler die Funktionsweise der Enigma besser verstehen konnten, sollte vorher innerhalb von drei Schulstunden die Geschichte der Enigma behandelt werden. Diese Unterrichtsstunden wurden dann durch meine Erprobung ersetzt, wodurch die Bedingung entstand, die Rotoren-Station ebenfalls mit den Schülerinnen und Schülern durchzuführen. Die Lehrkraft des Kurses und ich entschieden, dass es zeitlich machbar wäre, das gesamte SpionCamp zu bearbeiten, wenn es nur einige ausgewählte Pflichtstationen gäbe. Dadurch konnte auch überprüft werden, wie gut sich die neuen Stationen in das bereits vorhandene SpionCamp einfügen ließen.

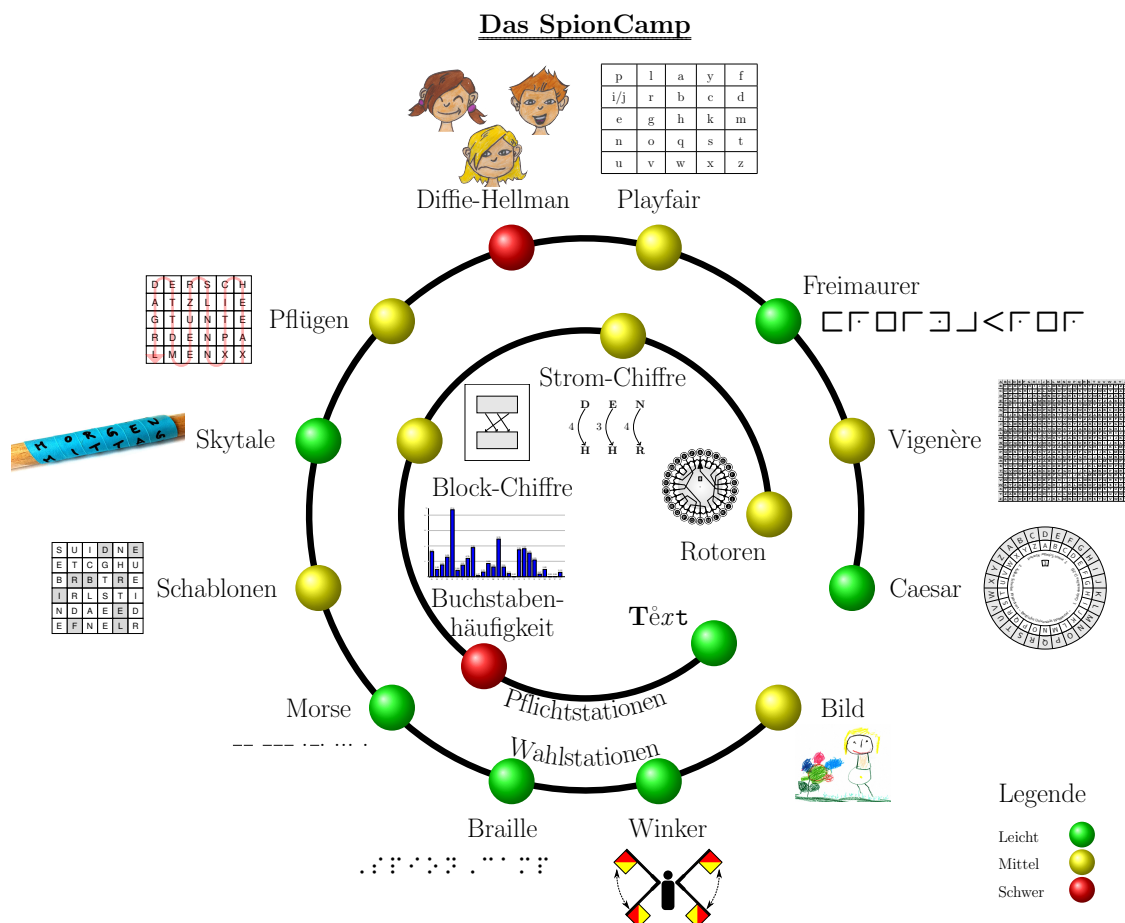


Abbildung 13: Überblick über die Stationen mit Angabe der Pflicht- und Wahlstationen

Beim Vorbereiten des benötigten Materials entstand auch die Grafik aus Abbildung 13, die aufzeigt, welche Stationen generell verfügbar und welche verpflichtend bearbeitet werden müssen. In dieser Grafik sind die Stationen nach Unterthemen sortiert, aber aufgrund der Übersichtlichkeit nicht zusätzlich markiert. Die Titel der neuen Stationen der Block- und Stromchiffre wurden erst nach den Erprobungen angepasst, weswegen in diesem Kapitel mit den alten Titeln gearbeitet wird. Die neuen Stationen sowie die Rotoren-Station waren als Pflichtstationen unabdingbar. Außerdem entschied ich mich, die neuen Stationen der Buchstabenhäufigkeit und der Steganographie als Text, die bei der Überarbeitung erstellt wurden, ebenfalls zu testen. Da die Analyse der Buchstabenhäufigkeit in einem Geheimtext ein Kryptoanalyseverfahren darstellt, passt es ebenfalls sehr gut als Einführung in das Knacken der Enigma. Die Stationen zum Diffie-Hellman-Algorithmus und zur Modulorechnung plante ich in eine gemeinsame Station ein, da eine Bearbeitung von nur einer von ihnen keinen sinnvollen Lernfortschritt erzeugt hätte. Die Grafik sollte den Schülerinnen und Schülern als Überblick und anstelle eines Laufzettels helfen, alle Pflichtstationen auf ihrem Lernweg zu durchlaufen.

Um eine anschließende Reflexion zu realisieren, sollten die Schülerinnen und Schüler Reflexionskarten bei der Bearbeitung der Stationen ausfüllen. Auf diesen hatten sie die Möglichkeit, ihre Kritik festzuhalten. Außerdem sollte ein Fragebogen (s. Fragebogen Einführungsphase im Anhang) Aufschluss geben, welche Stationen von den Schülerinnen und Schülern als positive Herausforderung angesehen wurden und ihr Selbstbild in der Informatik bestärkten.

5.1.2 Durchführung

Die Erprobung startete mit elf Schülerinnen und Schülern in einer Doppelstunde. Das SpionCamp war bereits aufgebaut, wobei sich die Stationen in der gleichen Anordnung wie in der Grafik in Abbildung 13 auf Seite 57 befanden. Dieser Aufbau ist in Abbildung 14 zu sehen. Die Pflichtstationen waren an den Gruppentischen in der Mitte und die Wahlstationen an den äußeren Tischen aufgebaut. Die Computer blieben ausgeschaltet und die Monitore nach hinten geschoben, um den Schülerinnen und Schülern ausreichend Platz zu geben. An jeder Station lagen zusätzlich zu den Materialien auch Reflexionskarten aus und die Schwierigkeitsgrade waren mithilfe von farbigen Fähnchen angegeben. Die Lösungsblätter befanden sich für die Schülerinnen und Schüler frei zugänglich am Lehrerpult in einem Hefter.



Abbildung 14: Aufbau des SpionCamps im Informatikraum

Am Anfang der Stunde setzten sich die Schülerinnen und Schüler zuerst an die Gruppentische und ich erklärte ihnen den Hintergrund und den Ablauf der Erprobung. Danach be-

gannen sie direkt damit, die Stationen an ihren Gruppentischen zu erledigen. Dabei kam es zu Schwierigkeiten, die durch einige Erläuterungen gelöst werden konnten. Die Schwierigkeiten traten auf, da die Schülerinnen und Schüler das Prinzip des SpionCamps noch nicht kannten. Sie versuchten sich an den Aufgaben, bevor sie die Erläuterungstexte lasen, und einige wählten zunächst schwierige Stationen. Nachdem mit den Schülerinnen und Schülern über die damit verbundenen Probleme gesprochen wurde, bearbeiteten sie auch andere Stationen. Dabei hatten sie auffallend viel Spaß an den spielerischen Stationen wie dem Winkeralphabet, dem Morsecode oder der Skytale. Der Unterschied zwischen Pflicht- und Wahlstation war nicht allen von ihnen bewusst, weswegen die Lehrkraft nach einiger Zeit noch einmal darauf hinwies, dass die Station zu den Rotoren als Grundlage für das Verständnis der Arbeit von TURING benötigt wird. Insgesamt hatte ich den Eindruck, die Schülerinnen und Schüler schauten nicht auf die Grafik am Whiteboard, wenn sie eine neue Station suchten, sondern orientierten sich an den angegebenen Schwierigkeitsstufen. Drei Schülerinnen und Schüler arbeiteten länger an der Buchstabenhäufigkeit und einer von ihnen erklärte, er wolle nicht zur nächsten Station, da er die Lösung noch herauskriegen wolle. Nach einem Blick in die Lösung wechselten zwei Schülerinnen und Schüler jedoch die Station. Eine Schülerin befasste sich mit der Aufgabe noch etwas länger.

Teilweise erschwerte es die Arbeit der Schülerinnen und Schüler, dass sie Erläuterungstexte und Beispiele nicht richtig lasen. Dadurch wurden beispielsweise an der Station zur Blockchiffre Klartexte verschlüsselt, in denen Leerzeichen beinhaltet waren und Füllbuchstaben fehlten. Diese Schwierigkeiten konnten aber immer durch einen Hinweis der Lehrkraft oder von mir beseitigt werden. Viele von ihnen bearbeiten auch nicht alle Aufgaben der Stationen, sondern hörten auf, wenn sie keine Lust mehr hatten. Dies wurde aufgrund der kurzen Zeit und dem Wunsch, alle Stationen auszuprobieren, nicht unterbunden. Da die Schülerinnen und Schüler die Reflexionskarten nur wenig verwendeten, ließ die Lehrkraft kurz vor Ende der Stunde noch eine Reflexionsrunde stattfinden, in der jeder eine kurze Rückmeldung geben sollte.

In der dritten Stunde der Erprobung im Unterricht waren ebenfalls elf Schülerinnen und Schüler anwesend. Für die drei Schüler, die in den ersten Stunden fehlten, erläuterte ich zuerst, was das SpionCamp genau ist und zeigte dies mittels der Grafik aus Abbildung 13 auf Seite 57 auf. Es wurde auch erneut darauf hingewiesen, dass es bestimmte Pflichtstationen gibt. Danach gingen alle in die Arbeit mit den Stationen. Die Reflexionskarten wurden aufgrund der wenigen Verwendung und der kurzen Zeit bis zur Ausfüllung des Fragebogens weggelassen. Kurz vor dem Ende der Bearbeitungszeit sollten die Schülerinnen und Schüler sich noch einmal die Stationen anschauen, die sie interessierten,

ohne dabei die Aufgaben zu machen. Dies führte dazu, dass sie einen besseren Überblick erlangten und wenigstens die Verfahren kennenlernen konnten. Nach etwa 30 Minuten wurde die Arbeit eingestellt und die Schülerinnen und Schüler füllten den Fragebogen aus. Die Unterrichtsstunde endete mit der Verabschiedung der Schülerinnen und Schüler und dem Abbau der Stationen.

5.1.3 Reflexion

In den ersten beiden Stunden der Erprobung wurden vier Reflexionskarten ausgefüllt. Leider gehörte keine davon zu den neuen Stationen der Block- und der Stromchiffre. Die folgenden Meinungen wurden von den Schülerinnen und Schüler notiert:

- Buchstabenhäufigkeit: „Ich finde, dass das Lösen des Geheimcodes Spaß gemacht hat, auch wenn es schwieriger war[,] als gedacht.“
- Braille-Schrift: „Gute Idee[,] um die Braille Schrift [...] auf spielerische Art und Weise [zu lernen.]“
- Morsealphabet: „1[,] Aufgabe war wie die vorherige mit [']Hallo['], wäre besser[,] wenn es ein anderes Wort wäre[.]“
- Winkeralphabet: „Sehr viel Spaß gehabt, einfach zu lösen, innovative Idee[.]“

In der Reflexionsrunde am Ende der Stunde kamen zusätzlich folgende Anmerkungen: Die durch farbige Flaggen gekennzeichneten Schwierigkeitsstufen passten gut zu den gelösten Stationen, wodurch auch das Wechseln der Stationen einfacher war. Die Erklärungen auf den Stationsblättern waren verständlich und nach dem Lesen konnten die Aufgaben gelöst werden, egal welcher Schwierigkeitsstufe sie zugeordnet waren. Es gab viele Auswahlmöglichkeiten, was jedoch für ein neues Thema ein bisschen zu viel auf einmal war. Die Schülerinnen und Schüler lobten, dass sie selbstständig arbeiten, frei entscheiden, anfassen und ausprobieren konnten. Nur das Drehen der Stromverschlüsseler war schwierig, was aber vermutlich am Papier lag. Die Umsetzung des Drehens an dieser und der Rotoren-Station wurde allerdings trotzdem gelobt. Insgesamt hat die Durchführung der Stationen Spaß gemacht und das spielerische Lernen gefiel den Schülerinnen und Schüler sehr gut. Sie fanden es sehr interessant, wie Texte verschlüsselt werden können. Vor allem das Arbeiten zu zweit oder in einer Gruppe wurde gelobt, da es sich nicht um die übliche Einzelarbeit handelt, sondern Abwechslung bringt. Die eigenen Botschaften, die man sich gegenseitig schicken konnte, wurden gerne ver- und entschlüsselt.

Der Fragebogen wurde nach den ersten beiden Stunden der Erprobung entwickelt, um speziell auf die Gruppe einzugehen. Die erste Seite bezog sich auf das gesamte Spion-Camp und die zweite Seite auf die neuen Stationen der Block- und Stromchiffre. Um eine Übersicht zu bekommen, wie viele und welche Stationen von den Schülerinnen und Schülern bearbeitet wurden, sollten sie diese zuerst angeben. Dies sollte ihnen auch noch einmal die Stationen ins Gedächtnis rufen. Tabelle 2 auf Seite 62 zeigt die Bearbeitung der Schülerinnen und Schüler, wobei viele Stationen teilweise nur kurz ausprobiert wurden. Die Pflichtstationen und insbesondere die Station zu den Rotoren, der Block- und der Stromchiffre wurden wie gewünscht auffallend häufig durchgeführt. Dann sollten sie Stationen nennen, die ihnen positiv oder negativ aufgefallen sind und auch einen Grund dafür nennen. Folgende Antworten wurden auf die Frage „Welche Stationen haben dir besonders gut gefallen und warum?“ gegeben:

- „Mir haben alle Stationen gut gefallen, allerdings vor allem Block-Chiffre und Morsealphabet, da man sich dort auf eine andere Art und Weise selbst betätigen konnte[.]“
- „Die Station Rotoren, weil man eine Verbindung zur Geschichte hat[.]“
- „Caesar[,] weil es mir leicht [fiel.]“
- „Winkeralphabet, da es sehr spielerisch war[.]“
- „Morsealphabet und Rotoren, weil ich es faszinierend finde, dass es so viele 'Geheimsprachen' gibt, die auf dem ersten Blick sehr kompliziert aussehen, jedoch mit den Hilfsmitteln sehr einfach zu lösen [sind].“
- „Braille-Schrift, da es sehr wichtig ist [...] sich mit der Braille Schrift vertraut zu machen, und das klappte gut[,] da man die Braille[-]Schrift auf spielerische Art und Weise erlernen konnte[.]“
- „Skytale, Braille-Schrift gute Umsetzung[.]“
- „Braille-Schrift[.]“
- „Mir hat die Station Strom-Chiffre besonders gut gefallen, da man viel ausprobieren konnte und es viel Spaß gemacht hat.“
- „Mir [gefiel] Diffie-Hellman besonders gut, weil man lange darüber nachdenken musste und weil ein bisschen Mathe dabei war.“

- „Die Station Rotoren hat mir besonders gut gefallen, weil das Thema sehr interessant und gut zu verstehen war durch den Informationstext.“

Bei der Frage „Welche Stationen haben dir weniger gut gefallen und warum?“ wurden die Stationen zu Playfair, zur Buchstabenhäufigkeit und auch zur Stromchiffre genannt. Bei der Playfair-Station wurde keine Erläuterung aufgeschrieben. Die Station zur Buchstabenhäufigkeit war laut Aussagen der Schülerinnen und Schüler zu schwierig, ihre Bearbeitung sehr zeitaufwendig und die Erklärung reichte den Schülerinnen und Schüler nicht aus. Eine Person schrieb, sie habe sich sehr häufig vertan, dies gehöre aber dazu. Bei der Stromchiffre war der Erläuterungstext ebenfalls schwer zu verstehen und der Stromverschlüsseler war nicht einfach zu verwenden, was die Motivation schwächte.

Stationen	Schülerinnen und Schüler									
Rotoren	X			X	X	X	X		X	X
Strom-Chiffre		X	X	X	X	X	X	X	X	X
Block-Chiffre	X		X	X	X	X	X			
Buchstabenhäufigkeit			X		X	X			X	X
Steganographie Text									X	X
Caesar			X	X						
Vigenère	X					X				
Freimaurer-Chiffre	X					X				
Playfair			X	X	X					
Diffie-Hellman			X						X	X
Pflügen										
Skytale	X			X	X	X	X			
Schablonen						X				
Morsealphabet	X	X	X	X	X	X				
Braille-Schrift				X	X	X	X	X		
Winkeralphabet				X						X
Steganographie Bild										

Tabelle 2: Angabe der bearbeiteten Stationen

Die meisten Schülerinnen und Schüler fanden die Hilfsmittel an allen Stationen hilfreich. Die Rotoren wurden sehr häufig gelobt. Zusätzlich sollten die Schülerinnen und Schüler angeben, welche Stationen sie zu leicht oder zu schwierig fanden. Als zu leicht wurden die Stationen zu der Caesar-Chiffre, dem Winker- und dem Morsealphabet, der Braille-Schrift und der Steganographie in Texten genannt. Alle diese Stationen waren bereits als leicht gekennzeichnet und sind eher für die Sekundarstufe I gedacht. Die Schülerinnen

und Schüler gaben die Stationen zur Buchstabenhäufigkeit, zur Stromchiffre und zum Diffie-Hellman-Algorithmus als zu schwierig an. Die Einordnung der Stromchiffre in den mittleren Schwierigkeitsgrad passte somit nicht. Als zu lang wurden die Bearbeitungszeiten der Stationen zu den Rotoren, der Buchstabenhäufigkeit und der Stromchiffre genannt. Wenn die zweite Erprobung im Unterricht diese Meinung verstärkt, müssen die Aufgaben der Station zur Stromverschlüsselung angepasst oder verkürzt werden. Um in der zweiten Erprobung auf jeden Fall eine Antwort auf diese Frage zu erhalten, wurde für die beiden neuen Stationen je eine Frage nach der Einschätzung zur Bearbeitungszeit gestellt.

Auf der zweiten Seite des Fragebogens ging es um die neu entwickelten und ausgearbeiteten Stationen und Materialien. Zuerst sollten die Schülerinnen und Schüler einschätzen, ob ihnen die Grafik am Whiteboard geholfen hat. Wenn dies überwiegend der Fall wäre, könnte man sie gemeinsam mit den neuen Stationen als Beispielablauf veröffentlichen. Da die Antworten jedoch sehr ausgeglichen ausfielen (drei Schülerinnen oder Schülern hat sie geholfen, drei waren sich nicht sicher und vier hat sie nicht geholfen) kann sie vermutlich weggelassen werden.

Bei den nächsten zwei Fragen sollten die Schülerinnen und Schüler ihre Meinung zur Station der Stromchiffre äußern. Neun von den zehn Schülerinnen und Schüler, die diese Station bearbeitet hatten, beantworteten auch die Fragen. Fünf von ihnen gaben an, dass die Station eine positive Herausforderung ist. Einige von ihnen lobten besonders die Umsetzung, die Erklärung auf dem Stationsblatt, die Materialien, die zum Ver- und Entschlüsseln gewählten Wörter und das Ausprobieren. Eine Person schrieb in das Feld nur „sehr kreativ“. Ob es sich dabei um die Ausarbeitung, die Idee oder die eigene kreative Arbeit handelt, kann nicht nachvollzogen werden. Sie sollten ebenfalls angeben, was sie an der Station schlecht fanden. Dabei gaben sie die Pappe, den Text, das schwierige Verstehen und den Zeitaufwand an. Mit „Text“ ist dabei vermutlich auch der Erklärungstext gemeint. Wieso manche Schülerinnen und Schüler die Erklärung als gut und manche als schlecht kennzeichneten, ist nicht erläutert. Vielleicht hängt dies mit dem Textverständnis, der Motivation oder Konzentration der Schülerinnen und Schüler zusammen. Die zweite Erprobung könnte auch dazu mehr Aufschluss bieten.

Es folgten drei Fragen zur Station der Blockchiffre. Vier der Schülerinnen und Schüler empfanden die Station als positive Herausforderung und eine Schülerin oder ein Schüler empfand die Station sogar als äußerst positiv. Auf die Frage, ob die Vorlagen für Texte ihnen geholfen haben, die Aufgaben zu erledigen, antworteten fünf mit „ja“ und zwei wussten es nicht genau. Sie heben an dieser Station besonders hervor, dass sie Spaß gemacht hat, die Vorlagen beim Entschlüsseln geholfen haben, dass sie mit einem Partner zusammenarbeiten konnten und wie die Station umgesetzt war. Negative Äußerungen gab

es keine, weswegen die Station insgesamt sehr gute Rückmeldungen bekommen hat. Zum Schluss sollten die Schülerinnen und Schüler einschätzen, wie viel sie vor und nach der Durchführung des SpionCamps über die Kryptologie wissen. Die Ergebnisse sind in Abbildung 15 dargestellt. Das Selbstbild der Schülerinnen und Schüler hat sich bei fast allen verbessert. Nur eine Schülerin oder ein Schüler sagt, sie oder er habe vor der Durchführung kein Wissen zur Kryptologie besessen und habe nun immer noch keins. Eine Person hat die Frage komplett ausgelassen.

Die letzte Frage war eine offene Frage nach Verbesserungen. Die Schülerinnen und Schüler füllten das Feld mit diesen Vorschlägen:

- „Informationstexte[...] bzw. Darstellung. Es war alles auf einmal und zu viel. Zu wenig Zeit.“
- „Dass man genug Zeit hat für alle Aufgaben.“
- „Das[s] man[,] wenn man Wörter entschlüsselt[,] nicht [so] oft das Wort [']Hallo['] vorkommt, sondern andere Wörter benutzt [werden.]“
- „Die Erklärungen zu den Stationen sind teilweise sehr lang und schwer zu verstehen.“

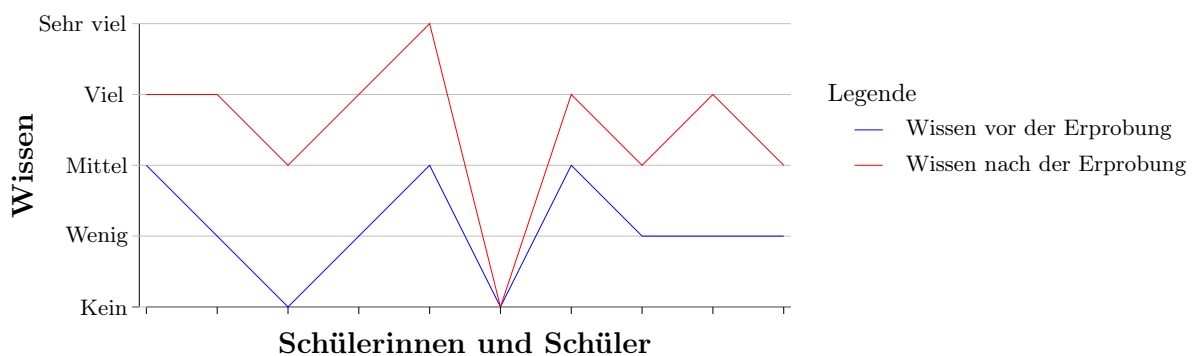


Abbildung 15: Wissen der einzelnen Schülerinnen und Schüler vor (blau) und nach (rot) der Durchführung des SpionCamps

5.2 Unterrichtserprobung mit neuem Material

Die andere Schule, an der ich die zweite Erprobung im Unterricht durchführte, plant das SpionCamp fest in den Lehrplan des Differenzierungskurses *Mathematik/Informatik* für die neunte Klasse ein. Da die Schule jeweils zwei Kurse parallel laufen lässt, aber nur ein Spionkoffer vorhanden ist, müssen die Kurse nacheinander das SpionCamp durchführen. Der jeweilige andere Kurs arbeitet an einem anderen Thema.

5.2.1 Vorbereitung

Die Erprobung des neuen Materials fand in der letzten Doppelstunde vor dem Beginn der Sommerferien in beiden Differenzierungskursen der neunten Klasse parallel statt. Dies war aufgrund der nebeneinanderliegenden und mit einer Tür verbundenen Informatikräume sehr gut realisierbar. Dabei sollten nur die neuen Stationen durchgeführt werden, da die Schülerinnen und Schüler bereits die anderen Stationen des SpionCamps bearbeitet hatten. Der eine Kurs hatte eine Doppelstunde vorher die Klausur zum SpionCamp geschrieben, weswegen das Vorwissen noch sehr präsent war.

Die zwei neuen Stationen sollten von allen Schülerinnen und Schülern durchgeführt werden, weswegen die Materialien sehr häufig benötigt wurden. Bei der Bearbeitung der anderen Stationen arbeiteten teilweise zwei oder mehr Schülerinnen und Schüler gemeinsam. Dies sollte auch bei den neuen Stationen frei entscheidbar sein. Die anderen beiden neu entwickelten Stationen der Buchstabenhäufigkeit und der Steganographie in Texten sollten als Alternativen gegeben sein.

Auch bei dieser Erprobung wurde ein Fragebogen (s. Fragebogen Differenzierungskurs im Anhang) zum Ende der Stunde eingeplant. Dieser sollte aufzeigen, wie die neuen Stationen im Vergleich zu den alten von den Schülerinnen und Schülern eingeschätzt werden. Der Fragebogen wurde speziell auf die Situation der Kurse und der Ergebnisse aus der vorherigen Erprobung angepasst. Die Fragen zur Grafik, dem Vorwissen und dem Wissen nach der Bearbeitung wurden durch Fragen zur Bearbeitungszeit und den Materialien ersetzt, wodurch diese Punkte genauer erfasst werden sollten. Dadurch konnte zwar keine Vergleichbarkeit mehr realisiert werden, diese wäre allerdings aufgrund der sehr unterschiedlichen Lerngruppen ohnehin schwierig gewesen.

Da die Erprobungen im Unterricht sehr nah beieinander lagen, konnte nicht jedes Feedback der Schülerinnen und Schüler der Einführungsphase vor der Durchführung in den Differenzierungskursen eingearbeitet werden. Während der Vorbereitung der Materialien wurde nur die bessere Drehbarkeit des Stromverschlüssellers beachtet und die Fragen des Fragebogens angepasst. Außerdem wurde zeitgleich der Text an der Station der Buchstabenhäufigkeit vereinfacht.

5.2.2 Durchführung

In der letzten Doppelstunde vor den Ferien waren in den Kursen relativ wenig Schülerinnen und Schüler anwesend. In einem Kurs fehlten zehn von 21 Schülerinnen und Schülern und im anderen zwei von 16, dies lag laut den Lehrkräften an Unterrichtsvorhaben anderer Fächer. Während ich im ersten Kurs bereits erklärte, was wir tun werden, und die Stationen vorne auf einigen Tischen auslegte, damit sich die Schülerinnen und Schüler

eine Station auswählen konnten, diskutierten die Schülerinnen und Schüler des anderen Kurses darüber, dass sie keine Lust hätten, richtig zu arbeiten. Ich erklärte auch ihnen, wieso die Durchführung wichtig sei, baute die Stationen auf und beide Kurse fingen an zu arbeiten. Dabei lagen die Lösungen der Stationen und feuchte Tücher zum Säubern der Permutationshilfen in einem der Räume auf dem Lehrerpult.

Die meisten Schülerinnen und Schüler begannen am Anfang mit den Stationen zur Block- oder Stromchiffre und wechselten danach zur jeweils anderen. War gerade kein Material der Stromchiffre verfügbar, überbrückten sie die Zeit mit der Steganographie in Texten. Manche schauten sich auch noch zum Ende der Stunde die Buchstabenhäufigkeit an, bearbeiteten sie jedoch aufgrund der fortgeschrittenen Zeit nur teilweise. Diese Schülerinnen und Schüler arbeiteten sehr konzentriert bis zum Ende der Erprobung und kamen so insgesamt auf mindestens drei Stationen. Einige Schülerinnen und Schüler wählten direkt zu Anfang die Station der Buchstabenhäufigkeit und knobelten bis zum Ende der zweiten Stunde an ihr. Dadurch konnten sie keine der anderen Stationen ausprobieren, waren jedoch sehr konzentriert bei der Sache und wollten die Station nicht wechseln. Eine Gruppe von Schülern ließ sogar die fünfminütige Pause aus, um weiter zu rätseln. Zwei andere Gruppen aus verschiedenen Kursen tauschten sich über die Stromverschlüsselung aus und erklärten sich gegenseitig das Prinzip. Die Unlust übermannte vier Schüler eines Kurses fast komplett, weswegen sie nur eine einzige Station angingen.

Auch die beiden Lehrkräfte versuchten sich an einigen Stationen und lasen sich die einzelnen Arbeitsmaterialien durch. Dabei gaben sie mir Hinweise zur besseren Verständlichkeit, wie beispielsweise dass einige wichtige Sätze schnell überlesen werden können. Diese Hinweise werden im Kapitel 5.3 noch einmal genauer betrachtet. Die Stabilität und Verstaubarkeit des Stromverschlüssellers war ebenfalls ein Thema, das wir besprachen. Sie wollten einen Stromverschlüsseler in den Spionkoffer legen und einen zweiten als Ersatz in einem Materialschränk im Informatikraum aufbewahren. Dafür entschieden sie, die Fähnchenhalter aus dem Spionkoffer rauszunehmen, da diese nicht verwendet werden, und an ihren Platz den Stromverschlüsseler zu positionieren. Die Lehrkräfte halfen den Schülerinnen und Schüler auch bei der Erledigung der Aufgaben und eine von ihnen knobelte längere Zeit mit einer Schülerin an der Station zur Buchstabenhäufigkeit.

Der Stromverschlüsseler wurde am Anfang von allen Schülerinnen und Schülern wie vorgesehen verwendet. Sobald sie allerdings verstanden hatten, dass es einer einfachen Addition oder Subtraktion entspricht, begannen sie damit, sich jeweils nur ein Band anzuschauen. Dabei kam es teilweise zu Rechenfehlern beim Übergang von **Z** zu **A** oder umgekehrt. Diese Fehler konnten durch ein erneutes Drehen vermieden werden. Ein anderes

Hindernis war die Lücke auf den Buchstabenbändern, die für Leerzeichen verwendet werden sollten. Diese wurden teilweise mitgezählt und ansonsten überhaupt nicht verwendet. Eine Lehrkraft empfahl ebenfalls, die Leerzeichen wegzulassen. Dies sollte bei der Überarbeitung – in Abhängigkeit der Ergebnisse der Befragung der Schülerinnen und Schüler – berücksichtigt werden.

Bei der Station zur Blockverschlüsselung traten sehr wenig Missverständnisse auf. Eine Schülerin fragte, was mit den Lücken bei zu kurzen Texten geschieht. Diese Frage konnte allerdings durch einen Verweis auf den zugehörigen Satz erklärt werden. Zwei Schülerinnen wollten bei der Entschlüsselung sicher sein, dass ihr Prinzip richtig ist, und fragten nach. Sie hatten das Prinzip aber bereits richtig erkannt. Auch das Säubern der Permutationshilfen wurde selbstständig von den Schülerinnen und Schülern durchgeführt, bevor ich mit meinem vorbereiteten feuchten Tuch helfen konnte.

In der zweiten Stunde der Unterrichtserprobung kamen zwei Schülerinnen aus der Qualifikationsphase 1 in einen der Kurse und fragten die Lehrkraft, ob sie mitmachen dürften. Da die Stationen eher für die Sekundarstufe II erstellt wurden, passte dies gut. Die beiden bearbeiteten die Stationen zur Block- und Stromchiffre und füllten netterweise die Fragebögen aus. Allerdings markierten sie diese, damit sie von den anderen unterscheidbar waren. Eine der beiden Schülerinnen aus der Qualifikationsphase 1 hatte keine Vorkenntnisse bzgl. Kryptologie, so dass die andere sie über die grundlegenden Elemente in Kenntnis setzen musste.

In den letzten 15 Minuten des Unterrichts wurden die Fragebögen ausgeteilt. Dabei hatte der eine Kurs Schwierigkeiten, auf die anderen Stationen des SpionCamps einzugehen, da es zu lange her war, dass sie diese bearbeitet hatten. Sie sollten die Fragen so gut wie möglich beantworten und ansonsten nur die Fragen zu den neuen Stationen ausfüllen.

5.2.3 Reflexion

Die Fragebögen, die in den Differenzierungskursen beantwortet wurden, sollten Aufschluss geben, ob sich die Stationen in das SpionCamp eingliedern lassen und welchen Eindruck sie auf die Schülerinnen und Schüler machten. Auf der ersten Seite wurden allgemeine Fragen zum SpionCamp gestellt. Durch sie sollte festgestellt werden, ob die Bearbeitung der neuen Stationen als deutlich schwieriger, leichter oder zeitaufwendiger angesehen wurden. Antworten, die sich nur auf die alten Stationen beziehen, bleiben in der folgenden Betrachtung unberücksichtigt.

Von den insgesamt 25 Schülerinnen und Schülern bearbeiteten 16 die Station zur Blockchiffre und 17 die zur Stromchiffre. Die Fragen auf der zweiten Seite des Fragebogens wurden nicht von allen Schülerinnen und Schülern beantwortet. Andere beantworteten diese, kreuzten jedoch nicht an, dass sie die Station bearbeitet hatten.

Die folgenden Antworten wurden in den Kursen auf die Frage gegeben, welche der Stationen von den Schülerinnen und Schülern als positive Herausforderung angesehen wurden:

- „Strom-Chiffre u. Pflügen, weil sie nicht so leicht waren, sodass man direkt fertig ist, aber nicht so schwer, sodass es unmöglich ist.“
- „Alle, da sie meistens knifflig und spannend waren und wir dazu selbstständig arbeiten konnten[.]“
- „Block-Chiffre, Morse-A., Skytale, Schablonen[.]“

Zwei Schülerinnen oder Schülern sahen somit die neuen Stationen als positive Herausforderung und eine weitere Person hebt knifflige Aufgaben positiv hervor.

Auf die Frage, welche Stationen als negative Herausforderung angesehen wurden, sind folgende Antworten hinsichtlich der neuen Stationen gegeben worden:

- „Strom-Chiffre, weil es schwer war.“
- „Strom-Chiffre, zu unerklärt und unverständlich[.]“
- „Strom-Chiffre[.]“

Dies zeigt, dass einigen Schülerinnen oder Schülern die Stromchiffre im Vergleich zu den anderen Stationen als negative Herausforderung ansehen. Dies liegt offensichtlich am Schwierigkeitsgrad, weswegen die Fragen auf der zweiten Seite zur Stromchiffre sehr gründlich betrachtet werden müssen.

Als Stationen mit hilfreichen Materialien wurden ebenfalls zweimal die Block- und einmal die Stromchiffre genannt. Eine Person fand die Materialien an allen Stationen hilfreich. Eine andere Person schrieb bei der Frage, welche Stationen zu leicht seien „fast alle“ und bei zu schwierig „Strom-Chiffre“. Außerdem fand sie die Bearbeitung der Stromchiffre als zu zeitaufwendig, hatte jedoch nicht angegeben, dass sie die Stromchiffre bearbeitet hat. Eine weitere Person gab die Stromchiffre bei den Fragen an, welche Stationen eine negative Herausforderung sei, welche Station zu schwer war und welche Bearbeitungszeit zu lang war. Leider gab sie auch auf der zweiten Seite keine Begründung dazu. Zwei Personen schrieben bei der Frage, welche Bearbeitung einer Station zu zeitaufwendig sei, dass sie für alle Stationen ca. 15–20 bzw. 20 Minuten gebraucht hätten.

Auf der zweiten Seite des Fragebogens wurden speziellere Fragen zu den neuen Stationen gestellt. Dabei sollten die Schülerinnen und Schüler einschätzen, ob sie die Stationen als positive Herausforderung wahrnehmen, wie lange sie an der Station gearbeitet haben und ob das Material geholfen hat. Die Frage nach der Bearbeitungszeit wurde mit dem besonderen Fokus auf die individuelle, subjektive Einschätzung formuliert. Sie sollten somit angeben, ob die Bearbeitungszeiten der Station ihnen zu lange oder zu kurz gedauert hat. Dies hängt natürlich mit der individuellen Konzentrationsfähigkeit, der Motivation und dem Spaß an den Verschlüsselungsverfahren zusammen. Eine einfache Angabe der Zeit wäre jedoch nicht sinnvoll, da eine schnelle Bearbeitung einer Schülerin oder einem Schüler nicht als eine solche vorkommen muss. Durch die subjektive Einschätzung konnte auf das individuelle Zeitgefühl eingegangen werden.

Außerdem gab es zu jeder Station eine offene Frage nach Punkten, die den Schülerinnen und Schülern besonders positiv oder negativ aufgefallen sind. Wie bereits bei der ersten Erprobung stand am Ende des Fragebogens eine Frage nach Verbesserungsvorschlägen. Diese wurde nicht mit den neuen Stationen in Verbindung gebracht, damit die Schülerinnen und Schüler sie auf alle Stationen beziehen und ihre Meinung mitteilen konnten.

Bei den Fragen zur Station der Stromchiffre gaben zwei Schülerinnen oder Schüler an, dass sie äußerst positiv aufgefallen ist, sieben, dass sie ihnen positiv aufgefallen ist und zehn ist sie weder positiv noch negativ aufgefallen. Dies zeigt, dass eine Überarbeitung sinnvoll sein kann, damit die Schülerinnen und Schüler bessere Lernergebnisse erzielen. Die Bearbeitungszeit wurde von den meisten Schülerinnen und Schülern als passend angegeben. Jeweils fünf gaben an, sie hätten zu lange oder zu kurz an ihr gearbeitet und neun, es wäre genau richtig gewesen. Dies lässt darauf schließen, dass die Aufgaben nicht verkürzt oder zusammengefasst werden sollten.

Das Material hat sieben von 19 Schülerinnen und Schülern sehr geholfen, sechs ein wenig, vier zu wenig und zwei der 19 Schülerinnen und Schüler hat das Material gar nicht geholfen. Dieses sollte also noch einmal überarbeitet werden, um alle Lernenden so gut wie möglich zu unterstützen.

Bei der offenen Frage nach positiven und negativen Einschätzungen wurden die folgenden Antworten gegeben.

Positive Einschätzungen:

- „alles[.]“
- „leicht[.]“
- „war gut[.]“
- „relativ einfach[.]“
- „war komplexer[.]“

Negative Einschätzungen:

- „zeitaufwendig[.]“
- „bisschen schwieriger[.]“
- „Das [Drehen] war unpraktisch[.]“
- „nicht klar zu verstehen[.] was zu tun ist -> also der Vorgang[.]“

Die Meinungen der Schülerinnen und Schüler gingen bei dieser Station also sehr weit auseinander. Einige fanden sie leicht, andere zu schwer. Ein paar fanden es gut, dass sie schwieriger war, andere nicht. Es kann aber auf jeden Fall festgehalten werden, dass der Vorgang besser erklärt werden sollte. Dies könnte in der ersten Aufgabe eingearbeitet werden, indem eine Anleitung gegeben wird. Dies wäre zwar untypisch für eine Station, könnte jedoch von den Schülerinnen und Schülern als Hilfe genutzt werden.

Die Station zur Blockchiffre wurde sehr positiv eingeschätzt. Sechs Schülerinnen und Schüler sahen die Station als äußerst positive Herausforderung, sieben als positive Herausforderung und nur drei als weder positive noch negative Herausforderung. Die subjektive Bearbeitungszeit wurde allerdings recht unterschiedlich eingeschätzt, da zwei Schülerinnen oder Schüler angaben, dass sie zu lange gedauert habe, zwei weitere, dass sie lange gedauert hat, einer das sie zu kurz war und drei, dass sie nur kurz an ihr gearbeitet haben. Für sieben Schülerinnen und Schüler war die Bearbeitungszeit genau richtig. Da insgesamt jeweils vier Schülerinnen und Schüler angaben, dass es zu lang bzw. zu kurz gedauert habe, scheint die Bearbeitungszeit der Station einen guten Ausgleich zu haben. Die Einschätzung zu den Materialien wurde bei der Blockchiffre aufgeteilt. Als Erstes wurde nach dem gesamten Material gefragt, das zehn Schülerinnen und Schüler sehr geholfen habe und fünf ein wenig. Eine Schülerin hat beide positiven Antworten angekreuzt. Danach wurde nach der Vorlage für die Texte gefragt. Diese hat zehn Schülerinnen und Schülern geholfen und sechs waren sich nicht sicher. Das kann daran liegen, dass sie keinen Vergleich ziehen konnten. Sie wussten nicht, wie die Bearbeitung ohne Vorlage ablaufen würde, da es keine Aufgabe ohne sie gab. Zwei weitere Schülerinnen oder Schüler, die keine der anderen Fragen beantwortet und die Station auch nicht angekreuzt haben, gaben an, die Vorlagen hilfreich zu finden. Was sie damit genau meinen, kann nicht nachvollzogen werden.

Bei der offenen Frage nach positiven Einschätzungen wurden die folgenden Antworten gegeben. Teilweise wurden sie auch doppelt genannt, was dahinter vermerkt ist.

- „leicht zu verstehen[.]“ (2-mal)
- „Die Aufgaben[.]“ (2-mal)
- „War interessant[.]“
- „Mir gefiel gut, dass wir die Permutationshilfen benutzen und eigene Verschlüsselungen ausdenken durften[.]“
- „leicht zu machen[.]“

Bei den negativen Einschätzungen wurde nur einmal die Antwort „Nix“ gegeben. Wie auch bei der ersten Erprobung im Unterricht zeigten diese Antworten, dass die Station zur Blockchiffre nicht verbessert werden muss. Die meisten Schülerinnen und Schülern fanden die Erklärungen auf dem Stationsblatt verständlich und sahen die Aufgaben als positive Herausforderung an.

Bei der offenen Frage nach Verbesserungsvorschlägen wurden einige Hinweise gegeben. Die folgenden beziehen sich auf die neuen Stationen:

- „große Abstände bei dem Material von Strom-Chiffre[.]“
- „[Bei der] Strom-Chiffre könnte die Bearbeitungsart genauer erklärt werden[.]“
- „genauere Erklärung[.]“
- „War perfekt!“

Auch bei dieser Frage zeigten die Schülerinnen und Schüler, dass sie verständlichere Erklärungen bei der Stromchiffre benötigen. Die Anpassung des Materials muss auf Realisierbarkeit überprüft werden und wird im Kapitel 5.3 aufgezeigt. Die Drehbarkeit des Stromverschlüssellers wurde nur einmal bemängelt. Dies zeigt, dass die kleine Anpassung zwischen den Erprobungen im Unterricht, die durch dünner ausgeschnittene Buchstabenbänder realisiert wurde, sinnvoll war.

Die Lehrkräfte der beiden Kurse gaben einige Hinweise zur Verbesserung des Materials. Eine von ihnen fand die Formulierung der ersten Aufgabe (s. Abbildung 16) bei der Station zur Blockchiffre missverständlich, wenn man sich die Materialien noch nicht angeschaut hat. Die Aufgabe besagt nicht, wo der Schlüssel vorgegeben ist, was zu Missverständnissen führen könnte. Außerdem ist nur in dem Satz „Ist die Nachricht zu kurz, werden Füllbuchstaben ans Ende gesetzt.“ auf dem Stationsblatt angegeben, was bei einer zu kurzen Nachricht geschehen muss. Dies führte bereits bei der Bearbeitung zu Schwierigkeiten, da der Satz überlesen wurde.

Aufgabe 1 Nimm dir die Permutationshilfe mit Blocklänge 8. Verschlüssele **WIR TREFFEN UNS UM DREI UHR** mit dem vorgegebenen Schlüssel.

Abbildung 16: Aufgabe 1 der Station zur Blockchiffre vor der Verbesserung

Die Beschriftung der Permutationshilfen wurde von einer Lehrkraft mit einer Nummerierung verwechselt, da auf dem Arbeitsblatt nicht angegeben ist, wieso es ausgerechnet

diese vier Permutationshilfen gibt. Dies lag vermutlich auch daran, dass an der Station zwanzig verschiedenfarbige Permutationshilfen lagen, damit alle Schülerinnen und Schüler gleichzeitig arbeiten konnten. In der Regel kann davon ausgegangen werden, dass dieses Problem bei der üblichen Arbeit mit den Stationen nicht auftritt. Die Schülerinnen und Schüler hatten zudem kein Problem, so dass keine Überarbeitungsnotwendigkeit entsteht.

Die Lehrkraft, die sich mit dem Stromverschlüsseler beschäftigte, empfahl mir, die Leerzeichen wegzulassen, da sie beim Drehen mitgezählt wurden. Von den Schülerinnen und Schülern wurden sie nicht zur Darstellung von Leerzeichen verwendet, weswegen dies keine große Umstellung wäre. Das Weglassen der Leerzeichen würde den Stromverschlüsseler sogar ein bisschen kleiner machen. Die Lehrkraft fragte mich auch, wieso es zehn Buchstabenbänder seien. Dadurch sei der Stromverschlüsseler sehr lang und die Schülerinnen und Schüler müssten trotzdem wieder am Anfang mit der Nachricht beginnen. Eigentlich würde auch ein oder zwei Bänder ausreichen, um das Prinzip zu verstehen.

Die zwei Schülerinnen aus der Qualifikationsphase 1, die in der zweiten Unterrichtsstunde dazustießen, bearbeiteten die Stationen zur Block- und Stromchiffre. Beide gaben die Station zur Stromchiffre auf der ersten Seite des Fragebogens als positive Herausforderung an und fanden das Material hilfreich war. Eine von ihnen fand sie sogar zu leicht. Auf der zweiten Seite gaben sie beide an, dass sie die Station zur Stromchiffre als äußerst positive Herausforderung ansahen, sie genau die richtige Bearbeitungszeit hatten und das Material ein wenig geholfen hat. Besonders positiv aufgefallen war ihnen das Erfolgserlebnis und negativ die Unübersichtlichkeit. Da beide fast genau dasselbe schrieben, kann man davon ausgehen, dass sie die Fragen nicht unabhängig voneinander beantworteten. Die Fragen zur Station der Blockchiffre beantworteten sie unterschiedlich. Beide sahen die Station als positive Herausforderung an, eine von ihnen fand die Bearbeitungszeit zu lang und die andere zu kurz. Das Material hat einer zu wenig und der anderen gar nicht geholfen. Die Vorlage für Texte fand eine hilfreich und die andere konnte es nicht genau einschätzen.

Diese Ergebnisse sind komplementär zu dem bisherigen Feedback. Die meisten anderen Schülerinnen und Schüler fanden die Station zur Blockchiffre besser als die Station zur Stromchiffre. Bei den beiden älteren Schülerinnen ist es aber genau andersrum. Dies könnte am Schwierigkeitsgrad liegen. Ihre Antworten unterstützen jedoch trotzdem die Einschätzungen, dass die Station zur Stromchiffre hinsichtlich der Übersichtlichkeit bzw. besseren Erklärungen überarbeitet werden muss.

5.3 Verbesserungen

Die Erprobungen im Unterricht waren zeitlich schlecht gelegt, da sie kurz vor den Sommerferien stattfanden. In diesen Stunden waren einige Schülerinnen und Schüler unmotivierter und arbeiteten schlecht mit. Aufgrund der Rahmenbedingungen der konkreten Erprobung mit diesen Lerngruppen sind die Ergebnisse durchaus kritisch zu betrachten. Dennoch unterstützen die ausführlichen Antworten, meinen Eindruck während der Unterrichtsstunden. Es kamen somit einige Verbesserungsvorschläge für die neuen Stationen der Block- und Stromchiffre auf, die umgesetzt werden sollten. Durch alle diese Verbesserungen sollen die Wünsche der Schülerinnen und Schüler berücksichtigt und der zukünftige Lernerfolg vergrößert werden.

Die Schülerinnen und Schüler schienen mit der Station und dem Material der Blockchiffre bereits zufrieden zu sein, nur die Lehrkräfte der beiden Differenzierungskurse sahen dies kritischer. Die Formulierung der ersten Aufgabe (s. Abbildung 16 auf Seite 71) sei missverständlich, wenn man sich die Materialien noch nicht genauer angeschaut hätte. Dies sah man ebenfalls an den Problemen der Schülerinnen und Schüler, da sie nicht wussten, wie sie mit Leerzeichen und zu kurzen Nachrichten umgehen sollten. Als Konsequenz wurde entschieden, die Aufgabenstellung anzupassen (s. Aufgabenblatt der Blocktransposition im Anhang). Nun können die Schülerinnen und Schüler sofort erkennen, wie der Schlüssel vorgegeben ist, dass sie die Leerzeichen auslassen sowie Füllbuchstaben verwenden müssen.

Bei der Stromverschlüsselung müssen zwei Dinge angepasst werden. Zum einen wünschen sich die Schülerinnen und Schüler, dass der Stromverschlüsseler überarbeitet wird, und zum anderen sollte der konkrete Vorgang detaillierter erklärt werden.

Zuerst wird die Anpassung des Stromverschlüsselers aufgezeigt. Die meisten Schülerinnen und Schüler verstehen nach einigen Aufgaben das Prinzip und rechnen nur noch mit den Buchstabenwerten. Die erste Idee ist also, ein Buchstabenband auf das Arbeitsblatt zu drucken, damit die Schülerinnen und Schüler, die das Band nur noch zum Rechnen benutzen, dieses nicht ständig drehen müssen. Dies konnte – wie auf den Arbeitsblättern zu den Codierungen – realisiert werden, indem eine Tabelle mit den Buchstaben und ihren Positionen im Alphabet abgedruckt wurde (s. Arbeitsblatt der Autokey-Chiffre im Anhang).

Viele Schülerinnen und Schüler hatten Probleme beim Zählen mit den Buchstabenbändern im Übergang von **Z** zu **A**, was teilweise am Mitzählen der Leerzeichen lag. Aus diesen Gründen wurde entschieden, die Berücksichtigung von Leerzeichen in der Überar-

beutung zu entfernen. An den Bändern befindet sich nur noch ein Kleberand unter dem **Z**. Der Wunsch nach mehr Abstand zwischen den Bändern konnte mit dem Wunsch nach weniger Bändern verbunden werden. Um die Wahl der Anzahl zu treffen, wurde ökologisch argumentiert. Das Ersetzen dreier Bänder auf dem Materialblatt durch die beiden Rechtecke, die sie halten, würde ein Papier weniger benötigen. Außerdem musste Aufgabe 3 nicht angepasst werden, da die Schülerinnen und Schüler für 21 Buchstaben dreimal beim vorderen Band beginnen müssen und dies nicht beeinträchtigt ist. Allerdings mussten sie bei Aufgabe 1 aufgrund der 15 Buchstaben für einen Buchstaben wieder vorne beginnen (s. Abbildung 17). Da die Bearbeitungszeit jedoch nicht optimal war, wurde der Klartext **FOLGE DEN PFEILEN** durch **FOLGE DEM PFEIL** ersetzt. Dies passt weiterhin zum Spionthema, ist aber schneller verschlüsselt. Die Lösung musste auch nur minimal angepasst werden.

Aufgabe 1 Verschlüssele **FOLGE DEN PFEILEN** mit dem Startschlüssel **16**.

1

Abbildung 17: Aufgabe 1 der Station zur Stromverschlüsselung vor der Verbesserung

Der Stromverschlüsseler besteht somit nur noch aus sieben Buchstabenbändern, die weiter auseinander liegen. Außerdem wurden die Rechtecke verbreitert, um sie besser halten zu können und die Buchstabenbänder minimal verschmälert. Nun ist zwischen je zwei Buchstabenbändern genug Platz, um den Stromverschlüsseler zu halten.

Um die Drehbarkeit des Stromverschlüssels noch weiter zu verbessern, wurde zwischen den Markierungen für die Tackernadeln mehr Platz gelassen. Da jedes Buchstabenband nun von zwei Tackernadeln gehalten wird, um die Lücken zu realisieren, kann dies auch noch selbst von den Lehrerinnen und Lehrern angepasst werden. Der verbesserte Stromverschlüsseler ist in Abbildung 18 zu sehen.

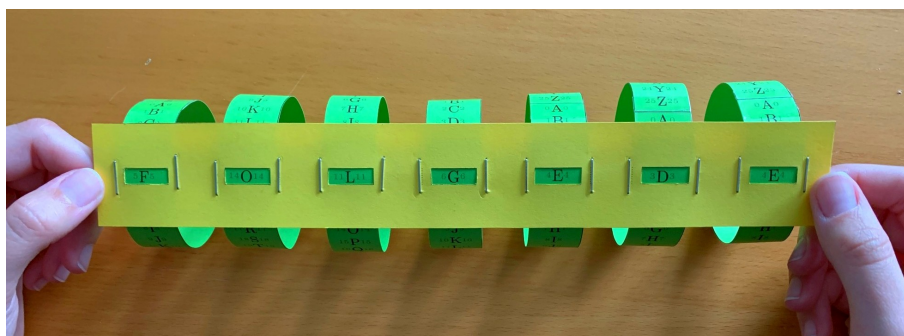
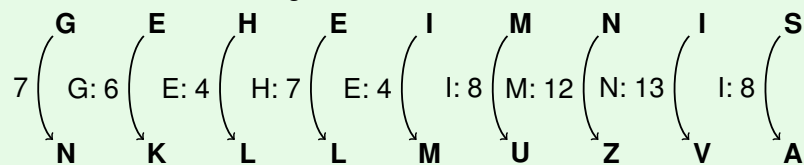


Abbildung 18: Verbesserter Stromverschlüsseler

Um die Erklärung auf dem Stationsblatt anzupassen, wurde zuerst das Beispiel leicht verändert, das mit dem Vigenère-Quadrat arbeitet. Das Schlüsselwort ist nun in rot geschrie-

ben, um es zu verdeutlichen. Dies wird auch in den anderen Beispielen weitergeführt, weswegen im zweiten Beispiel der Startschlüssel **7** und im letzten Beispiel das Schlüsselwort **CODE** rot geschrieben ist.

Beispiel Der Startschlüssel ist die Zahl **7** und unsere Nachricht lautet **GEHEIMNIS**. Nun stellen wir die Nachricht in der Stromverschlüsseler ein und drehen die Buchstabenbänder jeweils um den passenden Schlüssel weiter. Wir schieben also das **G** 7 Stellen weiter und erhalten ein **N**. Dann schieben wir das **E** um die Stelle vom vorherigen Klartext weiter, also 6 Stellen, und landen bei **K**. Dies machen wir so lange weiter bis wir alle Buchstaben verschlüsselt haben.

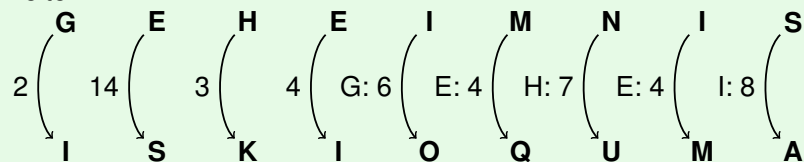


Unser Geheimtext lautet somit **NKLLMUZVA**.

Abbildung 19: Zweites Beispiel des Stationsblattes vor der Verbesserung

Der Text des zweiten Beispiels (s. Abbildung 19) wurde dahingehend geändert, dass die einzelnen Arbeitsschritte deutlicher beschrieben wurden. Das Einstellen der Nachricht ist erläutert, sodass die Schülerinnen und Schüler die Buchstaben in den Fenstern sehen können. Außerdem wird betont, dass die Verschlüsselung vorne beginnt, und mit welchem Schlüssel der zweite und die darauf folgenden Buchstaben verschlüsselt werden. Durch diese Anpassungen (s. Stationsblatt der Autokey-Chiffre im Anhang) werden die Schülerinnen und Schüler das Prinzip eher verstehen und auch ausführen können.

Beispiel Unser Startschlüssel ist jetzt **CODE**, was den Zahlen **2 14 3 4** entspricht, und unsere Nachricht lautet wieder **GEHEIMNIS**. Dann hängen wir, wie eben, den Klartext an den Schlüsselstrom, stellen die Nachricht in den Stromverschlüsseler ein und drehen die Buchstabenbänder jeweils um die passenden Stellen weiter.



Unser Geheimtext lautet also **ISKIOQUMA**.

Abbildung 20: Drittes Beispiel des Stationsblattes vor der Verbesserung

Das zweite Beispiel war vor der Verbesserung sehr kurz gehalten (s. Abbildung 20), weil das Prinzip und das Vorgehen übertragbar ist. Diese Übertragbarkeit fiel den Schülerin-

nen und Schülern jedoch schwer. Daher ist in der neuen Version (s. Stationsblatt der Autokey-Chiffre im Anhang) explizit beschrieben, dass die ersten vier Buchstaben mit dem Schlüsselwort verschlüsselt werden. Dies ist auch durch zusätzliche Buchstaben vor dem Schlüssel angezeigt. Es wird auch noch einmal darauf hingewiesen, dass die folgenden Buchstaben mit dem Klartext von Anfang an verschlüsselt werden.

Außerdem wurde die erste Aufgabe, wie auch schon bei der Blockverschlüsselung, um eine kurze Anleitung erweitert. Die alte Version der Aufgabe ist in Abbildung 17 auf Seite 74 zu sehen. Durch die neue Formulierung (s. Arbeitsblatt der Autokey-Chiffre im Anhang) können die Schülerinnen und Schüler der Anleitung folgen, indem sie die Nachricht einstellen, den ersten Buchstaben mit dem Schlüsselwort verschlüsseln sowie die darauf folgenden mit den Klartextbuchstaben.

6 Fazit

Das Unterrichtsfach Informatik ist zurzeit in Nordrhein-Westfalen in einem großen Wandel. Obwohl es noch nicht an jeder Schule angeboten wird und noch nicht jede Schülerin sowie jeder Schüler eine informatische Allgemeinbildung erfährt, wird es immer stärker ausgebaut. Zum einen muss Informatik zukünftig alleine oder in einer Fächerkombination als Wahlpflichtfach an allen Gymnasien angeboten werden (vgl. MSB-NW, 2018b, S. 3). Zum anderen sind zwei Schulstunden in der neuen G9-Studentafel für die informatische Bildung vorgesehen (vgl. MSB-NW, 2018a, S. 3). Wie die Leistungen der „informatischen Bildung“ genau zugeordnet werden, ist zurzeit noch nicht klar definiert. Zusätzlich führen die Bezirksregierungen Düsseldorf und Köln seit dem Schuljahr 2018/19 das Modellvorhaben *Informatik in der Erprobungsstufe des Gymnasiums* (Müller u. a., 2019) durch. Mehr als 80 Gymnasien haben für die nächsten vier Jahre mindestens einen Klassenzug eingeführt, der durchgängig eine Informatikstunde pro Woche hat. Die Auswirkungen dieses Modellvorhabens werden mittels Fragebögen festgehalten, die aufschlussreiche Ergebnisse liefern, ob sich die Kompetenzen, das Selbstbild und die Einstellung der Schülerinnen und Schüler zur Informatik positiv verändert hat. Die ersten Ergebnisse dieses Modellvorhabens zeigen das große Interesse der Schülerinnen und Schüler sowie deren Eltern an der Informatik. Viele Schulen, die an diesem Modellvorhaben teilnehmen, bieten Informatik ab nächstem Schuljahr in jeder fünften Klasse an.

Insgesamt werden zurzeit und auch zukünftig sehr viele Informatiklehrkräfte benötigt. Diese haben aufgrund der wenigen Angebote durch Lehrbücher allerdings einen hohen Vorbereitungsaufwand. An vielen Schulen gibt es auch nur eine Informatiklehrkraft, weswegen sie sich schlecht untereinander austauschen können. Angebote von Universitäten, Schulen oder Privatpersonen werden deswegen gerne genutzt, um den Aufwand zu verringern. Die in Kapitel 3.3 aufgezeigten Materialien bilden eine Hilfe für die Vorbereitung des Unterrichts in vielen verschiedenen Themen, insbesondere der Kryptologie. Das SpionCamp entlastet die Lehrkräfte bei ihren Planungs- und Materialentwicklungsprozessen. Durch einen Spionkoffer wird zusätzlich die praktische Vorbereitung erspart.

Die Kryptologie bietet sich für ein Stationenlernen an, da die einzelnen Verschlüsselungsverfahren als Stationen realisiert werden können. Die meisten Stationen des SpionCamps sind unabhängig voneinander bearbeitbar, wodurch ein selbstgewählter Lernweg gestaltet werden kann. Auch die Bearbeitungszeit ist kurz gehalten, was in den Erprobungen im Unterricht in Kapitel 5 aufgezeigt wurde. Bei diesen gaben die Schülerinnen und Schüler selbst an, dass sie nur 20 Minuten gebraucht hätten, bzw. in einer Doppelstunde mindestens drei Stationen erfolgreich bearbeitet hatten. Auch das Einsehen der Lösbarkeit

wurde in der ersten Erprobung aufgezeigt. Dort kamen einige Schülerinnen und Schüler zu dem Schluss, dass man alle Aufgaben mithilfe der Erklärungstexte unabhängig von der Schwierigkeitsstufe lösen konnte. Zusätzlich wird das kooperative Arbeiten durch das gegenseitige Schreiben von Nachrichten unterstützt. Durch die verschiedenen Materialien wird eine Methodenvielfalt erzeugt, die unterschiedliche Repräsentationsebenen anspricht. Mit diesem Angebot sollte es allen Schülerinnen und Schülern möglich sein, in ihrem jeweiligen Lerntempo die Stationen erfolgreich und abwechslungsreich zu bearbeiten.

Die Stationen des SpionCamps sind jedoch nicht nur als Stationenlernen verwendbar. Lehrkräfte können gezielt einzelne Stationen mit ihren Kursen bearbeiten oder beim Stationenlernen auslassen. Alle Materialien sind zusätzlich an die Lerngruppe und ihr Wissen anpassbar. Einige Schülerinnen und Schüler können bereits Vorwissen zur Kryptologie aufweisen, wenn sie beispielsweise eine Grundschule mit integriertem Informatikunterricht besucht haben. Das SpionCamp bietet die Möglichkeit einer Differenzierung an. Bestimmte Themen können auch schon in niedrigeren Stufen verwendet werden, wie man am Modul *Ich habe ein Geheimnis!* aus Kapitel 3.3.2 sieht. Das Material ist somit vielfältig einsetzbar und erleichtert den Lehrkräften die Unterrichtsvorbereitung.

Kapitel 4 hat gezeigt, dass die erstellten Stationen aufgrund ihrer neuen Thematik und Einsatzmöglichkeiten eine gute Ergänzung zum SpionCamp sind. Sie stellen Verfahren dar, die dem Wunsch nach anspruchsvolleren Stationen für die Sekundarstufe II gerecht werden. Bei der Blockverschlüsselung wurde zwar der unsicherste Modus gewählt, dieser wird jedoch teilweise noch angewandt. Er bietet somit eine einfache Grundlage für das Verständnis aller Blockverschlüsselungen. Die Schülerinnen und Schüler erkennen leichter, wieso Nachrichten in Blöcke unterteilt werden und verstehen im späteren Verlauf des Unterrichts den DES-Algorithmus schneller. Die Binärdarstellung wurde bewusst durch die einfache Darstellung der Buchstaben ersetzt, um eine erfolgreiche Bearbeitung der Aufgaben dieser Station zu ermöglichen. Dadurch müssen Buchstaben nicht als ihre Darstellung im Binärsystem geschrieben werden, was Hindernisse durch fehlendes Wissen vermeidet.

Bei der Stromverschlüsselung wurde ebenfalls ein einfaches Verfahren ohne Binärdarstellung gewählt. Dieses verwendet keinen Zufallszahlengenerator, endlichen Automaten sowie Schlüsselstromgeneratoren, die komplexen Funktionen entsprechen. Der Umgang mit den Ordinalzahlen der Buchstaben ist dennoch im SpionCamp alleinstehend. Diese Ordinalzahlen werden in der Wissenschaft häufig benutzt und bieten eine Grundlage für andere Verfahren. Durch die Verbindung mit der Vigenère-Station verstehen die Schülerinnen und Schüler das Prinzip der Autokey-Verschlüsselung schneller und können dieses Prin-

zip auch mit einem Schlüsselwort durchführen. Das Erkunden weiterer Stromverschlüsselungen kann so vorbereitet werden.

Durch die Erprobung der Stationen wurden einige Verbesserungen aufgezeigt. Es wäre auch spannend zu sehen, welche Kompetenzen die Schülerinnen und Schüler durch die Bearbeitung der Stationen entwickelt oder ausgebaut haben. Unser Ziel richtete sich allerdings vordringlich auf die Erprobungen der Verständlichkeit und Durchführbarkeit der neuen Stationen. Da die Gruppen sehr klein waren, wäre eine weitere Evaluation der neuen oder aller Stationen sinnvoll. Es konnte jedoch bereits an den kleinen Gruppen beobachtet und durch die Evaluation bestätigt werden, dass die Station zur Blockverschlüsselung gut umgesetzt war. Den Schülerinnen und Schülern machten die Aufgaben Spaß und sie verstanden das Prinzip sowie die Ausführung schnell. Bei der Stromverschlüsselung gab es einige Schwierigkeiten, die jedoch durch die Verbesserungen größtenteils beseitigt sein sollten. Schülerinnen und Schüler, die das Prinzip sehr schnell verstehen, können die Tabelle auf dem Arbeitsblatt zum Rechnen verwenden. Die anderen haben es durch größere Abstände, weniger Buchstabenbänder sowie den Wegfall der Leerzeichen einfacher, mit dem Stromverschlüsseler umzugehen. An beiden Stationen wurde die erste Aufgabe mit einem deutlich anleitenderen Charakter umgestaltet. Dadurch soll den Schülerinnen und Schülern der Einstieg in die Aufgaben erleichtert werden.

Durch die Bearbeitung der Stationen des SpionCamps können viele der in den Bildungsplänen (sowohl der Kernlehrpläne – als auch der Empfehlungen für Bildungsstandards der GI) ausgewiesenen Kompetenzen umgesetzt und angestrebt werden (siehe Kapitel 2). Deswegen sind sie eine gute Grundlage für die Bearbeitung von Fragenstellungen aus der Kryptologie. Eine Vollabdeckung der für die Kryptologie einzulösenden Kompetenzen erfordert allerdings noch die Ausgestaltung weiterer Elemente. Einige Kompetenzen werden bereits von Materialien anderer Institutionen abgedeckt, die ergänzend zum SpionCamp oder nach der Durchführung des SpionCamps aufbauend genutzt werden können. Diese Liste ist natürlich nicht vollständig, sondern umfasst nur ausgewählte Beispiele.

- Die Sensibilisierung der Schülerinnen und Schüler ist nicht als Station realisierbar, da sie über eigene sensible Daten nachdenken müssen. Für dieses Thema gibt es jedoch Material von anderen Institutionen. Der Chaos Computer Club e. V. hat beispielsweise ein Stammdaten-Spiel entwickelt, bei dem die Schülerinnen und Schüler persönliche Daten in verschiedene Privatsphärestufen einsortieren und Möglichkeiten, zum Schutz dieser diskutieren (vgl. Chaos macht Schule, 2019). Ein anderes Beispiel ist ein Modul zu Passwörtern der MedienMonster e. V., in dem die Schülerinnen und Schüler Grundlagen von Datenschutz und Datensicherung ver-

stehen, Verschlüsselungsverfahren kennenlernen und sichere Passwörter erzeugen (vgl. Schmidt-Dransfeld und Velten, 2018). Ein weiteres Modul zur Passwortsicherheit wurde an der Universität Münster erstellt. Schülerinnen und Schüler der dritten Klasse verwenden die Idee eines Automaten, um ein sicheres Passwort auszuwählen (Krzyzek, 2018).

- Das Entwickeln eigener Vereinbarungen ist schwierig als eigene Station zu formulieren, weil es Kreativität verlangt. In dem neuen Modul zur Kryptologie für die Erprobungsstufe soll dies jedoch in einer Unterrichtseinheit getan werden (vgl. Schmid, 2019).
- Die Einführung der Sicherheitsziele *Vertraulichkeit*, *Verfügbarkeit*, *Authentizität* und *Integrität* kann nur als Definition angegeben werden. Dies entspricht nicht dem Prinzip des *entdeckenden Lernens*.
- Über das SpionCamp hinausgehend, kann der Einsatz von Informatiksystemen dazu beitragen, die Codierung für die Verarbeitung der Daten mit einem Informatiksystem deutlicher darzustellen.
- Asymmetrische Verschlüsselungen und Signaturen sind sehr komplex und ohne Informatiksysteme nur umständlich berechenbar. Sie eignen sich somit besser für eine Behandlung im nachfolgenden Unterricht.
- Aktuelle Anwendungskontexte können aufgrund der Aktualität nicht als Material des SpionCamps vorbereitet werden.

Interessierte Schülerinnen und Schüler können außerdem abseits vom Unterricht ihr Interesse stärken. Das Buch *Codes* (Singh, 2002) von SINGH ist eine Jugendbuchfassung seines Buches *Geheime Botschaften* (Singh, 2000). Es stellt neben historischen und modernen Verfahren der Kryptologie auch geschichtliche Hintergründe dar. Der Film *Imitation Game* (Universum Film, 2015) ist außerdem eine gute Ergänzung, wenn bereits erstes Wissen zur Enigma vorhanden ist.

Die Kryptologie ist eines der Themen in der Informatik, an dem viele Schülerinnen und Schüler Freude haben. Dieses Vergnügen sollte durch den Unterricht und das verwendete Material unterstützt und nicht eingedämmt werden. Ein spielerischer Umgang wie im SpionCamp ist eine großartige Möglichkeit, die Schülerinnen und Schüler für die Informatik zu begeistern.



Die Buchstaben bleiben, **was** sie sind, aber nicht, **wo** sie sind.
Solche Verschlüsselungen heißen **Transposition**. (Das Wort *Transposition* ist abgeleitet vom lateinischen Wort *transponere* = verschieben.)

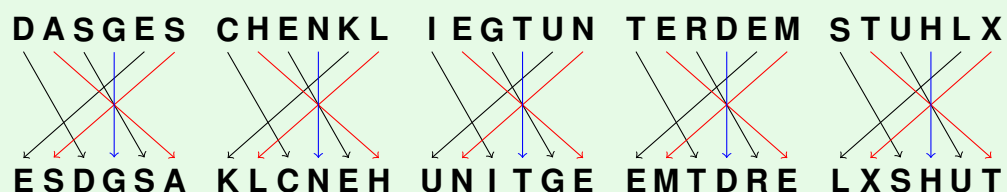
Bei einer Blockverschlüsselung wird eine Nachricht ohne Leerzeichen in Blöcke einer festen Länge unterteilt. Ist die Nachricht zu kurz, werden Füllbuchstaben ans Ende gesetzt. Es gibt verschiedene Möglichkeiten, die Blöcke zu verschlüsseln. Wir betrachten den Modus *Elektronic Code Book (ECB)*, bei dem jeder Block von den anderen unabhängig verschlüsselt wird. Dafür benutzen wir als Schlüssel Permutationen. Eine Permutation vertauscht die Buchstaben eines Textes auf eine vorgegebene Weise. Dabei schreiben wir die Permutation auf, indem wir die neuen Stellen der Buchstaben unter die alten Stellen schreiben.

Beispiel Für die Blocklänge 6 und die Permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 4 & 1 & 2 \end{pmatrix}$$

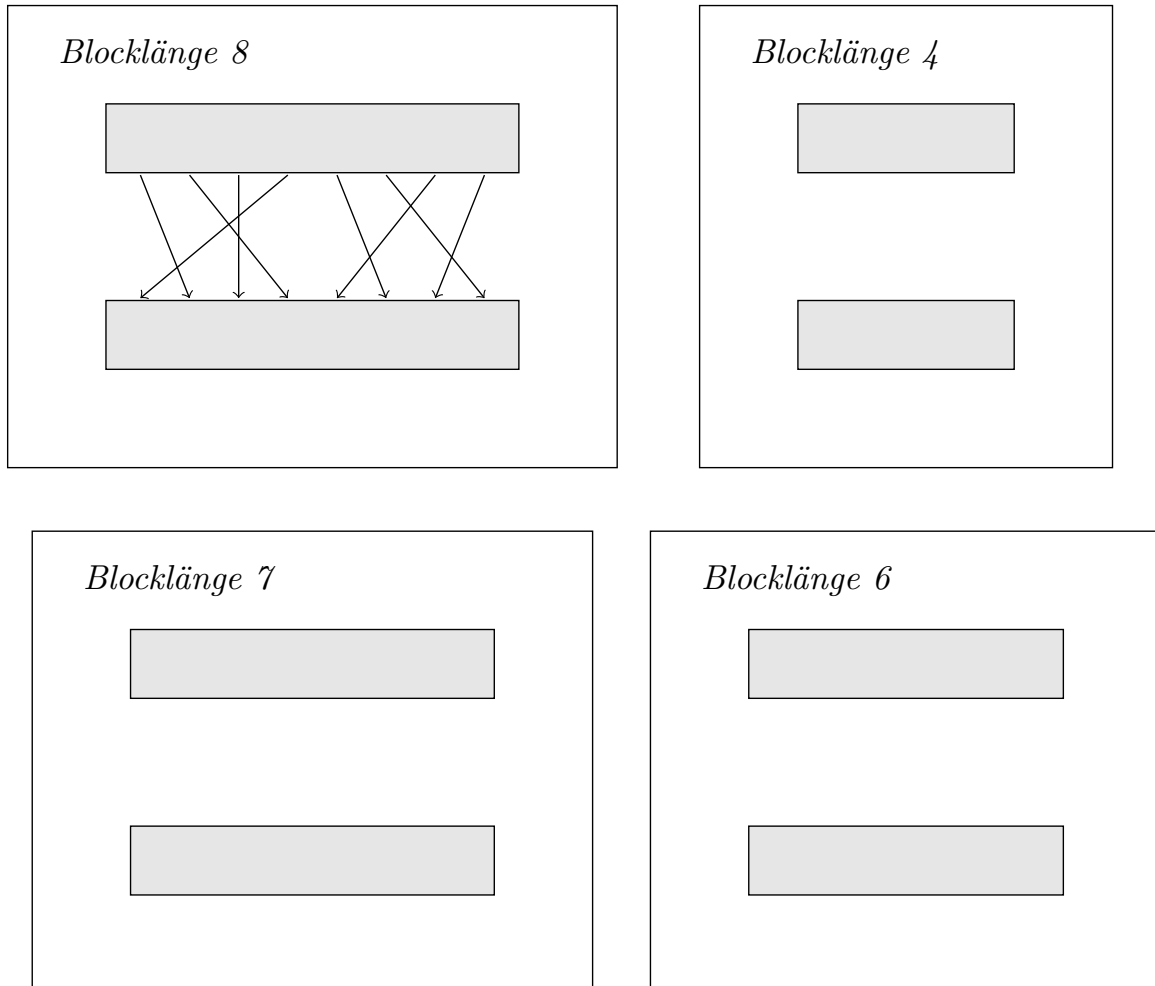
schreiben wir den ersten Buchstaben auf die dritte Stelle, den zweiten Buchstaben auf die sechste Stelle, den dritten Buchstaben auf die fünfte Stelle, den fünften Buchstaben auf die erste Stelle und den sechsten Buchstaben auf die zweite Stelle. Der vierte Buchstabe bleibt dabei einfach stehen.

Also wird die Nachricht **DAS GESCHENK LIEGT UNTER DEM STUHL** verschlüsselt zu **ESDGS AKLCNEHUNITGEEMTDRELXSHUT**. Dies sieht man besser, wenn man die Nachricht in Blöcke einteilt und mit Pfeilen zeigt, welche Buchstaben an welche Stellen geschoben werden:



Die Anordnung der Pfeile einer Permutation bleibt bei jedem Block gleich. Deswegen können wir die Permutationshilfen nutzen, um Nachrichten schneller und korrekt zu verschlüsseln. Dabei ist es wichtig, dass du die Buchstaben nicht zu nah aneinander schreibst. Nutze dafür die Vorlage für Texte und schreibe in jedes Kästchen genau einen Buchstaben. Lege dann die Permutationshilfe der richtigen Blocklänge mit dem oberen Fenster auf den Block des Klartextes und schreibe die Buchstaben dann entsprechend der Pfeile in das untere Fenster.

Vorlage für Permutationshilfen



Die Permutationshilfen und die Fenster (die dunklen Felder) ausschneiden und laminieren. Anschließend die Fenster wieder ausschneiden, damit durch sie geschrieben werden kann. Auf die laminierten Oberflächen können dann die Permutationen geschrieben werden.

This image shows a full page of blank graph paper. The grid consists of small, equal-sized squares formed by thin black lines. There are 20 columns and 20 rows of squares, creating a total of 400 square units. The grid covers the entire area of the page, leaving no margins or additional markings.

Aufgabe 1 Nimm dir die Permutationshilfe mit Blocklänge 8 und der aufgezeichneten Permutation. Verschlüssele **WIR TREFFEN UNS UM DREI UHR**, indem du Leerzeichen auslässt und Füllbuchstaben am Ende der Nachricht einfügst.

Aufgabe 2 Beschreibe, wie du eine empfangene Nachricht mit bekanntem Schlüssel (Permutation) entschlüsseln kannst.

Aufgabe 3 Entschlüssele die Nachricht **TDREFRFEKPNUSTTIAAHMNFDE** mit dem vorgegebenen Schlüssel auf der Permutationshilfe mit Blocklänge 8.

Aufgabe 4 Zeichne die Permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 1 & 6 & 5 \end{pmatrix}$$

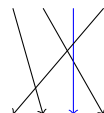
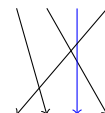
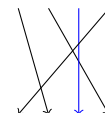
mit einem Folienstift auf die Permutationshilfe mit Blocklänge 6. Nutze dafür die Vorlage für Texte, um die Pfeile der Permutation richtig einzuzeichnen. Verschlüssele eine kurze Nachricht und lasse sie von jemandem entschlüsseln.

Aufgabe 5 Wählt eine Blocklänge (mit dazugehörige Permutationshilfe) und einen eigenen Schlüssel (Permutation) aus und schreibt euch gegenseitig eine Nachricht.

Aufgabe 6 Welche Schlüssel (Permutationen) sind mit Blocklänge 2 und 3 möglich?

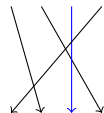
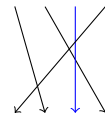
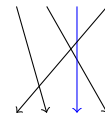
Hinweis: Säubere die Permutationshilfen bitte nach Abschluss deiner Bearbeitung, damit die oder der Nächste von neu beginnen kann.

Lösung 1 Durch verschiedene Füllbuchstaben kann der letzte Block variieren. Die Lösung kann zum Beispiel so aussehen:

W I R T R E F F	E N U N S U M D	R E I U H R A B
		
T W R I F R F E	N E U N M S D U	U R I E A H B R

Lösung 2 Das Verfahren ist umgekehrt zum Verschlüsselungsvorgang. Man teilt die Nachricht in Blöcke der bekannten Länge und wendet den Schlüssel (= Permutation) umgekehrt an. Das bedeutet, die Permutation wird von unten nach oben gelesen. Bei der Permutationshilfe legt man das untere Fenster auf die Nachricht und schreibt die Buchstaben dann entsprechend gegen die Pfeilrichtung in das obere Fenster.

Lösung 3 Die entschlüsselte Nachricht lautet **DER TREFFPUNKT IST AM HAFEN**.

D E R T R E F F	P U N K T I S T	A M H A F E N D
		
T D R E F R F E	K P N U S T T I	A A H M N F D E

Lösung 4 Zu dieser Aufgabe gibt es keine allgemeine Lösung.

Lösung 5 Zu dieser Aufgabe gibt es keine allgemeine Lösung.

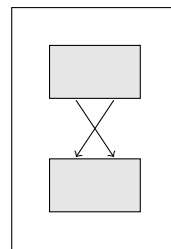
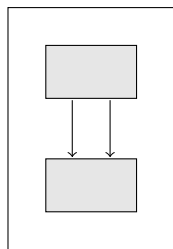
Lösung

6

Für die Blocklänge 2 gibt es zwei Schlüssel (Permutation), aber nur eine davon ist für eine Verschlüsselung sinnvoll. Die beiden Buchstaben werden dabei einfach vertauscht. Die Permutationen sehen so aus:

$$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

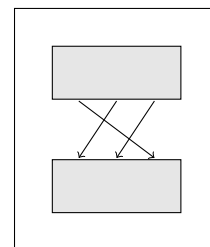
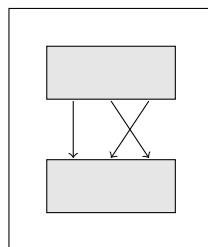
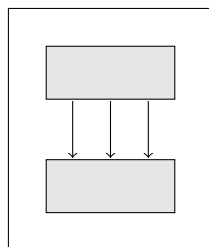


Für die Blocklänge 3 gibt es 6 mögliche Schlüssel (Permutationen). Dabei ist wieder eine nicht sinnvoll:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

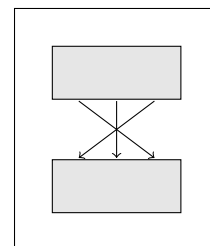
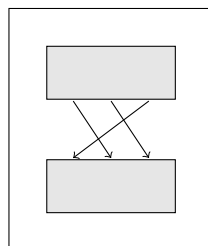
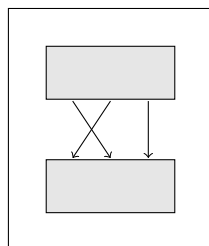
$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$



$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$





Die Buchstaben bleiben, **wo** sie sind, aber nicht, **was** sie sind. Solche Verschlüsselungen heißen **Substitution**. (Das Wort *Substitution* ist abgeleitet vom lateinischen Wort *substituere* = ersetzen.)

Bei einer Stromverschlüsselung benötigt man einen Startschlüssel. Aus dem Startschlüssel entsteht zusammen mit dem Klartext ein Schlüsselstrom. Das heißt eine Reihe von Schlüsseln, wovon wir uns aber nur den Startschlüssel merken müssen.

Wir betrachten den speziellen Fall der Autokey-Verschlüsselung. Diese wurde, wie die Vigenère-Verschlüsselung, vom Franzosen Blaise de Vigenère (1523 bis 1596, s. Bild) entwickelt. Bei der Autokey-Verschlüsselung wird an den Startschlüssel der Klartext gehangen. Also werden die einzelnen Buchstaben zum Schlüssel für folgende Buchstaben.



Hinweis: Solltest du die Vigenère-Station noch nicht bearbeitet haben, macht es Sinn, dies zuerst zu tun, damit du Verbindungen ziehen kannst. Ansonsten wirst du das erste Beispiel nicht verstehen, kannst diese Station aber trotzdem weiter bearbeiten.

Beispiel

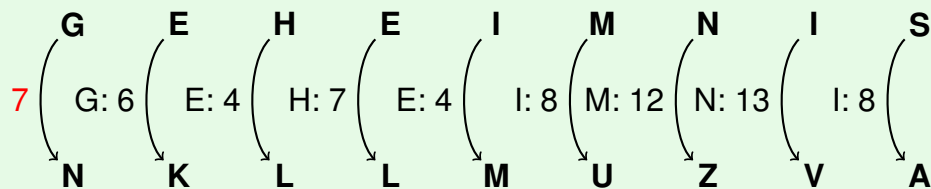
Mit dem Schlüssel **GEHEIM** können wir die Nachricht mit dem Vigenère-Quadrat verschlüsseln. Dafür verschlüsseln wir die ersten Buchstaben mit dem Schlüsselwort und die folgenden Buchstaben mit dem Klartext von Anfang an.

Nachricht:	DAS TREFFEN IST UM ACHT UHR
Schlüsselwort:	GEH EIM DAST REF FE NIST UMA
Geheimtext:	JEZ XZQIFWG ZWY ZQ NKZM OTR

Da wir das Arbeiten mit dem Vigenère-Quadrat jedoch bereits bei der Vigenère-Station gelernt haben, schauen wir uns eine weitere Möglichkeit für die Ver- und Entschlüsselung an. In der Wissenschaft wird häufig mit Zahlen anstatt mit Buchstaben gearbeitet. Dies vereinfacht vor allem die Arbeit mit Informatiksystemen. Außerdem veranschaulicht es besser, wieso die Autokey-Verschlüsselung als Stromverschlüsselung bezeichnet wird. Als Hilfsmittel verwenden wir den Stromverschlüsseler. Dieser zeigt dir die Stellen der einzelnen Buchstaben im Alphabet. Dabei fangen wir immer bei 0 an zu zählen. Deswegen wird der Buchstabe **A** mit der Stelle **0** gleichgesetzt.

Beispiel

Als Startschlüssel ist die Zahl **7** gewählt und unsere Nachricht lautet **GEHEIMNIS**. Nun stellen wir die Nachricht in den Stromverschlüsseler ein, indem wir die Buchstabenbänder so drehen, dass die Buchstaben in den ausgeschnittenen Fenstern unserer Nachricht entsprechen. Wir fangen von vorne an, die Buchstabenbänder jeweils um den passenden Schlüssel weiter zu drehen. Wir schieben also den ersten Buchstaben **G** 7 Stellen weiter und erhalten ein **N**. Dann schieben wir den zweiten Buchstaben **E** um die Stelle vom ersten Klartext weiter, also 6 Stellen, da G an der sechsten Stelle im Alphabet liegt, und landen bei **K**. Nun nehmen wir uns den dritten Buchstaben und schieben ihn um die Stelle vom zweiten Klartextbuchstaben weiter. Dies machen wir so lange, bis wir alle Buchstaben verschlüsselt haben.

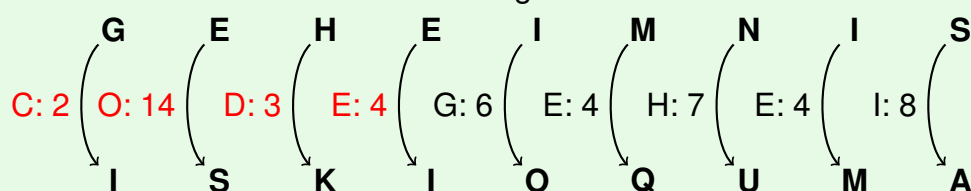


Unser Geheimtext lautet somit **NKLLMUZVA**.

Die »normale« Autokey-Verschlüsselung ist ziemlich leicht zu »knacken«. Etwas schwieriger wird es, wenn das Verfahren mit einem Startschlüssel aus mehreren Zahlen kombiniert wird. Um sich den Startschlüssel einfacher merken zu können, kann man auch ein Schlüsselwort wählen. Die Buchstaben des Schlüsselwortes werden wieder in Zahlen umgewandelt.

Beispiel

Unser Startschlüssel ist jetzt **CODE**, was den Zahlen **2 14 3 4** entspricht, und unsere Nachricht lautet wieder **GEHEIMNIS**. Dann stellen wir die Nachricht in den Stromverschlüsseler ein und verschlüsseln zuerst die ersten vier Buchstaben mit unserem Schlüsselwort und die folgenden wie eben mit den Klartextbuchstaben der Nachricht von Anfang an.



Unser Geheimtext lautet also **ISKIOQUMA**.

0	A	0
1	B	1
2	C	2
3	D	3
4	E	4
5	F	5
6	G	6
7	H	7
8	I	8
9	J	9
10	K	10
11	L	11
12	M	12
13	N	13
14	O	14
15	P	15
16	Q	16
17	R	17
18	S	18
19	T	19
20	U	20
21	V	21
22	W	22
23	X	23
24	Y	24
25	Z	25

0	A	0
1	B	1
2	C	2
3	D	3
4	E	4
5	F	5
6	G	6
7	H	7
8	I	8
9	J	9
10	K	10
11	L	11
12	M	12
13	N	13
14	O	14
15	P	15
16	Q	16
17	R	17
18	S	18
19	T	19
20	U	20
21	V	21
22	W	22
23	X	23
24	Y	24
25	Z	25

0	A	0
1	B	1
2	C	2
3	D	3
4	E	4
5	F	5
6	G	6
7	H	7
8	I	8
9	J	9
10	K	10
11	L	11
12	M	12
13	N	13
14	O	14
15	P	15
16	Q	16
17	R	17
18	S	18
19	T	19
20	U	20
21	V	21
22	W	22
23	X	23
24	Y	24
25	Z	25

0	A	0
1	B	1
2	C	2
3	D	3
4	E	4
5	F	5
6	G	6
7	H	7
8	I	8
9	J	9
10	K	10
11	L	11
12	M	12
13	N	13
14	O	14
15	P	15
16	Q	16
17	R	17
18	S	18
19	T	19
20	U	20
21	V	21
22	W	22
23	X	23
24	Y	24
25	Z	25

0	A	0
1	B	1
2	C	2
3	D	3
4	E	4
5	F	5
6	G	6
7	H	7
8	I	8
9	J	9
10	K	10
11	L	11
12	M	12
13	N	13
14	O	14
15	P	15
16	Q	16
17	R	17
18	S	18
19	T	19
20	U	20
21	V	21
22	W	22
23	X	23
24	Y	24
25	Z	25

0 A₀
1 B₁
2 C₂
3 D₃
4 E₄
5 F₅
6 G₆
7 H₇
8 I₈
9 J₉
10 K₁₀
11 L₁₁
12 M₁₂
13 N₁₃
14 O₁₄
15 P₁₅
16 Q₁₆
17 R₁₇
18 S₁₈
19 T₁₉
20 U₂₀
21 V₂₁
22 W₂₂
23 X₂₃
24 Y₂₄
25 Z₂₅

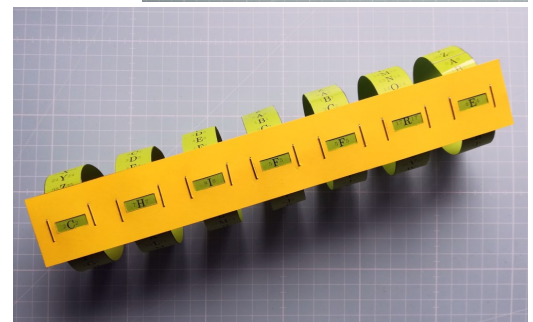
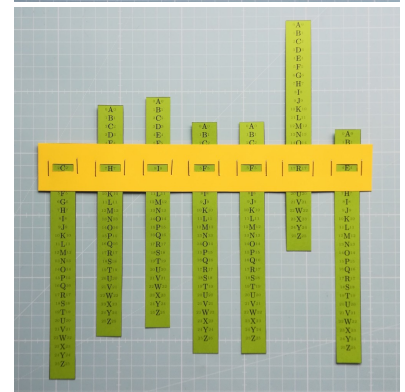
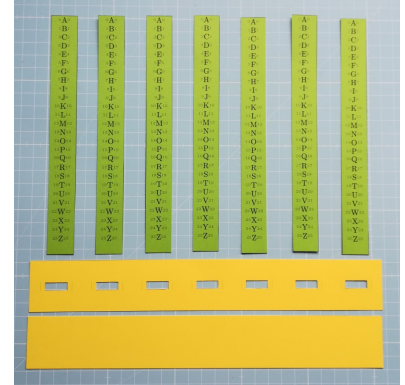
0 A⁰
1 B¹
2 C²
3 D³
4 E⁴
5 F⁵
6 G⁶
7 H⁷
8 I⁸
9 J⁹
10 K¹⁰
11 L¹¹
12 M¹²
13 N¹³
14 O¹⁴
15 P¹⁵
16 Q¹⁶
17 R¹⁷
18 S¹⁸
19 T¹⁹
20 U²⁰
21 V²¹
22 W²²
23 X²³
24 Y²⁴
25 Z²⁵



Bastelanleitung

Du benötigst zusätzlich zum ausgedruckten Material einen Tacker und Klebeband.

- Schneide die Buchstabenbänder aus. Bei Papier sollte der schwarze Rand noch zu sehen sein, bei Pappe nicht mehr. Dann passen die Bänder gut in die dafür vorgesehenen Plätze.
- Schneide die beiden Rechtecke aus und trenne die Fenster (die dunklen Felder) heraus.
- Lege die beiden Rechtecke übereinander und tackere sie an den gepunkteten Linien zusammen.
- Schiebe die Buchstabenbänder zwischen die Tackernadeln und prüfe, ob man die Bänder gut durchziehen kann. Schneide sie, wenn benötigt, etwas dünner aus.
Der Stromverschlüsseler kann bereits jetzt verwendet werden, wenn er platzsparender aufbewahrt werden muss, da die Verschiebung trotzdem durchgeführt werden kann.
- Klebe die Bänder mit Klebeband an den Enden so zusammen, dass **A** direkt **Z** folgt. Nutze die freie Fläche dabei als Klebefläche. Prüfe wieder, ob man die Bänder auch bei den Klebeflächen gut durchziehen kann.



Aufgabe Verschlüssele **FOLGE DEM PFEIL** mit dem Startschlüssel **16**.

1 Stelle dazu zuerst die ersten sieben Buchstaben im Stromverschlüsseler ein, sodass du sie in den Fenstern sehen kannst. Verschlüssele den ersten Buchstaben mit dem Startschlüssel **16** und die darauf folgenden mit dem jeweiligen vorherigen Klartextbuchstaben.

Aufgabe Beschreibe, wie du eine empfangene Nachricht mit bekanntem Startschlüssel entschlüsseln kannst.

2

Aufgabe Entschlüssele die Nachricht **JHVJUJHTSHALBUEUJYRNX** mit dem Startschlüssel **6**.

3

Aufgabe Warum ist dieses Verschlüsselungsverfahren leicht zu »knacken«?

4

Aufgabe Wählt einen Startschlüssel aus mehreren Zahlen und schreibt euch gegenseitig eine Nachricht.

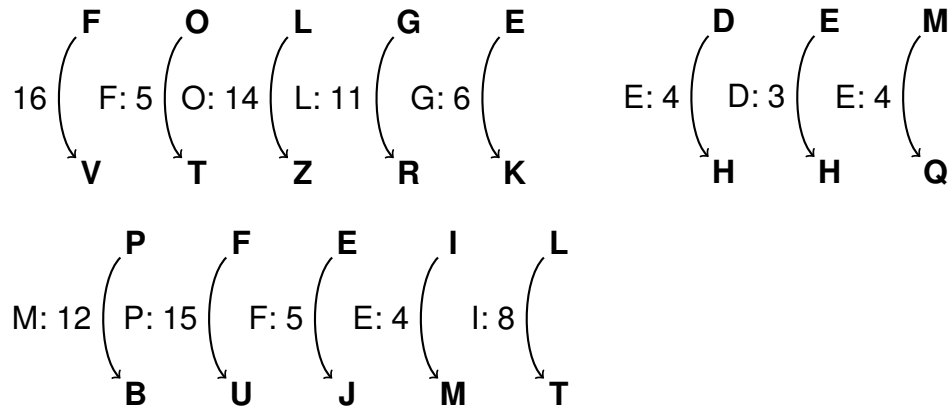
5

Aufgabe Was passiert beim Ver- und was beim Entschlüsseln, wenn du einen Buchstaben um ein Stelle zu weit schiebst?

6

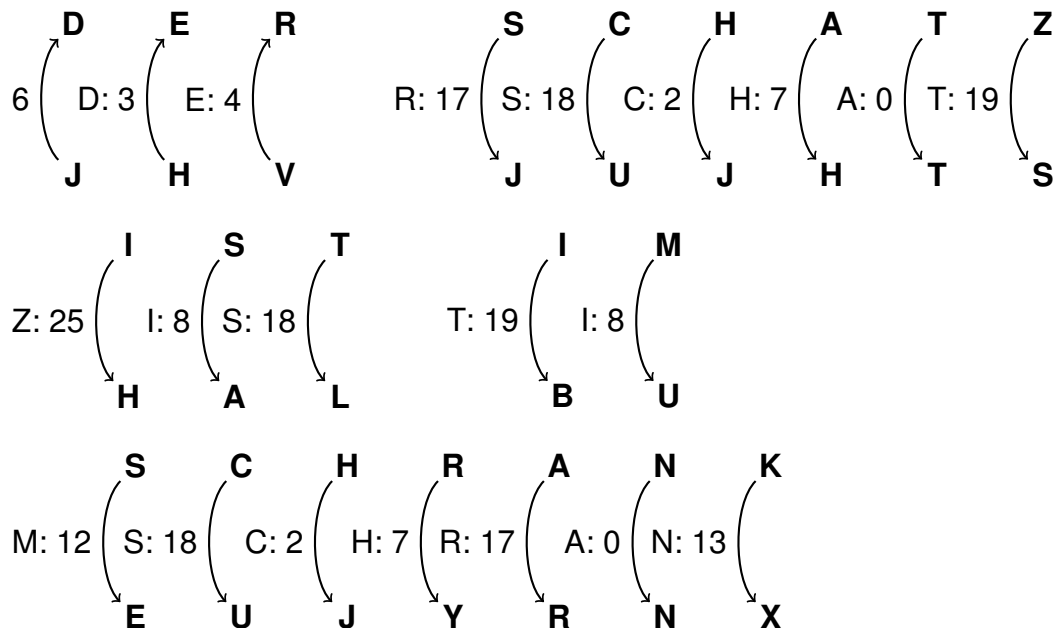
Buchstabe	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Stelle	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Lösung 1 Die Geheimnachricht lautet **VTZRKHHRCUJMTPR**. Die Verschlüsselung sieht so aus:



Lösung 2 Das Verfahren ist umgekehrt zum Verschlüsselungsvorgang. Man fängt ebenfalls vorne mit dem Startschlüssel an und schiebt die Buchstaben einzeln mit dem passenden Schlüssel zurück. Dabei verwendet man jeweils den entschlüsselten Klartextbuchstaben als nächsten Schlüssel. Die Stromverschlüsselungshilfe zeigt dir direkt den nächsten Schlüssel neben dem Buchstaben an.

Lösung 3 Der Klartext lautet **DER SCHATZ IST IM SCHRANK**. Die Entschlüsselung sieht so aus:





Lösung 4 Das Verfahren ist leicht zu »knacken«, da man höchstens 26 Startschlüssel durchprobieren muss, um die Lösung zu erhalten.

Lösung 5 Zu dieser Aufgabe gibt es keine allgemeine Lösung.

Lösung 6 Beim Verschlüsseln merkt man nicht, wenn man einen Buchstaben zu weit verschoben hat, da nur der dazugehörige Buchstabe des Geheimtextes fehlerhaft wird. Allerdings führt dieser Fehler bei der Entschlüsselung dazu, dass der komplette darauf folgende Klartext falsch entschlüsselt wird. Dies liegt daran, dass der Schlüsselstrom an einer Stelle einen zu hohen Schlüssel aufweist und sich das auf alle weiteren Schlüssel auswirkt.

Welche Stationen hast du bearbeitet?

- | | | | |
|--|---|--|---|
| ☐ Rotoren | ☐ Strom-Chiffre | ☐ Block-Chiffre | ☐ Buchstabenhäufigkeit |
| ☐ Steganographie Text | ☐ Caesar | ☐ Vigenère | ☐ Freimaurer-Chiffre |
| ☐ Playfair | ☐ Diffie-Hellman | ☐ Pflügen | ☐ Skytale |
| ☐ Schablonen | ☐ Morsealphabet | ☐ Braille-Schrift | ☐ Winkeralphabet |
| ☐ Steganographie Bild | | | |

Welche Stationen haben dir besonders gut gefallen und warum?**Welche Stationen haben dir weniger gut gefallen und warum?****An welchen Stationen fandest du das Material hilfreich?****Welche Stationen fandest du zu leicht oder zu schwierig?**

Zu leicht:

Zu schwierig:

Welche Stationen waren zu zeitaufwendig?

Hat dir die Grafik am Whiteboard geholfen, dich zurechtzufinden?

- ☐ Ja ☐ Ich weiß nicht ☐ Nein

Wie gefiel dir die Station zur Strom-Chiffre?

- ☐ Sehr gut ☐ Gut ☐ Mittel ☐ Schlecht ☐ Sehr schlecht

Was gefiel dir an der Station zur Strom-Chiffre besonders gut oder schlecht?

gut:

schlecht:

Wie gefiel dir die Station zur Block-Chiffre?

- ☐ Sehr gut ☐ Gut ☐ Mittel ☐ Schlecht ☐ Sehr schlecht

**Haben dir die Vorlagen für Texte geholfen, die Aufgaben zu erledigen?
(Block-Chiffre und Schablonen)**

- ☐ Ja ☐ Ich weiß nicht ☐ Nein

Was gefiel dir an der Station zur Block-Chiffre besonders gut oder schlecht?

gut:

schlecht:

Wie viel Vorwissen hattest du zur Kryptologie?

- ☐ Sehr viel ☐ Viel ☐ Mittel ☐ Wenig ☐ Keins

Wie viel weißt du nun zur Kryptologie?

- ☐ Sehr viel ☐ Viel ☐ Mittel ☐ Wenig ☐ Nichts

Was könnte verbessert werden?

Welche Stationen hast du bearbeitet?

- | | | | |
|--|---|---|--|
| ☐ Strom-Chiffre | ☐ Block-Chiffre | ☐ Buchstabenhäufigkeit | ☐ Steganographie Text |
| ☐ Rotoren | ☐ Caesar | ☐ Vigenère | ☐ Freimaurer-Chiffre |
| ☐ Playfair | ☐ Diffie-Hellman | ☐ Pflügen | ☐ Skytale |
| ☐ Schablonen | ☐ Morsealphabet | ☐ Braille-Schrift | ☐ Winkeralphabet |
| ☐ Steganographie Bild | | | |

Welche Stationen haben dir besonders gut gefallen und warum?**Welche Stationen haben dir weniger gut gefallen und warum?****An welchen Stationen fandest du das Material hilfreich?****Welche Stationen fandest du zu leicht oder zu schwierig?**

Zu leicht:

Zu schwierig:

Welche Stationen waren zu zeitaufwendig?

Wie gefiel dir die Station zur Strom-Chiffre?

- ☐ Sehr gut ☐ Gut ☐ Mittel ☐ Schlecht ☐ Sehr Schlecht

Wie lange hast du an der Station zur Strom-Chiffre gearbeitet?

- ☐ Sehr lange ☐ Lange ☐ Genau richtig ☐ Kurz ☐ Zu kurz

Hat dir das Material an der Station zur Strom-Chiffre geholfen?

- ☐ Ja ☐ Ein wenig ☐ Zu wenig ☐ Nein

Was gefiel dir an der Station zur Strom-Chiffre besonders gut oder schlecht?

gut:

schlecht:

Wie gefiel dir die Station zur Block-Chiffre?

- ☐ Sehr gut ☐ Gut ☐ Mittel ☐ Schlecht ☐ Sehr schlecht

Wie lange hast du an der Station zur Block-Chiffre gearbeitet?

- ☐ Sehr lange ☐ Lange ☐ Genau richtig ☐ Kurz ☐ Zu kurz

Hat dir das Material an der Station zur Block-Chiffre geholfen?

- ☐ Ja ☐ Ein wenig ☐ Zu wenig ☐ Nein

Hat dir die Vorlage für Texte geholfen, die Aufgaben zu erledigen?

- ☐ Ja ☐ Ich weiß nicht ☐ Nein

Was gefiel dir an der Station zur Block-Chiffre besonders gut oder schlecht?

gut:

schlecht:

Was könnte verbessert werden?

Literatur

- Aust, Anne-Katrin, Dorothee Müller und Peter Gabriel (2011). „SpionCamp – Kryptographie als Stationenlernen“. In: *Informatik mit Kopf, Herz und Hand – Praxisbeiträge zur 14. GI-Fachtagung Informatik und Schule (INFOS 2011)*. Hrsg. von Michael Weigend, Marco Thomas und Frank Otte. Münster: ZfL-Verlag, S. 236–244. ISBN: 978-3-86877-009-4. URL: <https://t1p.de/rf5t> (besucht am 03.08.2019).
- Bauer, Friedrich L. (1997). *Entzifferte Geheimnisse. Methoden und Maximen der Kryptologie*. 2., erw. Aufl. Berlin, Heidelberg und New York: Springer-Verlag. ISBN: 3-540-62632-8.
- Bauer, Roland (1997). *Schülergerechtes Arbeiten in der Sekundarstufe I: Lernen an Stationen*. 1. Aufl. Berlin: Cornelsen Scriptor. ISBN: 3-589-21117-2.
- Buchmann, Johannes (2010). *Einführung in die Kryptographie*. 5. Aufl. Berlin, Heidelberg: Springer-Verlag. ISBN: 978-3-642-11185-3.
- Chaos macht Schule (März 2019). *Datenschutz. Stammdaten-Spiel*. URL: <https://t1p.de/bsah> (besucht am 03.08.2019).
- Didaktik der Informatik an der Bergischen Universität Wuppertal, Hrsg. (2019). *Informatik an Grundschulen. Schülerinnen und Schüler erwerben Informatikkompetenzen an Grundschulen – wir haben das Konzept und erproben es!* URL: <https://t1p.de/q11a> (besucht am 03.08.2019).
- Didaktik der Informatik an der Universität Paderborn, Hrsg. (2019). *Informatik an Grundschulen*. URL: <https://t1p.de/etw0> (besucht am 03.08.2019).
- Fachbereich C / Mathematik der Bergischen Universität Wuppertal, Hrsg. (2001). *Mathe-Prisma. Eine wachsende Modulsammlung zur Mathematik*. URL: <https://t1p.de/6r4u> (besucht am 03.08.2019).
- Frommer, Andreas, Stefanie Krivsky und P. Zöllner (2000). *Posterserie zum WMY2000*. Hrsg. von Fachbereich Mathematik Universität Wuppertal. WMY2000 – World Mathematical Year 2000. URL: <https://t1p.de/sck2> (besucht am 03.08.2019).
- Gesellschaft für Medien in der Wissenschaft (2001). *MEDIDA PRIX 2001. Mediendidaktischer Hochschulpreis*. URL: <https://t1p.de/tuu9> (besucht am 03.08.2019).
- GI, Hrsg. (Apr. 2008). *Grundsätze und Standards für die Informatik in der Schule – Bildungsstandards Informatik für die Sekundarstufe I*. Erarbeitet vom Arbeitskreis „Bildungsstandards“ – Beschluss des GI-Präsidiums vom 24. Januar 2008 – veröffentlicht als Beilage zur LOG IN 28 (2008) Heft 150/151. GI – Gesellschaft für Informatik e. V. URL: <https://t1p.de/xb2w> (besucht am 03.08.2019).
- Hrsg. (Apr. 2016). *Bildungsstandards Informatik für die Sekundarstufe II*. Erarbeitet vom Arbeitskreis „Bildungsstandards SII“ – Beschluss des GI-Präsidiums vom

29. Januar 2016 – veröffentlicht als Beilage zur LOG IN 36 (2016) Heft 183/184. GI – Gesellschaft für Informatik e. V. URL: <https://t1p.de/vxhy> (besucht am 03.08.2019).
- GI, Hrsg. (7. Feb. 2019). *Kompetenzen für informatische Bildung im Primarbereich. Empfehlungen der Gesellschaft für Informatik e. V.* Erarbeitet vom Arbeitskreis „Bildungsstandards Primarbereich“ – Beschluss des GI-Präsidiums vom 31. Januar 2019 – wird in gedruckter Form der LOG IN 39 (2019) Heft 191/192 beigelegt. GI – Gesellschaft für Informatik e. V. URL: <http://uni-w.de/1gm> (besucht am 03.08.2019).
- Humbert, Ludger u. a. (21. März 2019). *Handreichungen und Unterrichtsmaterial. Hinweise zur Schulung/Fortbildung.* Hrsg. von MSB-NW – Informatik an Grundschulen (IaG). MSB-NW – Ministerium für Schule und Bildung des Landes Nordrhein-Westfalen. URL: <https://t1p.de/iu9z> (besucht am 03.08.2019).
- International Mathematical Union (2000). *World Mathematical Year 2000. Launched by the International Mathematical Union (IMU) supported by UNESCO.* URL: <https://t1p.de/85q6> (besucht am 03.08.2019).
- Kontschinsky, Birgit (2003). „Stationenlernen“. In: *Methodenpool.* Hrsg. von Kersten Reich. Universität zu Köln. URL: <https://t1p.de/uor1> (besucht am 03.08.2019).
- Krzyzek, Sabine (Apr. 2018). *Woran und wie erkennt ein System ein gutes Kennwort (Kriterien, reguläre Sprache, Automat)?* URL: <https://t1p.de/c6j1> (besucht am 03.08.2019).
- MSB-NW, Hrsg. (6. Sep. 2018a). *Faktenblatt – G9 Stundentafel. Mehr Zeit und neue Spielräume für den Unterricht: Die Stundentafel für das neue G9 in NRW.* MSB-NW – Ministerium für Schule und Bildung des Landes Nordrhein-Westfalen. URL: <https://t1p.de/dj6n> (besucht am 03.08.2019).
- Hrsg. (19. Nov. 2018b). *Vierte Verordnung zur Änderung der Ausbildungs- und Prüfungsordnung Sekundarstufe I.* MSB-NW – Ministerium für Schule und Bildung des Landes Nordrhein-Westfalen. Düsseldorf. URL: <https://t1p.de/r4jb> (besucht am 03.08.2019).
- Hrsg. (Juli 2018c). *Zentralabitur 2019 – Informatik.* MSB-NW – Ministerium für Schule und Bildung des Landes Nordrhein-Westfalen. URL: <https://t1p.de/u15k> (besucht am 03.08.2019).
- Hrsg. (Juli 2018d). *Zentralabitur 2020 – Informatik.* MSB-NW – Ministerium für Schule und Bildung des Landes Nordrhein-Westfalen. URL: <https://t1p.de/sedh> (besucht am 03.08.2019).
- Hrsg. (31. Juli 2019a). *Kernlehrplan für die Sekundarstufe I Gymnasium in Nordrhein-Westfalen. Wahlpflichtfach Informatik.* MSB-NW – Ministerium für Schule und Bil-

- derung des Landes Nordrhein-Westfalen. URL: <https://t1p.de/xsv7> (besucht am 03.08.2019).
- MSB-NW, Hrsg. (2019b). *Zentralabitur 2021 – Informatik*. MSB-NW – Ministerium für Schule und Bildung des Landes Nordrhein-Westfalen. URL: <https://t1p.de/6ps3> (besucht am 03.08.2019).
- MSW-NW, Hrsg. (Aug. 2016). *Informatik an Grundschulen. Pilotprojekt zur Erprobung von Konzepten zur informatischen Bildung im Rahmen des Sachunterrichts an Grundschulen*. MSW-NW – Ministerium für Schule und Weiterbildung des Landes Nordrhein-Westfalen. URL: <http://IaG.nrw.de/> (besucht am 03.08.2019).
- Hrsg. (2008). *Richtlinien und Lehrpläne für die Grundschule in Nordrhein-Westfalen. Deutsch, Sachunterricht, Mathematik, Englisch, Musik, Kunst, Sport, Evangelische Religionslehre, Katholische Religionslehre*. 1. Aufl. Heft 2012. MSW-NW – Ministerium für Schule und Weiterbildung des Landes Nordrhein-Westfalen. Frechen: Ritterbach Verlag. ISBN: 978-3-89314-965-0. URL: <https://t1p.de/9v4m> (besucht am 03.08.2019).
- Hrsg. (2013). *Kernlehrplan Informatik für die gymnasiale Oberstufe*. MSW-NW – Ministerium für Schule und Weiterbildung des Landes Nordrhein-Westfalen. URL: <https://t1p.de/q58a> (besucht am 03.08.2019).
- (1. Nov. 2015a). *Kernlehrplan für die Gesamtschule/Sekundarschule in Nordrhein-Westfalen – Wahlpflichtfach Informatik*. MSW-NW – Ministerium für Schule und Weiterbildung des Landes Nordrhein-Westfalen. URL: <https://t1p.de/xhov> (besucht am 03.08.2019).
- (1. Nov. 2015b). *Kernlehrplan für die Realschule in Nordrhein-Westfalen – Wahlpflichtfach Informatik*. MSW-NW – Ministerium für Schule und Weiterbildung des Landes Nordrhein-Westfalen. URL: <https://t1p.de/8rxm> (besucht am 03.08.2019).
- Müller, Dorothee (Juli 2012). *SpionCamp-Stationen*. URL: <https://uni-w.de/1u> (besucht am 03.08.2019).
- (Apr. 2013). *Fünf „Informatik-Tricks“*. Wuppertal. URL: <https://uni-w.de/2p> (besucht am 03.08.2019).
- Müller, Dorothee u. a. (2019). „Interesse an Informatik und Informatikselbstkonzept zu Beginn der Sekundarstufe I des Gymnasiums – Eine empirische Untersuchung“. In: *Informatik für alle, INFOS 2019, 18. GI-Fachtagung Informatik und Schule, 16.–18. September 2019, Dortmund, Germany*. Hrsg. von Arno Pasternak. Bd. P288. LectureNotes in Informatics (LNI)-Proceedings. n. n. e.; Preprint-Version, die die eingereichte und angenommene Fassung darstellt und bis zur Veröffentlichung noch überarbeitet wird. Bonn: Gesellschaft für Informatik e. V. (GI), xx-yy. ISBN: 978-3-88579-682-4. URL: <http://uni-w.de/11t> (besucht am 03.08.2019).

- Müller, Jürgen (17. Juli 2018). *Cryptography*. Skript zur Vorlesung „Einführung in die Kryptographie“ im Sommersemester 2018 an der Bergischen Universität Wuppertal. URL: <https://t1p.de/szou> (besucht am 03.08.2019).
- Pasternak, Arno, Hrsg. (Sep. 2019). *Informatik für alle, INFOS 2019, 18. GI-Fachtagung Informatik und Schule, 16.–18. September 2019, Dortmund, Germany*. Bd. P288. LectureNotes in Informatics (LNI)-Proceedings. n. n. e. Bonn: Gesellschaft für Informatik e. V. (GI). ISBN: 978-3-88579-682-4.
- Pieper, Johannes und Dorothee Müller, Hrsg. (Juni 2013). *Material für den Informatikunterricht*. Arnsberg, Dortmund, Hamm, Wuppertal, Solingen. URL: <https://uni-w.de/1t> (besucht am 03.08.2019).
- QUA-LiS NRW, Hrsg. (11. Apr. 2014). *Beispiel für einen schulinternen Lehrplan zum Kernlehrplan für die gymnasiale Oberstufe Informatik (Stand: 01.06.2018)*. QUA-LiS: Qualitäts- und UnterstützungsAgentur – Landesinstitut für Schule. URL: <https://t1p.de/k1q5> (besucht am 03.08.2019).
- Hrsg. (21. Apr. 2016a). *Beispiel für einen schulinternen Lehrplan zum Kernlehrplan GE WP Informatik (Stand: 21.04.2016)*. QUA-LiS: Qualitäts- und UnterstützungsAgentur – Landesinstitut für Schule. URL: <https://t1p.de/eoh6> (besucht am 03.08.2019).
- Hrsg. (21. Apr. 2016b). *Beispiel für einen schulinternen Lehrplan zum Kernlehrplan RS WP Informatik (Stand: 21.04.2016)*. QUA-LiS: Qualitäts- und UnterstützungsAgentur – Landesinstitut für Schule. URL: <https://t1p.de/77da> (besucht am 03.08.2019).
- Reich, Kersten, Hrsg. (2003). *Methodenpool*. Universität zu Köln. URL: <https://t1p.de/fmnq> (besucht am 03.08.2019).
- Schmeh, Klaus (2013). *Kryptographie. Verfahren, Protokolle, Infrastrukturen*. 5., akt. Aufl. Heidelberg: dpunkt.Verlag. ISBN: 978-3-86490-015-0.
- Schmid, Vesna (25. Juli 2019). „Informatikunterricht in der Sekundarstufe I – von Anfang an. Datenstrukturen und Kryptologie als aufschließende Gegenstände“. Masterthesis. Wuppertal: Fachgebiet Didaktik der Informatik – Bergische Universität.
- Schmidt-Dransfeld, Erich und Marc Velten (Okt. 2018). *Unterrichtskonzept Passwörter. Von Datensicherung bis Passwortsafe*. Hrsg. von MedienMonster e. V. URL: <https://t1p.de/plf7> (besucht am 03.08.2019).
- Schülerlabor Informatik – InfoSphere, Hrsg. (2016). *NRW-Projekt „Informatik an Grundschulen“*. Kooperation mit der Uni Paderborn, der Uni Wuppertal und dem Schulministerium NRW. Aachen. URL: <https://t1p.de/9sx1> (besucht am 03.08.2019).

- Schwill, Andreas (1993). „Fundamentale Ideen der Informatik“. In: *ZDM* 25.1. *ZDM – Zentralblatt für Didaktik der Mathematik*, S. 20–31. ISSN: 0044-4103. URL: <http://t1p.de/ysq7> (besucht am 03.08.2019).
- Singh, Simon (2000). *Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internets*. München und Wien: Carl Hanser Verlag. ISBN: 3-446-19873-3.
- (2002). *Codes. Die Kunst der Verschlüsselung – Die Geschichte – Die Geheimnisse – Die Tricks*. München: Carl Hanser Verlag. ISBN: 3-446-20169-6.
- Thomas Roth, Hrsg. (13. Feb. 2016). *The Da vinci Code - Sakrileg - Trailer HD deutsch*. URL: <https://t1p.de/bj3i> (besucht am 03.08.2019).
- Universität Hildesheim (2001). *Vom 19. - 21. September 2001 fand die Europäische Fachtagung „Virtueller Campus“ – Szenarien – Strategien – Studium – mit Verleihung des medidaprix 2001 in Hildesheim statt*. URL: <https://t1p.de/fqsr> (besucht am 03.08.2019).
- Universum Film, Hrsg. (2. Apr. 2015). *The Imitation Game – Ein streng geheimes Leben – Trailer (deutsch/german)*. URL: <https://t1p.de/qi9c> (besucht am 03.08.2019).
- Weigend, Michael, Marco Thomas und Frank Otte, Hrsg. (2011). *Informatik mit Kopf, Herz und Hand – Praxisbeiträge zur 14. GI-Fachtagung Informatik und Schule (INFOS 2011)*. Münster: ZfL-Verlag. ISBN: 978-3-86877-009-4. URL: <https://t1p.de/rf5t> (besucht am 03.08.2019).

Bildquellen

Das Löwenlogo auf der Titelseite entstammt der Corporate-Design-Vorlage der Bergischen Universität Wuppertal <http://www.grafik.uni-wuppertal.de/>

Abbildungsverzeichnis

1	Prozess- und Inhaltsbereiche des Informatikunterrichts in den Bildungsstandards (GI, 2019, S. 7)	8
2	Kompetenzbereiche und Inhaltsfelder im Kernlehrplan des Wahlpflichtfaches Informatik an Gymnasien (nach MSB-NW, 2019a, S. 18)	11
3	Kompetenzbereiche und Inhaltsfelder im Kernlehrplan Informatik für die gymnasiale Oberstufe (nach MSW-NW, 2013, S. 19)	12
4	Phasen des Stationenlernens (vgl. Kontschinsky, 2003, S. 10-13)	19
5	Überblick zum SpionCamp (D. Müller, 2012)	22
6	Spionkoffer	23
7	DES-Chiffrierschritte (nach F. L. Bauer, 1997, S. 169)	37
8	Ver- und Entschlüsseln mit der Permutationshilfe	42
9	Beschriften der Permutationshilfe	43
10	Vigenère-Quadrat (D. Müller, 2012)	47
11	Verwendung des Stromverschlüssellers, links: Klartext vor dem Verschlüsseln, rechts: Verschlüsseln des achten Klarbuchstabens	52
12	Gepackter Spionkoffer mit den neuen Stationen	53
13	Überblick über die Stationen mit Angabe der Pflicht- und Wahlstationen	57
14	Aufbau des SpionCamps im Informatikraum	58
15	Wissen der einzelnen Schülerinnen und Schüler vor (blau) und nach (rot) der Durchführung des SpionCamps	64
16	Aufgabe 1 der Station zur Blockchiffre vor der Verbesserung	71
17	Aufgabe 1 der Station zur Stromverschlüsselung vor der Verbesserung	74
18	Verbesserter Stromverschlüsseler	74
19	Zweites Beispiel des Stationsblattes vor der Verbesserung	75
20	Drittes Beispiel des Stationsblattes vor der Verbesserung	75

Erklärung über die Eigenständigkeit

gem. § 20 Abs. 9 PO (Allgemeine Bestimmungen)

Hiermit erkläre ich, dass ich die von mir eingereichte Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt sowie Stellen der Hausarbeit, die anderen Werken dem Wortlaut oder Sinn nach entnommen wurden, in jedem Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Wuppertal, 05. August 2019

Ort, Datum

Unterschrift

Erklärung

Hiermit erkläre ich mich damit einverstanden, dass meine Abschlussarbeit (Master-Thesis) wissenschaftlich interessierten Personen oder Institutionen und im Rahmen von externen Qualitätssicherungsmaßnahmen des Studienganges zur Einsichtnahme zur Verfügung gestellt werden kann.

Korrektur- oder Bewertungshinweise in meiner Arbeit dürfen nicht zitiert werden.

Wuppertal, 05. August 2019

Ort, Datum

Unterschrift

Lizenz

Die vorliegende Arbeit steht unter einer Creative Commons Namensnennung – Weitergabe unter gleichen Bedingungen 4.0 International-Lizenz. Die Bedingungen der Lizenz können hier eingesehen werden

<https://creativecommons.org/licenses/by-nc-nd/4.0/deed.de>