UNIKASSEL VERSITÄT

ZENTRUM FÜR LEHRERBILDUNG ZLB

Wissenschaftliche Hausarbeit

im Rahmen der Ersten Staatsprüfung für das Lehramt an Gymnasien

im Fach Mathematik, eingereicht der Hessischen Lehrkräfteakademie

– Prüfungsstelle Kassel –

Kryptographie im Mathematikunterricht des Gymnasiums

Mai 2018

Verfasser:

Manuel Matting

Gutachter:

Prof. Dr. Hans-Georg Rück

Inhaltsverzeichnis

Arguing that you don't
care about the right to privacy because you have
nothing to hide is no different than
saying you don't
care about free speech because you have
nothing to say.

(Edward Snowden)[1]

[1] Zumindest mutmaßlich, vgl. reddit.com 2015.

1. Das Neuland und die Kryptographie

Die Bedeutung vernetzter, informationstechnologischer Systeme hat in den letzten Jahrzehnten immer mehr zugenommen. Wir bezeichnen unser Zeitalter selbst als Informationszeitalter. In der öffentlichen Verwaltung und der Wirtschaft, aber auch im privaten Bereich wird zunehmend vernetzt. Das Neuland Internet ist wohl in der einen oder anderen Weise in alle Lebensbereiche vorgedrungen. Bundeskanzlerin Angela Merkel hat diesen Begriff im Sommer 2013 geprägt, als sie in einer, live ins Netz gestreamten, Pressekonferenz sagte: „Das Internet ist für uns alle Neuland.“[2]

So eigentümlich diese Worte auch klingen mögen, so verweisen sie doch auf einen wichtigen Punkt: Mögen wir uns auch in dem neuen Land schon häuslich eingerichtet haben und uns nicht derart fremd fühlen, wie es offenbar Frau Merkel tut, so leben wir noch nicht so lange dort. Wir kommen möglicherweise im Alltag des neuen Landes zurecht, wir kennen die neusten Trends und nutzen die vielfältigen Angebote. Doch unter dieser Oberfläche liegt eine Vielzahl von Themen, Fragen und Problemen, die sicher nur sehr wenige in vollem Umfang überhaupt erkannt haben.

Eine zentrale Eigenschaft digitaler Informationen – gewissermaßen die Atome des Neulandes –, ist die Möglichkeit ihrer unbegrenzten und exakten Vervielfältigung. Informationen konnten schon früher kopiert werden, durch mündliche Wiedergabe, Buchdruck und so weiter. Im digitalen Bereich aber gibt es zunächst keine Möglichkeit, einzelne Kopien voneinander zu unterscheiden und die Vervielfältigung erfordert praktisch keinen Aufwand. Zudem ist sie jederzeit und augenblicklich möglich. Das hat weitreichende Konsequenzen, die sich in folgenden Fragen widerspiegeln: Wie können Daten vor unberechtigtem Kopieren und unberechtigter Einsicht geschützt werden? Wie kann die Identität von Personen im Digitalen so repräsentiert werden, dass

[2] Vgl. Spiegel Online 2013.

ihre Identitätseigenschaft sicher gestellt ist? Wie kann intransparente Datenmanipulation verhindert werden? Mit anderen Worten, wie können Vertraulichkeit, Authentizität und Integrität im Digitalen hergestellte werden?

Die Auseinandersetzung mit diesen drei Fragen ist der Kern der Kryptographie, einer Wissenschaft, die zugleich Mathematik, Informatik und angewandte Programmierung umfasst. Die Relevanz dieser Fragen rechtfertigt die Auffassung, dass ein grundlegendes Verständnis kryptographischer Ideen und Konzepte zur freiheitlichen und selbstbestimmten Mündigkeit der Bürger des Neuland Internet beitragen kann. Demgegenüber steht die Tatsache, dass die Kryptographie im schulischen Fächerkanon nur eine untergeordnete Rolle einnimmt. So spielt sie im hessischen Kerncurriculum der – nur in der Oberstufe angebotenen – Informatik eine untergeordnete Rolle, in den Kerncurricula der Mathematik findet sie sich überhaupt nicht.[3] Ebenso wenig in den entsprechenden Lehrplänen.[4] Insofern erscheint eine verstärkte Einbindung der Kryptographie in die schulische Allgemeinbildung – insbesondere mit einem mathematischen Schwerpunkt – erstrebenswert.

Umgekehrt kann die Kryptographie auch eine Bereicherung des Mathematikunterrichts sein, wenn die grundlegenden mathematischen Konzepte fokussiert und mit den herkömmlichen Themengebieten vernetzt werden. Denn einerseits wird sich in der Kryptographie der verschiedensten, mathematischen Konzepte und Methoden aus Arithmetik, Algebra und Stochastik bedient, die so also sinnstiftend angewendet werden können. Und andererseits bietet sie durch ihre diskrete Charakteristik die Möglichkeit, komplexere algebraische Denkweisen zu erlernen und überhaupt das Profil des Mathematikunterrichts hinsichtlich Algebra und Zahlentheorie zu schärfen.

Die Strukturierung des Themengebiets der Kryptographie für den Mathematikunterricht des Gymnasiums, unter Berücksichtigung der genannten Zusammenhänge und Chancen, ist die grundlegende Intention dieser Arbeit.

[3] Vgl. Kerncurricula Informatik, Mathematik (Sek I & II).
[4] Vgl. Lehrplan Mathematik (Sek I & II).

2. Leitlinien, Methodik und Struktur

In der Einleitung ist bereits eine ungefähre Leitlinie dieser Arbeit skizziert worden. Aus der Überzeugung heraus, dass zur Allgemeinbildung in der Informationsgesellschaft auch ein umfassendes Wissen gehört, über die grundlegenden Funktionsweisen der, diese Informationsgesellschaft tragenden, Infrastruktur, soll diese Arbeit einen Teil dieser Infrastruktur für die Schule, speziell für das Gymnasium, zugänglich machen.

Kryptographie ist – wie gesagt – diejenige Wissenschaft, deren Verschlüsselungsverfahren Daten in verschiedenen Kontexten schützen kann, vor unberechtigter Einsicht, Manipulation und Aneignung. Die insbesondere mathematischen Grundlagen dieses Themengebiets sollen in besonderer Weise zusammengetragen, für die Schule aufbereitet und mit den Inhalten des regulären Mathematikunterrichts verflochten werden. Das Stichwort ist hier *Vernetzung*. Damit ist gemeint, dass die Kryptographie als sinnhaft zusammenhängendes Ganzes zugänglich gemacht werden soll, bei dem die einzelnen Themengebiete nicht lose aneinander gereiht sind, sondern ihre systemischen Zusammenhänge herausgearbeitet werden. Gleichzeitig wird die genannte Vernetzung der kryptographischen Inhalte und Methoden in sinnstiftender Weise mit dem Mathematikunterricht angestrebt.

Dadurch kann einerseits das Hauptanliegen der Vermittlung der Kryptographie verfolgt werden und darüber hinaus auch der reguläre Mathematikunterricht bereichert werden. Denn erstens findet die Mathematik in der Kryptographie eine faszinierende und sinnvolle Anwendung, zweitens kann so problemorientiert der Bereich der Zahlentheorie und Algebra im Mathematikunterricht gestärkt werden und so drittens, durch Auseinandersetzung mit abstrakten, algebraischen Denkweisen, ein Beitrag zur wissenschaftspropädeutischen Bildung in der Schule geleistet werden.

Aus dem Anspruch, eine auf den mündigen Bürger der Informationsgesellschaft ausgerichtete Bildung zu befördern, folgt eine Ausrichtung der Themenauswahl auf die mo-

derne Kryptographie. Es sollen also nicht interessante, historische Verschlüsselungsverfahren um ihrer selbst willen, oder weil sie leichter zugänglich sind, behandelt werden. Inhaltliches Ziel ist vielmehr, einen Zugang zu Verfahren der modernen Kryptographie zu ermöglichen. Die Auseinandersetzung mit historischen Verfahren dient also immer dem Zweck, den Boden zu bereiten, auf dem ein Verständnis moderner Kryptographie möglich ist.

Die wesentlichen Konzepte und Methoden der Kryptographie werden in Abschnitt 3 dargelegt. Voraus greifend soll an dieser Stelle aber bereits die inhaltliche Zielsetzung spezifiziert werden: Kryptographie entwickelt und untersucht Daten-Verschlüsselungsverfahren. Dazu gehört auch der Bereich der Kryptoanalyse, die gegebene Verfahren auf Schwachstellen hin untersucht. Verschiedene Angriffsmethoden haben zur Entwicklung heutiger Verschlüsselungsverfahren geführt. Diese Zusammenhänge werden durch die vorliegende Arbeit adressiert. Moderne kryptographische Verfahren können in symmetrische und asymmetrische Verschlüsselungsverfahren unterschieden werden. Beide Klassen sollen durch konkrete Beispiele dargestellt und erfahrbar gemacht werden. Konkret sind in der, in dieser Arbeit entwickelten, Unterrichtsreihe der DES-Algorithmus und das RSA-Verfahren als Beispiele für die beiden Klassen vorgesehen.

Die Unterrichtsreihe selbst ist organisatorisch als begleitende Reihe über mehrere Schuljahre hinweg geplant. Vom Umfang her mag die Unterrichtseinheit einer Jahrgangsstufe etwa zum Ende des Schuljahres in den verbleibenden fünf, sechs Unterrichtsstunden untergebracht werden können, die in die Zeit nach der letzten Klausur fallen. Auch Projekttage oder Ähnliches können eine Gelegenheit sein, die Unterrichtsreihe zu verwirklichen. Die Verteilung der Reihe über mehrere Jahre, genauer von der 5. bis zur 11. Jahrgangsstufe, mag für die Umsetzung im Schulalltag, mit ständig wechselnden Lehrern und Klassenzusammensetzungen, ungünstig erscheinen. Es wird jedoch die Auffassung vertreten, dass nur in dieser Weise die angestrebte, starke Vernetzung hergestellt werden kann. Darüber hinaus kann so die Einbindung des Themengebiets der Kryptographie, als kanonischer Bestandteil der Inhalte des Mathema-

tikunterrichts als Gedankenexperiment erprobt werden, hinsichtlich Machbarkeit und Chancen. (Angesichts der Stofffülle in der gymnasialen Oberstufe, erklärt sich die Beschränkung auf die Sekundarstufe I und die 11. Jahrgangsstufe.) Diese Arbeit ist somit zugleich eine – wenn auch umfänglich eingeschränkte – grundlegende Untersuchung, inwiefern Kryptographie konkret als Bestandteil des gymnasialen Mathematikunterricht etabliert werden könnte. Insofern erscheint die sperrig anmutende Aufteilung über sieben Schuljahre gerechtfertigt.

Im Gesagten ist bereits mehrfach eine inhaltliche Orientierung angeklungen. Die Kryptographie soll an konkreten Beispielen zugänglich gemacht werden. Daraus ergibt sich die Notwendigkeit bestimmter mathematischer Konzepte und Methoden. Dagegen wird in dieser Arbeit der Bereich der didaktischen Kompetenzmodelle ausgeklammert, da er hinsichtlich des Anliegens, Kryptographie in der Sache aufzubereiten, als zweitrangig erscheint. Diese Arbeit ist weniger eine mathematikdidaktische Arbeit im Sinne aktueller Paradigmen, sondern eine *stoffdidaktische* Arbeit zur mathematischen Kryptographie. Demgemäß werden auch nicht die oben angeführten Kerncurricula Referenzpunkt der Vernetzung einzelner Unterrichtseinheiten sein, sondern die etwas in die Jahre gekommenen hessischen Lehrpläne für die Sekundarstufe I und II des Gymnasiums, in denen sich inhaltliche Leitlinien finden lassen.[5]

In diesem Zusammenhang sind die in den Lehrplänen an den Anfang gestellten Aufgaben und Ziele des Fachs Mathematik interessant, da sie sich in gewissem Maße auch in der Konzeption dieser Arbeit wiederfinden, und demnach auch zur Verdeutlichung herangezogen werden können: „Der Mathematikunterricht verfolgt drei Aspekte von Mathematik, die gleichgewichtig nebeneinander stehen: Mathematik als Hilfe zum Verstehen der Umwelt [...] Mathematik als Geistesschulung [...] [und] Mathematik als deduktives Gedankengebäude“.[6]

Der Beitrag der Kryptographie zum Verstehen der besonderen, informationstechnolo-

[5] Vgl. Lehrplan Mathematik (Sek I/Sek II).
[6] Lehrplan Mathematik (Sek I & II), beide S. 2(f).

gischen Umwelt ist sicher deutlich genug geworden. Aber die angestrebte Konzeption der Unterrichtsreihe ermöglicht auch eine Realisierung der anderen beiden Aspekte. Gerade die Notwendigkeit der Auseinandersetzung mit zahlentheoretischen und algebraischen Ideen und Methoden, welche sonst im schulischen Mathematikunterricht keine Rolle spielen, kann aus Sicht des Autors besondere „kognitive Strategien und intellektuelle Techniken“[7] und so die Geistesschulung befördern. Ferner findet sich der deduktive Charakter der Mathematik insbesondere auch in der Kryptographie und ihrer zugrundeliegenden Mathematik wieder.

In dieser Arbeit wird versucht, einen Mittelweg zu finden, zwischen deduktiver Strenge und organischem Zusammenhang. Gerade die zahlentheoretischen und algebraischen Grundlagen werden (unter Voraussetzung einiger Grundlagen) in deduktiver Weise hergeleitet und bieten so eine solide Basis, auf der Mathematik in ihrem deduktiven Charakter im Unterricht dargestellt werden kann. Hinsichtlich der kryptographischen Theorie, ist im Sinne der umfänglichen Beschränkung und im Sinne der Zielsetzung des sinnhaft zusammenhängenden Ganzen, eine eher narrative Darstellung gewählt worden. Eine Besonderheit ist die zusätzliche, wissenschaftspropädeutische Zielsetzung der Unterrichtsreihe. Es soll über die Jahre verstärkt mathematisches Argumentieren adressiert werden, bis hin zur letzten Einheit, in der die Gültigkeit des RSA-Verfahrens streng bewiesen wird. Derart werden sicher die beiden Aspekte der Geistesschulung und der Deduktivität angesprochen.

Das so skizzierte Konzept birgt die Gefahr, den Rahmen dieser Arbeit zu überschreiten. Es sind also Beschränkungen und Verkürzungen notwendig. Der Bereich der kryptographischen Theorie, der nicht durchweg deduktiv aufgebaut werden soll, wurde bereits erwähnt, aber auch in der Ausarbeitung der Unterrichtsreihe wird eine Art Mittelweg gewählt werden, der einerseits ein Stück weit konkrete Darstellungen einzelner Unterrichtssegmente erlaubt und andererseits große Teile stark verkürzt, um den Anforderungen der Beschränkung gerecht zu werden. Zu Beginn der Unterrichtsreihe sind

[7] Lehrplan Mathematik (Sek I & II), beide S. 2.

viele Begriffe und grundlegende Konzepte der Kryptographie erst zu etablieren. Auch mögliche Methodiken sind hier zu erproben. Und nicht zuletzt ist die Erfordernis der didaktischen Reduktion und kindgerechten Aufbereitung des Lernstoffs in den unteren Klassenstufen am größten. Daher wird die Ausführlichkeit der Darstellung des konkreten Unterrichtsgeschehens im Verlauf der Unterrichtsreihe abnehmen und vermehrt durch abstraktere Beschreibungen abgelöst werden, bis hin zu den letzten Einheiten, die größtenteils unmittelbar die Inhalte des theoretischen Teils umsetzen. Dieser Umstand ist auch in den entsprechenden Überschriften kenntlich gemacht worden. Derart ist hoffenswerterweise ein ausgeglichener Weg gefunden, der einen angemessenen Umfang wahrt und sich dennoch nicht in abstrakter Bodenlosigkeit verliert.

Bevor nun abschließend die Struktur der vorliegenden Arbeit erläutert wird, sei ein kurzer Hinweis bezüglich der didaktischen Forschung im Feld der mathematischen Kryptographie gegeben. Dieses Feld ist nicht nur in den schulischen Curricula, wie auch den inhaltlicher orientierten Lehrplänen unterrepräsentiert. Ebenso in der Mathematikdidaktik scheint das Thema kaum Gegenstand der Forschung zu sein. Nach den Recherchen des Autors gibt es keine relevanten Veröffentlichungen im Printbereich und auch online ließen sich nur wenige ausführlichere Arbeiten finden. Die bemerkenswerteste Arbeit ist die Dissertation von Monika Stohr: *Unterricht in Kryptologie* aus dem Jahr 2007. Die Auswahl der kryptographischen Verfahren betreffend, sind einige Überschneidungen zur vorliegenden Arbeit gegeben, ansonsten sind die Schwerpunkte anders gelagert. Stohr fokussiert stärker auf die Legitimierung eines Kryptographieunterrichts und auf Themen der Schulentwicklung, etwa die Möglichkeiten fächerübergreifenden Unterrichts. Fragen, die in dieser Arbeit nur teilweise und recht knapp in der Einleitung und diesem Abschnitt behandelt worden sind. Dagegen liegt die Besonderheit der vorliegenden Arbeit in der besprochenen, zusammenhängenden Einheit und ihrer Aufteilung über die gesamte Sekundarstufe I und den Beginn der Oberstufe, ferner in ihrem Fokus auf die stoffdidaktische Vernetzung mit den Lehrplänen. Insofern nimmt diese Arbeit eine Vorreiterrolle ein und ein ausführlicher Abschnitt zur didaktischen Forschungsliteratur entfällt.

Diese Arbeit enthält zwei Hauptteile, die unmittelbar im Anschluss an diesen Abschnitt folgen. Und zwar zunächst ein theoretischer Teil, in dem in vier Abschnitten erstens die benötigten, mathematischen Grundlagen, zweitens die Kryptographie und kryptographische Verfahren allgemein, drittens Sicherheit und kryptoanalytische Methoden und schließlich viertens eine Auswahl von in der Unterrichtsreihe verwendeten, konkreten Verschlüsselungsverfahren erarbeitet wird.

Der zweite Hauptteil umfasst die sieben einzelnen Unterrichtseinheiten. Dabei ist mit der angegebenen Jahrgangsstufe jeweils ein Zeitraum *zum Ende dieser Jahrgangsstufe* gemeint, entsprechend der oben vorgeschlagenen Durchführung gegen Ende des Schuljahres. Jede Einheit besteht aus einem Abschnitt zu Lernzielen und Vernetzung, in dem kurz die angestrebten Inhalte und Techniken zusammengefasst werden und eine Vernetzung in den ebenfalls oben dargelegten Richtungen versucht wird. Das sind im Besonderen der Zusammenhang des gesamten, kryptographischen Themengebiets und die Verflechtung mit dem regulären Stoff des Mathematikunterrichts.

Die Arbeit endet mit einem kürzeren Schlussteil, in dem kritisch Stellung bezogen wird, zu den, in diesem Abschnitt formulierten Zielsetzungen. Darüber hinaus wird ein Ausblick gegeben, hinsichtlich Erweiterungsmöglichkeiten der Unterrichtsreihe, als auch hinsichtlich weiterer didaktischer Forschungsfelder im Anschluss an die Ergebnisse dieser Arbeit.

3. Die Wissenschaft der Kryptographie

3.1 Mathematische Grundlagen

Kryptographie basiert in elementarer Weise auf Mathematik, insbesondere auf den Bereichen Algebra und Zahlentheorie. Diese Arbeit verfolgt nicht das Ziel, die mathematische Theorie von Grund auf lückenlos darzustellen. Vielmehr wird in den folgenden Erörterungen ein mathematisches Grundlagenwissen vorausgesetzt, dass sich üblicherweise in Anfängervorlesungen der Mathematik wiederfindet, etwa Grundlagen der Analysis und linearen Algebra, grundlegende algebraische Konzepte, aber auch einige wenige Begriffe der Stochastik. Drei Einstiegswerke sind in Abschnitt 6 als Literaturempfehlungen angeführt. Diese Grundlagen korrelieren in gewisser Weise auch mit dem kanonischen Schulstoff. Dagegen sind andere algebraische und zahlentheoretische Konzepte und deren Eigenschaften zu erarbeiten, die für die Kryptographie unerlässlich sind, aber im schulischen Kontext nicht zwingend zur Anwendung kommen. Ausgehend von Erkenntnissen zur Teilbarkeit und Primzahlen, wird insbesondere die Restklassenarithmetik im Restklassenring $\mathbb{Z}/n\mathbb{Z}$ dargestellt, da diese die arithmetische Grundlage aller, hier dargestellter, kryptographischer Modelle ist.

Vorausgesetzt werden besonders die Zahlbereiche $\mathbb{N}$ und $\mathbb{Z}$, wobei festgelegt wird, dass $0 \notin \mathbb{N}$. Ferner Ringeigenschaften von $\mathbb{Z}$, Ordnung, Nullteilerfreiheit, oder auch die Wohlordnung von $\mathbb{N}$ und ähnlich Grundlegendes. Auch die 2-adische Darstellung von natürlichen Zahlen und der Zusammenhang zu Computerbits wird größtenteils vorausgesetzt, insbesondere die XOR-Verknüpfung wird aber zur Erinnerung kurz angesprochen.

Die mathematische Theorie und auch die kryptographischen Konzepte und Verfahren sind im Wesentlichen inspiriert durch die Standardwerke von insbesondere Buchmann, aber auch Beutelspacher, Küsters & Wilke, Swoboda et al. und Willems. Ebenfalls

ist Wikipedia.org als Inspirationsquelle besonders hinsichtlich Ideen der Beweisführung zu nennen. Selbstverständlich sind Zitate jeglicher Art separat ausgewiesen. Nach diesen einleitenden Worten, kann nun in die spannende Theorie der Kryptographie eingestiegen werden.

Die Ring-Eigenschaften der ganzen Zahlen $\mathbb{Z}$ vorausgesetzt, soll hier zu Beginn eine weitere Eigenschaft in den Blick genommen werden, die bereits in elementarer Weise in der Grundschule gelehrt und angewendet wird, nämlich die *Division mit Rest*. Ihre Existenz und die Eindeutigkeit des Quotienten und des Rests sichert folgender Satz:

Satz 1. ***Division mit Rest***

Für $a, b \in \mathbb{Z}, b > 0$ existieren eindeutige $q, r \in \mathbb{Z}$, so dass gilt:

$$a = q \cdot b + r \qquad mit \qquad 0 \leq r < b$$

Dabei ist $q = \lfloor \frac{a}{b} \rfloor$ und $r = a - qb$.

Beweis. (Existenz)

Wähle $q \coloneqq \lfloor \frac{a}{b} \rfloor$ und $r \coloneqq a - qb$, dann gilt

$$qb + r = \lfloor \frac{a}{b} \rfloor \cdot b + a - \lfloor \frac{a}{b} \rfloor \cdot b = a$$

Und wegen $r = a - qb = a - \lfloor \frac{a}{b} \rfloor \cdot b$ gilt ferner:

$$a - \left(\frac{a}{b} - 1\right) \cdot b \quad > \quad r \quad \geq \quad a - \left(\frac{a}{b}\right) \cdot b$$

$$\Longrightarrow \qquad a - a + b = b > r \geq 0 = a - a$$

(Eindeutigkeit)

Seien also $q, r \in \mathbb{Z}$, so dass (1) gilt, dann folgt sofort:

$$0 \leq r = a - qb < b$$

Wegen $b > 0$:

$$\Longrightarrow \quad 0 \leq \frac{r}{b} = \frac{a}{b} - q < 1 \quad \Longrightarrow \quad -\frac{a}{b} \leq -q < 1 - \frac{a}{b} \quad \Longrightarrow \quad \frac{a}{b} \geq q > \frac{a}{b} - 1$$

Und wegen $q \in \mathbb{Z}$ ist dann:

$$q = \lfloor \frac{a}{b} \rfloor$$

□

Die Frage wann es *keinen* Rest gibt, führt zum Begriff der *Teilbarkeit*, der im Folgenden definiert wird. Darüber hinaus werden grundlegende Rechenregeln abgeleitet.

Definition 1. *Für $a, b \in \mathbb{Z}$ heißt a **Teiler** von b, wenn $\exists k \in \mathbb{Z}$, so dass $ak = b$. Wir sagen auch „a teilt b“ und schreiben $a \mid b$. Ist a kein Teiler von b, so notieren wir $a \nmid b$.*

Satz 2. ***Rechenregeln zur Teilbarkeit***

$\forall a, b, c, d, e \in \mathbb{Z}$ gilt:

i) $1 \mid a, \quad a \mid a, \quad a \mid 0$ *und mit* $0 \mid a \;\Rightarrow\; a = 0.$

ii) $a \mid b \;\Rightarrow\; -a \mid b \;\wedge\; a \mid -b$

iii) $a \mid b \;\wedge\; b \mid c \;\Rightarrow\; a \mid c.$

iv) $a \mid b \;\Rightarrow\; ac \mid bc.$

v) $a \mid b \;\wedge\; a \mid c \;\Rightarrow\; a \mid (bd + ce).$

vi) $a \mid b \;\wedge\; b \neq 0 \;\Rightarrow\; 0 < |a| \leq |b|.$

vii) $a \mid b \;\wedge\; b \mid a \;\Rightarrow\; |a| = |b|.$

Beweis. Seien also $a, b, c, d, e \in \mathbb{Z}$.

i) Es gilt $a \cdot 1 = a \;\Rightarrow\; 1 \mid a \;\wedge\; a \mid a$. Ferner $a \cdot 0 = 0 \;\Rightarrow\; a \mid 0$
und mit $0 \mid a \;\Rightarrow\; \exists k \in \mathbb{Z} : a = 0 \cdot k = 0 \;\Rightarrow\; a = 0$

ii) $\exists k \in \mathbb{Z} : ak = b \Rightarrow (-a)(-k) = b \wedge a(-k) = -b$

iii) $\exists k, l \in \mathbb{Z} : ak = b \wedge bl = c \;\Rightarrow\; akl = c$ mit $kl \in \mathbb{Z} \;\Rightarrow\; a \mid c$

iv) $\exists k \in \mathbb{Z} : ak = b \;\Rightarrow\; \forall c \in \mathbb{Z} : akc = bc \;\Rightarrow\; ac \mid bc$

v) $\exists k, l \in \mathbb{Z} : ak = b \wedge al = c \;\Rightarrow\; \forall d, e \in \mathbb{Z} :$
$bd + ce = akd + ale = a(kd + le) \;\Rightarrow\; a \mid (bd + ce)$

vi) $\exists k \in \mathbb{Z} : ak = b \neq 0 \;\Rightarrow\; a \neq 0, k \neq 0 \;\Rightarrow\; |b| = |ak| = |a||k| \geq |a| > 0$

vii) $\exists k, l \in \mathbb{Z} : ak = b \wedge bl = a$, dann ist $a = 0 \Leftrightarrow b = 0$
Andernfalls gilt mit v) $|a| \leq |b| \wedge |b| \leq |a| \;\Rightarrow\; |a| = |b|$.

□

Die *Primzahlen* und die eindeutige Zerlegbarkeit jeder ganzen Zahl in Primfaktoren sind neben der Theorie der Teilbarkeit der zentrale Inhalt der elementaren Zahlentheorie:[8]

Definition 2. *Eine Zahl $p \in \mathbb{N}$ heißt **Primzahl**, wenn sie genau zwei verschiedene Teiler in $\mathbb{N}$ hat. Man sagt auch p **ist prim** und schreibt für die Menge aller Primzahlen $\mathbb{P}$.*

Bemerkung. *Nach Satz 2 wird jede Zahl durch* 1 *und sich selbst geteilt. Also sind die Teiler einer Primzahl p immer* 1 *und p selbst. Insbesondere ist* 1 *keine Primzahl, da sie nicht zwei verschiedene Teiler hat. Die* 1 *ist trivialerweise die einzige Zahl in $\mathbb{N}$, die diese Eigenschaft hat.*

Satz 3. *Der kleinste Teiler $b \in \mathbb{N}, b \neq 1$ einer Zahl $a \in \mathbb{Z}$ ist eine Primzahl.*

[8] Vgl. Buchmann 2001, S. 18f.

Beweis. Zunächst gibt es tatsächlich für $a \in \mathbb{Z}$ einen kleinsten Teiler $b \in \mathbb{N}, b \neq 1$, denn wieder mit Satz 2 ist mindestens $|a|$ Element der Teilermenge von a und aufgrund der Wohlordnung von $\mathbb{N}$ und der unteren Schranke 1 muss diese ein kleinstes Element ungleich 1 enthalten. Angenommen b ist nicht prim, dann $\exists \hat{p} \in \mathbb{N}$ mit $1 < \hat{p} < p \leq a$, so dass $\hat{p} \mid p$, also $\hat{p} \mid a$. Ein Widerspruch, denn so wäre p nicht der kleinste Teiler.

□

Satz 4. ***Hauptsatz der elementaren Zahlentheorie***

Jede natürlich Zahl $a \neq 1$ kann in ein Produkt endlich vieler Primzahlen zerlegt werden. Diese Darstellung ist bis auf die Reihenfolge der Faktoren eindeutig.

Bemerkung. *Man spricht auch von der* ***Primfaktorzerlegung****. Es lässt sich unmittelbar einsehen, dass auch jede ganze Zahl eindeutig in Primfaktoren und den Faktor* (-1) *zerlegt werden kann.*

Beweis. (Existenz)

Angenommen es gibt natürliche Zahlen ungleich 1, die nicht in Primfaktoren zerlegbar sind. Sei a die kleinste solche Zahl, dann gilt $a \in \mathbb{N}$, $a \neq 1$ und a nicht prim, also $\exists b \in \mathbb{N} : 1 < b < a \wedge b \mid a$, also existiert nach Definition $k \in \mathbb{N} : kb = a$ und insbesondere gilt auch hier $1 < k < a$. Nun müssen b, k Primfaktorzerlegungen besitzen, da sie kleiner a sind und a die kleinste Zahl ohne Primfaktorzerlegung ist. Dann aber ist das Produkt dieser beiden Zerlegungen zugleich eine Zerlegung von a in Primfaktoren.

(Eindeutigkeit)

Angenommen es gibt Zahlen mit nicht eindeutigen Primfaktorzerlegungen, dann gibt es wieder wegen der Wohlordnung eine kleinste solche Zahl, etwa n. Es gilt $n \in \mathbb{N}$, $n > 1$. Sei nun $p \in \mathbb{N}$ diejenige Primzahl, die kleinster Teiler von n ist (existiert wegen Satz 3). Dann gilt $n = pk$ mit $k \in \mathbb{N}$, $1 < k < n$. Da n die kleinste Zahl ohne eindeutige Primfaktorzerlegung ist, muss k dagegen eindeutig zerlegbar sein, etwa

$k = \prod_{i=1}^{s} p_i$. Nun gibt es laut Annahme eine weitere Zerlegung von n in Primfaktoren, etwa $\prod_{i=1}^{t} q_i$. Es gilt $\forall i \in \{1, ..., t\} : q_i > p$, da erstens p kleinster Teiler von n ist und zweitens, falls $\exists i \in \{1, ..., t\} : q_i = p$ wegen der eindeutigen Zerlegbarkeit von k ein Widerspruch zur Annahme einer weiteren, verschiedenen Primfaktorzerlegung besteht. Betrachte nun

$$\hat{n} \coloneqq n - p \prod_{i=1, i\neq j}^{t} q_i = \left(q_j - p\right) \prod_{i=1, i\neq j}^{t} q_i \quad \text{mit} \quad j \in \{1, ..., t\}$$

Es ist $\hat{n} \in \mathbb{N}$ wegen $q_j > p$ und ferner $\hat{n} < n$, weshalb $\hat{n}$ eine eindeutige Primfaktorzerlegung besitzen muss. Diese enthält p als Faktor, denn mit $p \mid n \implies p \mid \hat{n}$. Wegen $p \nmid \prod_{i=1, i\neq j}^{t} q_i \implies p \mid \left(q_j - p\right) \implies p \mid q_j$, was im Widerspruch zur Annahme steht, dass q_j eine Primzahl ist.

□

Mit dem Hauptsatz lässt sich leicht das äußerst nützliche *Lemma von Euklid* nachweisen, das hier der Vollständigkeit halber aufgeführt wird:

Satz 5. ***Lemma von Euklid***

Für alle $a, b \in \mathbb{Z},\ p \in \mathbb{P}$ *mit* $p \mid ab \quad \implies \quad p \mid a \ \vee \ p \mid b$

Beweis. $a, b \in \mathbb{Z}$ können eindeutig in Primfaktoren mit eventuellem Vorzeichen zerlegt werden:

$$a = (-1)^u \prod_{i=1}^{s} a_i \quad \text{und} \quad b = (-1)^v \prod_{i=1}^{t} b_i \quad \text{mit} \quad u, v \in \{0, 1\}, \quad a_i, b_i \in \mathbb{P}$$

Teilt nun $p \mid ab$ und o.B.d.A $p \nmid a$, dann mit

$$p \mid \left((-1)^{u+v} \prod_{i=1}^{s} a_i \prod_{i=1}^{t} b_i\right) \quad \implies \quad \exists i \in \{1, ..., t\} : p = b_i$$

wegen der Eindeutigkeit der Primfaktorzerlegung. Also $p \mid b$.

□

Gerüstet mit der eindeutigen Primfaktorzerlegung und den wichtigsten Rechenregeln zur Teilbarkeit, kann der größte gemeinsame Teiler definiert werden.

Satz 6. *Für alle $a, b \in \mathbb{Z}$ mit $(a, b) \neq (0, 0)$ hat die Menge derjenigen Zahlen, die sowohl a, als auch b teilen, ein größtes Element in den natürlichen Zahlen.*

Beweis. Sei o.B.d.A $a \neq 0$. Dann gilt nach Satz 2 für alle Teiler $g \in \mathbb{Z}$ von a : $|g| \leq |a|$. Die Teilermenge ist also beschränkt, also muss es einen größten Teiler geben. Dieser muss ebenso nach Satz 2 eine natürliche Zahl sein, denn ist g Teiler, dann auch $-g$.

□

Definition 3. *Für alle $a, b \in \mathbb{Z}$ mit $(a, b) \neq (0, 0)$ heißt eine solche Zahl, die größtes Element der Menge $\{g \in \mathbb{Z} \mid (g \mid a \wedge g \mid b)\}$ ist,* ***größter gemeinsamer Teiler*** *(ggT) von a, b und man schreibt $g = ggT(a, b)$.*

Bemerkung. *Insbesondere ist der ggT immer in $\mathbb{N}$, denn 1 teilt jede Zahl in $\mathbb{Z}$.*

Der folgende Satz sagt aus, dass der ggT zweier Zahlen immer als eine Linearkombination derselben dargestellt werden kann, was sich für die Restklassenarithmetik als äußerst nützlich erweisen wird.

Satz 7. ***Lemma von Bézout***

Für alle $a, b \in \mathbb{Z}$ mit $(a, b) \neq (0, 0)$ existieren $x, y \in \mathbb{Z}$, so dass

$$ggT(a, b) = ax + by.$$

Beweis. Da die natürlichen Zahlen nach oben unbeschränkt sind, gibt es für alle $a, b \in \mathbb{Z}$ eine Darstellung $ax + by > 0,\ x, y \in \mathbb{Z}$. Sei nun g das kleinste Element der Menge $\{k \in \mathbb{N} \mid k = ax + by,\ x, y \in \mathbb{Z}\} \subset \mathbb{N}$, dann gilt $\text{ggT}(a, b) \mid g$.

Mit Satz 1 und der Tatsache, dass $g \neq 0$, $\exists q, r \in \mathbb{Z}$, so dass

$$a = qg + r = q(ax + by) \quad \text{mit} \quad 0 \leq r < g = (ax + by)$$

$$\Longrightarrow \qquad r = a - q(ax + by) = a(1 - qx) + b(-qy)$$

r ist also eine Linearkombination von a, b. Da aber $0 \leq r < g$ und g minimal ist $\Longrightarrow$ $a = qg \Longrightarrow g \mid a$. Analog gilt $g \mid b$ und wegen $\text{ggT}(a, b) \mid g \Longrightarrow g = \text{ggT}(a, b)$.

□

Mit Satz 1 über die Division mit Rest kann eine Relation definiert werden, die das, für die Kryptographie unerlässliche Instrument der Restklassen begründet.

Definition 4. *Man sagt für $a, \hat{a} \in \mathbb{Z}, n \in \mathbb{N}$: a ist **kongruent** $\hat{a}$ **modulo** n und schreibt*

$$a \equiv \hat{a} \bmod n \quad :\Longleftrightarrow$$

$$\exists q, \hat{q}, r \in \mathbb{Z}: \quad a = qn + r \quad \wedge \quad \hat{a} = \hat{q}n + r \quad \textit{mit} \quad 0 \leq r < n.$$

Bemerkung. *Die Zahl n wird auch als **Modul** bezeichnet. Gilt $a \equiv \hat{a} \bmod n$, so haben mit anderen Worten a und $\hat{a}$ bei Division mit n denselben Rest.*

Folgender Satz ermöglicht eine flexiblere Anwendung der Definition:

Satz 8. *Für alle $a, \hat{a} \in \mathbb{Z}, n \in \mathbb{N}$ sind folgende Aussagen äquivalent:*

i) $a \equiv \hat{a} \bmod n$

ii) $\exists k \in \mathbb{Z}: a = \hat{a} + kn$

iii) $n \mid (a - \hat{a})$

Beweis. Seien also $a, \hat{a} \in \mathbb{Z}, n \in \mathbb{N}$.

i) $\implies$ ii): Gilt $a \equiv \hat{a} \bmod n$, dann $\exists q, \hat{q} \in \mathbb{Z}$:

$$a - qn = \hat{a} - \hat{q}n \implies a - \hat{a} = (q - \hat{q})\, n \implies n \mid (a - \hat{a})$$

ii) $\implies$ iii): Gilt $n \mid (a - \hat{a})$, dann

$$\exists k \in \mathbb{Z} : kn = a - \hat{a} \implies a = \hat{a} + kn$$

iii) $\implies$ i): $\exists k \in \mathbb{Z} : a = \hat{a} + kn$, so gilt mit Satz 1:

$$\exists q, \hat{q}, r, \hat{r} \in \mathbb{Z} : \quad a = qn + r, \quad \hat{a} = \hat{q}n + r, \quad 0 \leq r < n, \quad 0 \leq \hat{r} < n$$

Insbesondere gilt damit $|r - \hat{r}| < n$. Weiter gilt:

$$kn = qn + r - (\hat{q}n + \hat{r}) = (q - \hat{q}) \cdot n + (r - \hat{r})$$

$$\implies n \mid ((q - \hat{q}) \cdot n + (r - \hat{r})) \implies n \mid (r - \hat{r})$$

Wegen $|r - \hat{r}| < n$ folgt $r - \hat{r} = 0$, also $r = \hat{r}$, wodurch die Definition erfüllt ist und also $a \equiv \hat{a} \bmod n$.

□

Man überzeugt sich leicht, dass es sich bei obiger Relation um eine Äquivalenzrelation handelt, denn es gilt immer $a \equiv a \bmod n$ (Reflexivität), mit $a \equiv \hat{a} \bmod n \implies \hat{a} \equiv a \bmod n$ (Symmetrie) und mit $a \equiv \hat{a} \bmod n \wedge \hat{a} \equiv \hat{\hat{a}} \bmod n \implies a \equiv \hat{\hat{a}} \bmod n$ (Transitivität).

Die Äquivalenzklassen – oder auch *Restklassen* – modulo n sind die Teilmengen

$$k + n\mathbb{Z} \coloneqq \{k + n \cdot m : m \in \mathbb{Z}\} \subset \mathbb{Z}, \; k \in \mathbb{Z}$$

$\mathbb{Z}$ wird modulo n in genau n Restklassen zerlegt und diese bilden die Elemente

folgender Menge:

Definition 5. $\mathbb{Z}/n\mathbb{Z} := \{0+n\mathbb{Z}, 1+n\mathbb{Z}, \dots, (n-1)+n\mathbb{Z}\}$ *ist die Menge der n Restklassen modulo n.*

Wenn im Folgenden von Restklassen die Rede ist und nichts anderes gesagt ist, geht es immer um die Restklassenmenge $\mathbb{Z}/n\mathbb{Z}$. Unter dieser Voraussetzung werden die Restklassen zur Übersicht im folgenden Abschnitt auch kurz mit $\overline{k} := k + n\mathbb{Z}$ notiert. Es sollen nun für $\mathbb{Z}/n\mathbb{Z}$ Ringeigenschaften nachgewiesen werden, so dass einfach mit Restklassen gerechnet werden kann. Dazu werden zunächst eine wohldefinierte Addition und Multiplikation benötigt:

Definition 6. *Für alle* $\overline{k}, \overline{l} \in \mathbb{Z}/n\mathbb{Z}$ *wird definiert eine*

i) Addition: $\overline{k} + \overline{l} = (k + n\mathbb{Z}) + (l + n\mathbb{Z}) := (k + l) + n\mathbb{Z} = \overline{k + l}$

ii) Multiplikation: $\overline{k} \cdot \overline{l} = (k + n\mathbb{Z}) \cdot (l + n\mathbb{Z}) := (k \cdot l) + n\mathbb{Z} = \overline{k \cdot l}$

Die Wohldefiniertheit ist leicht einzusehen, wenn man je zwei Vertreter $k, \hat{k} \in \mathbb{Z}$ und $l, \hat{l} \in \mathbb{Z}$ betrachtet, also der Zusammenhang $k \equiv \hat{k} \bmod n \ \wedge \ l \equiv \hat{l} \bmod n$ gilt: Dann ist nämlich

i) $(k + l) - \left(\hat{k} + \hat{l}\right) \equiv \left(k - \hat{k}\right) + \left(l - \hat{l}\right) \equiv 0 \bmod n$, also $k + l \equiv \left(\hat{k} + \hat{l}\right) \bmod n$

ii) $(k \cdot l) - \left(\hat{k} \cdot \hat{l}\right) \equiv \left(k - \hat{k}\right) \cdot \hat{l} + k \cdot \left(l - \hat{l}\right) \equiv 0 \bmod n$, also $k \cdot l \equiv \hat{k} \cdot \hat{l} \bmod n$

Es ist $\overline{0}$ das neutrale Element der Addition und $\overline{1}$ das neutrale Element der Multiplikation, ferner ist $\forall \overline{k} \in \mathbb{Z}/n\mathbb{Z}$ das Element $-\overline{k}$ das additiv Inverse. Da sich Assoziativität, Kommutativität und Distributivität von $\mathbb{Z}$ nach $\mathbb{Z}/n\mathbb{Z}$ vererben, ist die Menge der Restklassen mit obiger Addition und Multiplikation ein Ring und es kann problemlos gerechnet werden. Auf die Balkennotation wird nun wieder verzichtet.

Beispiel 1. *Ein wichtiges Beispiel eines Restklassenrings ist $\mathbb{Z}/2\mathbb{Z}$. Durch Tupel über $\mathbb{Z}/2\mathbb{Z}$ wiederum lassen sich Bitfolgen, wie sie in Computern verwendet werden, darstellen. Zur Erinnerung: Durch Interpretation der Bits als Koeffizienten a_i des Polynoms*

$$a = \sum_{i=0}^{n} a_i \cdot 2^i$$

lassen sich mit geeignetem $n \in \mathbb{N}$ wiederum alle Zahlen $a \in \mathbb{N}$ als Bitfolgen kodieren. In unserem Anwendungsfall werden Bitfolgen oder eben Tupel über $\mathbb{Z}/2\mathbb{Z}$ allerdings komponentenweise addiert. Diese Operation entspricht der XOR-Verknüpfung der einzelnen Bits:

$$+ : \ (\mathbb{Z}/2\mathbb{Z})^2 \to \mathbb{Z}/2\mathbb{Z}, \quad (x,y) \mapsto \begin{cases} 0 & \textit{falls } (x,y) = (0,0) \vee (x,y) = (1,1) \\ 1 & \textit{sonst} \end{cases}$$

$$\textit{XOR: } \{0,1\}^2 \to \{0,1\}, \quad (x,y) \mapsto \begin{cases} 0 & \textit{falls } (x,y) = (0,0) \vee (x,y) = (1,1) \\ 1 & \textit{sonst} \end{cases}$$

Ferner ist auch die Subtraktion äquivalent, denn in $\mathbb{Z}/2\mathbb{Z}$ gilt $1 \equiv -1 \ mod\ 2$ und also gilt $\forall x \in \mathbb{Z}/2\mathbb{Z} : x \equiv -x \ mod\ 2$. Da nur die Elemente 0 und 1 in $\mathbb{Z}/2\mathbb{Z}$ liegen, ist durch jede Ziffer eindeutig eine Komponente eines Tupels, beziehungsweise ein Bit bestimmt. Daher werden Tupel der Form $(a,b,c,...)$, $a,b,c,... \in \mathbb{Z}/2\mathbb{Z}$ im Folgenden kurz als $(abc...)_2$ notiert.

In $\mathbb{Z}$ gibt es bis auf 1 und -1 keine multiplikativ invertierbaren Elemente. Wie verhält es sich aber im Restklassenring $\mathbb{Z}/n\mathbb{Z}$? In der Tat gibt es hier andere invertierbare Elemente und zwar genau diejenigen Elemente, die *teilerfremd* zum Modul n sind:

Satz 9. ***Inverse in Restklassenringen***

$$a \in \mathbb{Z} \quad \textit{ist in} \quad \mathbb{Z}/n\mathbb{Z} \quad \textit{invertierbar} \qquad \Longleftrightarrow \qquad ggT(a,n) = 1$$

Inverse sind eindeutig bestimmt.

Beweis. ($\Longrightarrow$)

Sei also $a \in \mathbb{Z}$ in $\mathbb{Z}/n\mathbb{Z}$ invertierbar, dann $\exists x \in \mathbb{Z} : ax \equiv 1 \bmod n$. Sei ferner $g \coloneqq \text{ggT}(a, n)$. Dann gilt nach Satz 8:

$$n \mid (ax - 1) \implies g \mid (ax - 1)$$

Und mit $g \mid a \ \wedge \ g \geq 0$

$$\implies g \mid 1 \implies g = 1$$

($\Longleftarrow$)

Gelte nun $\text{ggT}(a, n) = 1$, dann mit Satz 7 $\exists s, t \in \mathbb{Z} : sa + tn = 1$

$$\implies \quad sa - 1 = -tn \quad \implies \quad n \mid (sa - 1)$$

$$\implies \quad sa \equiv 1 \bmod n \quad \implies \quad s \text{ invers zu } a$$

(*Eindeutigkeit*)

Seien $s, \hat{s} \in \mathbb{Z}$ invers zu $a \in \mathbb{Z}$, dann

$$sa \equiv \hat{s}a \bmod n \quad \implies \quad n \mid (a \cdot (s - \hat{s}))$$

Wegen $\text{ggT}(a, n) = 1$ gilt dann

$$n \mid (s - \hat{s}) \quad \implies \quad s \equiv \hat{s} \bmod n$$

Folglich sind Inverse in $\mathbb{Z}/n\mathbb{Z}$ eindeutig.

□

Damit ist die Frage nach der Existenz von Inversen geklärt, nicht aber das Problem

ihrer Bestimmung. Inverse in $\mathbb{Z}/n\mathbb{Z}$ können, falls sie existieren, durch den *Erweiterten Euklidischen Algorithmus* (EEA) berechnet werden. Dieser wiederum ist eine Weiterentwicklung des klassischen *Euklidischen Algorithmus*, der äußerst effizient den größten gemeinsamen Teiler zweier Zahlen $a, b \in \mathbb{Z}$ berechnen kann. Der EEA berechnet nun über den größten gemeinsamen Teiler hinaus auch diejenigen Zahlen $x, y \in \mathbb{Z}$, für die gilt, dass $ax + by = \text{ggT}(a, b)$ und deren Existenz nach Satz 7 gesichert ist. Wählt man nun $b := n$, dann gilt $ax = \text{ggT}(a, n) - ny$, was kongruent zu $\text{ggT}(a, n) \bmod n$ ist. Existiert nun ein Inverses zu a, so ist der größte gemeinsame Teiler gleich 1 und das Inverse durch $a^{-1} := x$ gegeben.

Der folgende Satz zeigt, dass sich der ggT zweier Zahlen nicht ändert, wenn die eine Zahl durch den Rest der Division mit der anderen ersetzt wird und dient als Hilfssatz, um anschließend die Korrektheit des Euklidischen Algorithmus nachzuweisen.

Satz 10. *Für alle $a, b \in \mathbb{Z}, (a, b) \neq (0, 0)$ gilt:*

i) $ggT(a, b) = |a|, \quad falls\ b = 0.$

ii) $ggT(a, b) = ggT(|b|, a \bmod |b|), \quad falls\ b \neq 0.$

Beweis. Seien also $a, b \in \mathbb{Z}$.

i) Folgt mit $(b = 0 \implies a \neq 0)$ sofort aus Satz 2.

ii) Sei $b \neq 0$. Wegen Satz 1 $\exists q, r \in \mathbb{Z}$ mit $0 \leq r < |b|$, so dass $a = q|b| + r$. Mit anderen Worten ist $a = q|b| + (a \bmod |b|)$.
Damit gilt für $g := \text{ggT}(a, b)$ und $\hat{g} := \text{ggT}(|b|, a \bmod |b|)$:

$$g \mid (q|b|) \quad \wedge \quad g \mid (a \bmod |b|) \quad \implies \quad g \mid (a \bmod |b|)$$

und

$$\hat{g} \mid (q|b|) \quad \wedge \quad \hat{g} \mid (a \bmod |b|) \quad \implies \quad \hat{g} \mid a.$$

Die Behauptung folgt mit der positiven Definitheit des ggT und Satz 2.

□

Durch obigen Satz 10 ist bereits ein rekursives Verfahren begründet, durch das der ggT(a, b) berechnet werden kann. Indem nämlich fortwährend die größere Zahl durch die kleinere mit Rest geteilt wird, ist zu hoffen, dass nach endlich vielen Schritten der Rest Null wird und so die verbliebene Zahl den ggT angibt. Genau dieses Verfahren bezeichnet der Euklidische Algorithmus. Er soll nun in seiner erweiterten Form exakt beschrieben werden, Erweitert bedeutet, es werden zusätzlich Informationen gesammelt, die helfen den ggT als Linearkombination gemäß Satz 7 darzustellen.

Satz 11. ***Erweiterter Euklidischer Algorithmus***

Für $a, b \in \mathbb{Z}, (a, b) \neq (0, 0)$ sei folgendes Verfahren gegeben:[9]

Setze: $a_0 := |a|, \quad b_0 := |b|$

Iteriere folgende Anweisung über $i \in \mathbb{N}$:

- *Falls $b_{i-1} = 0$, terminiere das Verfahren.*
- *Sonst setzte* $a_i := b_{i-1} \quad (*) \quad$ *und* $\quad b_i := a_{i-1} - q_{i-1} \cdot b_{i-1} \quad (**)$
  mit $q_i \in \mathbb{Z}$, so dass $0 \leq b_i < b_{i-1}$.

Es gelten folgende Aussagen:

i) Das Verfahren ist wohldefiniert und terminiert nach endlich vielen Schritten $k \in \mathbb{N}$.

ii) Gilt nach $k \in \mathbb{N}$ Schritten $b_{k-1} = 0$, so gilt $a_{k-1} = ggT(a, b)$.

iii) Es lassen sich aus den a_i, b_i und q_i zwei Zahlen $x, y \in \mathbb{Z}$ berechnen, die Satz 7 erfüllen, für die also gilt $ax + by = ggT(a, b)$.

Beweis. Seien also $a, b \in \mathbb{Z}, (a,) \neq (0, 0)$. Es gelte o.B.d.A. $|a| \geq |b|$.

[9] Das Verfahren kann auch reduzierter dargestellt werden, indem etwa direkt $r_0 := |a|$ und $r_1 := |b|$ gesetzt wird. Hier wurde mit Blick auf didaktische Erwägungen die gegebene, umfassendere Version gewählt, die näher an der manuellen Umsetzung des Algorithmus liegt.

i) Mit Satz 1 gibt es insbesondere für $a_{i-1}, b_{i-1} \in \mathbb{Z}$ zwei Zahlen $q, r \in \mathbb{Z}$, so dass

$$a_{i-1} = qb_{i-1} + r \quad \text{mit} \quad 0 \leq r < b_{i-1} \qquad \Longrightarrow \qquad r = a_{i-1} - qb_{i-1}$$

Dann ist das Verfahren durch $q_{i-1} \coloneqq q$ und $b_i \coloneqq r$ wohldefiniert. Es gilt also $\forall i \in \mathbb{N}$, dass $0 \leq b_i < b_{i-1}$ und auch $b_i \in \mathbb{N}_0$, das heißt die Folge $(b_i) \subset \mathbb{N}_0$ ist streng monoton fallend, solange $b_i \neq 0$. Das heißt aber $\exists k \in \mathbb{N} : b_k = 0$, das Verfahren terminiert.

ii) Für jeden Durchlauf des Algorithmus gilt, dass a_i und b_i entsprechend Satz 10 gebildet wurden, somit gilt $\forall i \in \mathbb{N} : \text{ggT}(a, b) = \text{ggT}(a_i, b_i)$, also ist insbesondere $\text{ggT}(a, b) = \text{ggT}(a_{k-1}, b_{k-1}) = \text{ggT}(a_{k-1}, 0) = a_{k-1} \in \mathbb{N}$.

iii) Es gilt mit den Gleichungen $(*)$ und $(**)$:

$$\begin{aligned}
\text{ggT}(a, b) &= a_{k-1} \\
&\overset{(*)}{=} b_{k-2} \\
&\overset{(**)}{=} a_{k-3} + b_{k-3} \cdot (-q_{k-3}) \\
&\overset{(*)}{=} b_{k-4} + b_{k-3} \cdot (-q_{k-3}) \\
&\overset{(**)}{=} b_{k-4} + (a_{k-4} + b_{k-4} \cdot (-q_{k-4})) \cdot (-q_{k-3}) \\
&= a_{k-4} \cdot (-q_{k-3}) + b_{k-4} \cdot (1 + q_{k-4} \cdot q_{k-3}) \\
&\overset{(*)}{=} b_{k-5} \cdot (-q_{k-3}) + b_{k-4} \cdot (1 + q_{k-4} \cdot q_{k-3}) \\
&\overset{(**)}{=} b_{k-5} \cdot (-q_{k-3}) + (a_{k-5} + b_{k-5} \cdot (-q_{k-5})) \cdot (1 + q_{k-4} \cdot q_{k-3}) \\
&= a_{k-5} \cdot (1 + q_{k-4} \cdot q_{k-3}) + b_{k-5} \cdot (-q_{k-5} - q_{k-3} - q_{k-5} \cdot q_{k-4} \cdot q_{k-3}) \\
&\ldots
\end{aligned}$$

Mittels der Gleichungen $(*)$ und $(**)$ können a_{k-j} und b_{k-j} für alle $j \in \{2, ..., k\}$ aus ihren Vorgängern hergeleitet werden. Mit geeigneten Umformungen (Distri-

butivität) findet sich immer eine Darstellung

$$\begin{aligned} \text{ggT}(a,b) &= a_{k-j} \cdot \hat{x} + b_{k-j} \cdot \hat{y}, \quad \forall j \in \{2,...,k\} \quad \text{und insbesondere} \\ \text{ggT}(a,b) &= a_0 \cdot \hat{x} + b_0 \cdot \hat{y} \end{aligned}$$

mit $\hat{x}, \hat{y}$, die sich aus Summen und Produkten der verschiedenen q_i zusammen setzen und also $\hat{x}, \hat{y} \in \mathbb{Z}$. Wählt man nun geeignete $x, y \in \mathbb{Z}$, also falls $a < 0$: $x \coloneqq \hat{x}$, sonst $x \coloneqq \hat{x}$, für y analog, so hat man eine Linearkombination $\text{ggT}(a,b) = ax + by$ gefunden.

□

Der obige Beweis liefert zugleich ein konstruktives und nachvollziehbares Verfahren, zur Berechnung der Koeffizienten x, y und somit, wie oben dargestellt, eine Möglichkeit Inverse mod n zu berechnen, so sie denn existieren.

Damit sind fast alle in dieser Arbeit relevanten Bausteine für die Restklassenarithmetik zusammen getragen. Es wird noch eine Möglichkeit der schnellen Potenzierung in Restklassenringen und der *Satz von Euler* dargestellt, der einen besonderen Zusammenhang hinsichtlich bestimmter Potenzen betrifft. Die Umkehrung der Potenzierung, also die Berechnung n-ter Wurzeln ist aus algorithmischer Sicht problematisch. Ähnlich wie auch für das prominentere Faktorisierungsproblem gibt es hier keine bekannten Verfahren, die eine annehmbare, geschweige denn vergleichbare Laufzeit vorweisen können. Dieser Umstand ist die Grundlage der Sicherheit bestimmter, kryptographischer Verfahren und wird später genauer untersucht.

Die k-te Potenz eines gegebenen $a \in \mathbb{Z}/n\mathbb{Z}$ mit einer Zahl $k \in \mathbb{N}$ kann effizient berechnet werden, wenn zunächst k durch seine 2-adische Darstellung substituiert wird, also:

$$k = \sum_{i=0}^{s} k_i 2^i \qquad \text{wobei} \qquad \forall i \in \{0,...,s\} \text{ gilt } k_i \in \{0,1\}$$

Dann gilt durch einfache Potenzumformungen nämlich:

$$a^k = a^{\sum_{i=0}^{s} k_i 2^i} = \prod_{i=0}^{s} (a^{2^i})^{e_i} = \prod_{0 \leq i \leq s, e_i = 1} a^{2^i}$$

Es ist relativ einfach sukzessive die 2er-Potenzen von a zu berechnen, also alle a^{2^i} für alle $0 \leq i \leq s$, insbesondere als Restklassen, da in jedem Rechenschritt immer auf verhältnismäßig handliche Reste „gekürzt“ werden kann. Von diesen brauchen nur noch diejenigen multipliziert werden, deren korrespondierendes $e_i = 1$ ist.

Für den ausstehenden Satz von Euler, der die Grundlagen abschließen wird, definieren wir nun die *eulersche φ-Funktion* bezüglich $n \in \mathbb{N}$, durch die Anzahl aller teilerfremden Zahlen kleiner gleich n:

Definition 7. *Die Funktion*

$$\varphi : \mathbb{N} \to \mathbb{N}, \quad \varphi(n) = |\{a \in \{1, \dots, n\} \mid ggT(a, n) = 1\}|$$

heißt ***eulersche φ-Funktion.***

Für die φ-Funktion gilt folgender Satz:

Satz 12. *Für $p \in \mathbb{N}$ eine Primzahl, ist $\varphi(p) = p - 1$.*

Beweis. Eine Primzahl p hat genau zwei Teiler, nämlich 1 und p selbst. Folglich sind alle Zahlen zwischen 1 und $p - 1$ teilerfremd zu n. Zusammen mit der 1 sind das genau $p - 1$ Zahlen kleiner gleich p, deren ggT gleich 1 ist.

□

Nun kann schließlich der Satz von Euler nachgewiesen werden, der grundlegend für die Umkehrung der Potenzierung in der Kongruenzrechnung ist, welche Eigenschaft

wiederum für den Nachweis der Gültigkeit des RSA-Verfahrens benötigt wird:

Satz 13. ***Satz von Euler***

Für $n \in \mathbb{N}$, $a \in \mathbb{Z}$ gilt:

$$ggT(a,n) = 1 \quad \Longrightarrow \quad a^{\varphi(n)} \equiv 1 \; mod \; n$$

Beweis. Betrachte $(\mathbb{Z}/n\mathbb{Z})^x := \{a \in \mathbb{Z}/n\mathbb{Z} \mid a \text{ invertierbar}\}$. Mit Satz 9 gilt für alle $a \in (\mathbb{Z}/n\mathbb{Z})^x$, dass $\text{ggT}(a,n) = 1$. Es gibt also in $(\mathbb{Z}/n\mathbb{Z})^x$ genau $\varphi(n)$ Elemente, die wir wie folgt bezeichnen und durch zählen können: $(\mathbb{Z}/n\mathbb{Z})^x = \{r_1, \; ... \; , r_{\varphi(n)}\}$.

Betrachte nun die Funktion

$$f : (\mathbb{Z}/n\mathbb{Z})^x \to (\mathbb{Z}/n\mathbb{Z})^x, \quad f(x) = a \cdot x, \quad a \in (\mathbb{Z}/n\mathbb{Z})^x$$

f ist wohl definiert, da für x, y invertierbar $\Longrightarrow 1 \equiv x^{-1}x \cdot y^{-1}y \equiv (x^{-1}y^{-1}) \cdot (xy) \bmod n$ $\Longrightarrow$ (xy) invertierbar. Ferner gilt für alle $a \in (\mathbb{Z}/n\mathbb{Z})^x$, da nach Definition invertierbar, dass aus $ax \equiv ay \bmod n$ folgt $x \equiv y \bmod n$. Dies zeigt, dass f injektiv ist. Da die Definitionsmenge und die Wertemenge von f nach Definition gleichmächtig und endlich sind, ist f bijektiv und insbesondere eine Permutation.

Damit gilt für die oben benannten Elemente $r_1, \; ... \; , r_{\varphi(n)}$ von $(\mathbb{Z}/n\mathbb{Z})^x$ und $a \in (\mathbb{Z}/n\mathbb{Z})^x$ (also $\text{ggT}(a,n) = 1$) folgender Zusammenhang:

$$r_1 \cdot ... \cdot r_{\varphi(n)} \overset{\text{(Permutationseigenschaft)}}{\equiv} ar_1 \cdot ... \cdot ar_{\varphi(n)} \equiv r_1 \cdot ... \cdot r_{\varphi(n)} \cdot a^{\varphi(n)} \bmod n$$

Mit der Invertierbarkeit der r_i folgt

$$a^{\varphi(n)} \equiv 1 \bmod n$$

□

3.2 Kryptographie und Kryptosysteme

Der Begriff der *Kryptographie* beruht auf den altgriechischen Wörtern κρυπτός, zu deutsch *heimlich*, *verheimlicht*, *verborgen* und γράφειν, zu deutsch *schreiben*. Demnach geht es bei der Kryptographie um Geheimschriften, also Verfahren, um die *Vertraulichkeit* von Schriftstücken, oder Nachrichten, zu gewährleisten. Dieses Ziel wird durch Verschlüsselung (*Chiffrierung)* der ursprünglichen Nachrichten (*Klartexte*) in unverständliche Zeichenfolgen (*Chiffretexte*) angestrebt. Nur der legitime Empfänger soll in der Lage sein, die Verschlüsselung umzukehren, den Chiffretext also in den zugehörigen Klartext zu entschlüsseln (*dechiffrieren*). Dazu ist ein *Schlüssel* erforderlich, eine geheime Information, die die Ver- und die Entschlüsselung möglich macht.

Gelegentlich wird auch der Begriff der *Kryptologie* verwendet, teils als synonyme Entsprechung zur Kryptographie, teils sogar diffus vermischt.[10] Begrifflich mag es näher liegen den Bereich der Wissenschaft geheimer Nachrichtenübermittlung als Kryptologie zu fassen und insbesondere die *Kryptoanalyse*, das ist die Lehre vom Entschlüsseln oder ‚Brechen' kryptographischer Verfahren ohne Kenntnis des Schlüssels, als Gegenstück zur Kryptographie in Anschlag zu bringen und im Begriff der Kryptologie zusammen zu fassen. Da aber erstens unter Kryptographie meist beides gefasst wird[11] und zweitens ‚reine' Kryptographie, ohne die Methoden der Kryptoanalyse, ihre eigenen Zielsetzungen nur schwer überprüfen kann, wird in dieser Arbeit die synonyme Auffassung vertreten und vom Begriff der Kryptologie abgesehen.[12]

Anzufügen ist noch die Unterscheidung zur Steganographie, welche sich mit dem Verstecken von Nachrichten befasst, in dem Sinne, dass nicht legitimierten Teilnehmern der Kommunikationskette die Existenz der Nachricht verborgen bleibt, wohingegen die Kryptographie die Existenz nicht verschleiert, sondern lediglich die Bedeutung. Die Steganographie wird in dieser Arbeit nicht genauer betrachtet, oder in der Un-

[10] Vgl. Beutelspacher 2002, S. viii.
[11] Vgl. etwa Buchmann 2001, Titel.
[12] Vgl. insg. Küsters & Wilke 2011, S. 1.

terrichtsreihe zur Anwendung gebracht, ist aber aufgeführt, aufgrund der Möglichkeit ihrer Relevanz in der freien Auseinandersetzung der Kinder mit der Zielsetzung der geheimen Nachrichtenübermittlung.

Die moderne Kryptographie im Zeitalter der Informationstechnologie umfasst über den Bereich der Geheimhaltung oder Vertraulichkeit hinaus noch weitere, bereits in der Einleitung dieser Arbeit angesprochene Ziele, die zwar in der Unterrichtsreihe nicht unmittelbar und im Detail adressiert werden, aber gerade in den höheren Klassenstufen als erweiternde Information diskutiert werden können. Die Ziele sind *Authentizität*, also die Überprüfbarkeit der Urheberschaft von Nachrichten, oder Daten allgemein, sowie *Integrität* von Nachrichten oder Daten, also die Nachweisbarkeit, dass Daten unverändert und vollständig sind. Ferner kann *Verbindlichkeit* als Ziel angesehen werden, welche – ähnlich der Authentizität – die Urheberschaft betrifft, aber deren Nachweisbarkeit gegenüber dem Urheber fokussiert.

Ganz allgemein kann ein Verfahren der Verschlüsselung und Entschlüsselung, ein sogenanntes *Kryptosystem* wie folgt definiert werden:

Definition 8. *Ein **Kryptosystem** ist ein 5-Tupel $\{\mathcal{P}, C, \mathcal{K}, \mathcal{E}, \mathcal{D}\}$ mit den Eigenschaften:*

1. *$\mathcal{P}$ ist eine endliche Klartextmenge (plaintexts).*
2. *C ist eine endliche Chiffretextmenge (ciphertexts).*
3. *$\mathcal{K}$ ist eine endliche Schlüsselmenge (keys).*
4. *$\mathcal{E} = \{E_k \mid k \in \mathcal{K}\}$ ist eine (endliche) Menge von Funktionen $E_k : \mathcal{P} \to C$, die Verschlüsselungsfunktionen heißen (encryption).*
5. *$\mathcal{D} = \{D_k \mid k \in \mathcal{K}\}$ ist eine (endliche) Menge von Funktionen $D_k : C \to \mathcal{P}$, die Entschlüsselungsfunktionen heißen (decryption).*
6. *Für alle $e \in \mathcal{K}$ existiert $d \in \mathcal{K}$, so dass für alle $p \in \mathcal{P}$ der Zusammenhang $D_d(E_e(p)) = p$ gilt.*

Mit anderen Worten handelt es sich um ein Verfahren, dass mittels Ver- und Ent-

schlüsselungsfunktion (E_e, D_d), welche durch die Wahl von zwei zugehörigen, nicht notwendigerweise gleichen, Schlüsseln (e, d) bestimmt sind, Klartexte (p) auf Chiffretexte (c) abbilden kann, so dass diese Verschlüsselungsfunktion durch die korrespondierende Entschlüsselungsfunktion eindeutig umkehrbar ist, also der ursprüngliche Klartext (p) rekonstruierbar ist. Dies erfordert, dass die Funktionen in $\mathcal{E}$ injektiv und also die Funktionen in $\mathcal{D}$ surjektiv sind. Damit folgt unmittelbar:

Satz 14. *Für ein Kryptosystem* $\{\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}\}$ *gilt:* $|\mathcal{P}| \leq |\mathcal{C}|$

Es werden zwei grundlegende Formen von Kryptosystemen unterschieden. *Symmetrische* Kryptosysteme nutzten Schlüssel für die Ver- und Entschlüsselung, die in einem engen Zusammenhang stehen, das heißt, aus dem einen kann der jeweils andere ohne große Schwierigkeiten abgeleitet werden. Dagegen besteht bei *asymmetrischen* Kryptosystemen kein solcher Zusammenhang zwischen den beiden Schlüsseln. Man unterscheidet zwischen dem *öffentlichen* und dem *privaten* Schlüssel – aus diesem Grund hat sich auch der Begriff *public-key*-Kryptographie eingebürgert. Mit dem öffentlichen Schlüssel werden Klartexte verschlüsselt, aber nur der Besitzer des privaten Schlüssels kann mit diesem den Chiffretext wieder entschlüsseln.

Symmetrische Verschlüsselungsverfahren gibt es schon seit der Antike. Das klassische Beispiel ist die Cäsar-Chiffre (mit festem Schlüssel $e = 3$), oder allgemeiner die Substitutionschiffre (mit beliebigem Schlüssel $e \in \mathcal{K} = \{0, \ldots, 26\}$), bei der jeder Buchstabe des Klartextes auf denjenigen Buchstaben des Alphabets abgebildet wird der e Stellen später auftritt. Wird das Ende des Alphabets erreicht, beginnt man wieder von Vorne – ein Vorgehen, dass sich durch Kongruenzrechnung modellieren lässt. Die beiden Schlüssel für Ver- und Entschlüsselung können leicht aus dem jeweils anderen berechnet werden, denn es gilt der enge – also leicht zu berechnende – Zusammenhang $e = -d$. Damit handelt es sich in der Tat um ein symmetrisches Kryptosystem.

In der vorliegenden Unterrichtsreihe werden Substitutionschiffren und affine Chiffren, also Chiffren die nicht nur additiv, sondern auch multiplikativ operieren, betrachtet.

Im Unterrichtskontext wird von Verschiebechiffren und multiplikativen Chiffren beziehungsweise kombinierten Chiffren gesprochen. Dabei werden diese zunächst und in der Hauptsache nur *monoalphabetisch* aufgefasst, das heißt eine einzelne Verschlüsselungsoperation betrifft je die einzelnen Zeichen des zugrundeliegenden Alphabets. Das bedeutet insbesondere, dass auf jedes Zeichen derselbe Schlüssel angewendet wird. Im Gegensatz dazu ist eine *polyalphabetische* Chiffre, wenn Teile des Klartextes als Blöcke durch einen Schlüssel verschlüsselt werden, der für die einzelnen Zeichen eines Blockes je unabhängig beschaffen ist. Durch kombinatorische Eigenschaften erhöht sich so die Anzahl möglicher Schlüssel. Die ausführliche Darstellung der in der Unterrichtsreihe betrachteten Verfahren erfolgt weiter unten übersichtlich in Abschnitt 3.4.

Diese klassischen Verschlüsselungsverfahren sind mit Blick auf die Berechnungsmöglichkeiten moderner Computer und auch hinsichtlich moderner Sicherheitsparadigmen (vgl. Abs. 3.3) obsolet und dienen nur noch didaktischen und historischen Zwecken. Es soll deshalb auch eine vereinfachte Form des DES, des Data Encryption Standard, im Unterricht erprobt werden, um einen Einblick in die, an moderne Chiffrierverfahren gestellten, Notwendigkeiten zu erhalten. Der DES wurde 1977 von der US-Regierung als Standard für EDV-Systeme festgelegt und hat sich danach international durchgesetzt und lange Jahre erhalten. Heute gilt er als veraltet und ist etwa durch den AES (Advanced Encryption Standard) abgelöst worden. Er kann dennoch exemplarisch für moderne, symmetrische Verfahren analysiert werden. Im schulischen Kontext und also in dieser Arbeit ist es zielführend lediglich den sogenannten Simplified DES zu untersuchen, der prinzipiell wie der DES arbeitet, aber hinsichtlich des Rechenaufwands wesentlich weniger aufwendig ist. Ziel moderner Chiffren, wie dem DES ist einerseits, statistische Eigenschaften von Klartexten zu verschleiern, um etwa durch statistische Häufigkeitsanalysen von Zeichen (-ketten) nicht angreifbar zu sein, und andererseits nicht auf affin lineare Chiffren reduzierbar zu sein, da diese durch Known-Plaintext-Attacken grundsätzlich kompromittierbar sind.[13] Dies wird in Abschnitt 3.4 noch näher

[13] Vgl. Buchmann 2001, S. 80f.

beleuchtet.

Asymmetrische Verschlüsselung ist für die moderne Kryptographie, hinsichtlich weltweiter Netzwerke, unabdingbar. Mit steigender Teilnehmerzahl eines Systems, in dem für jede mögliche Paarung zweier Teilnehmer verschlüsselte Kommunikation möglich sein soll, steigt der Bedarf an Schlüsseln bei symmetrischer Verschlüsselung quadratisch an. Der n-te Teilnehmer benötigt für den Kontakt zu den anderen $n-1$ Teilnehmern eben so viele Schlüssel (beziehungsweise Schlüsselpaare), der $(n-1)$-te entsprechend $n-2$ Schlüssel, und so weiter, also sind insgesamt $\sum_{k=1}^{n-1} k = \frac{n(n-1)}{2}$ Schlüssel nötig. Diese müssen jeweils geheim übertragen werden, was im Sinne der Sicherheit sehr problematisch ist. Dagegen sind bei asymmetrischer Verschlüsselung für n Teilnehmer nur n Schlüsselpaare notwendig und das Problem der Schlüsselübertragung entfällt gänzlich.[14]

Weiter können durch asymmetrische Kryptosysteme die oben angeführten Ziele der Authentizität, Integrität und Verbindlichkeit realisiert werden, wenn das Verfahren umkehrbar ist, in dem Sinne, dass der öffentliche Schlüssel die Entschlüsselung von durch den privaten Schlüssel erzeugte Chiffretexte ermöglicht. Der Sender einer Nachricht verschickt diese einmal unverschlüsselt und einmal verschlüsselt mit seinem privaten Schlüssel. Der Empfänger entschlüsselt die zweite Nachricht und vergleicht sie mit der ersten. Sind sie identisch, so muss der Verfasser der Nachricht im Besitz des privaten Schlüssels sein, wodurch Authentizität und Verbindlichkeit erfüllt werden. Ferner ist die Datenintegrität gewahrt, denn ein Angreifer ist nicht in der Lage, den Chiffretext derart anzupassen, dass er in entschlüsselter Form mit den vollzogenen Änderungen des Klartextes übereinstimmt.

Das erste asymmetrische Verschlüsselungsverfahren ist das nach seinen Erfindern Ron Rivest, Adi Shamir und Len Adleman benannte RSA-Verfahren, das 1977 im An-

[14] Es ergeben sich in der Folge natürlich neue Schwierigkeiten, beispielsweise das Problem der Sicherstellung, dass ein veröffentlichter Schlüssel tatsächlich dem intendierten Empfänger gehört und nicht etwa im Rahmen eines „Man-in-the-middle-Angriffs“ gefälscht wurde. Diese fortgeschrittene Problematik wird hier jedoch außen vor gelassen.

schluss an die ein Jahr zuvor erfolgte, theoretische Grundlegung der Idee der asymmetrischen Verschlüsselung durch Whitfield Diffie und Martin Hellman entwickelt wurde.[15] Die mathematische Umsetzung basiert – so wie jedes asymmetrische Kryptosystem – auf so genannten *Einwegfunktionen*, die algorithmisch leicht zu berechnen sind, ihre Umkehrung jedoch nicht, zumindest nicht ohne eine Zusatzinformation. Damit ist gemeint, dass bei geeigneten Bedingungen und in Anbetracht aktueller Rechenleistung die Umkehrung nicht in praktisch relevanter Zeit möglich ist. Wird ein solche Einwegfunktion zur Verschlüsselung verwendet, so ist die Umkehrung, also die Entschlüsselung eben praktisch nicht möglich, es sei denn durch den privaten Schlüssel, also den Besitz der Zusatzinformation.

Die genaue Definition solcher Funktionen und insbesondere die Diskussion darüber, ob sie tatsächlich existieren, oder leicht zu berechnende Umkehrungen bis jetzt einfach nicht gefunden wurden, führt in dieser Arbeit zu weit. Ein konkretes Beispiel einer (vermuteten) Einwegfunktion, auf das sich die RSA-Verschlüsselung in gewisser Weise zurückführen lässt, ist das Faktorisierungsproblem.[16] Dieses Problem ist uralt und zugleich sehr populär, auch über den kryptographischen Bereich hinaus. Seine Bedeutung für die Kryptographie hat die Bemühungen weiter verstärkt, effiziente Algorithmen zur Berechnung zu finden. Trotzdem erreichen moderne Computer bei großen Zahlen schnell ihr Leistungslimit. So nennen Küsters & Wilke etwa als aktuellen Rekord Stand 2011 die Faktorisierung einer 768 Bit langen Zahl (das entspricht 232 dezimalen Stellen) durch ein Netzwerk von „einigen hundert Computern.“, deren Rechenzeit etwa 1500 Jahre auf einem handelsüblichen PC mit 2,2 GHz und 2 GB RAM betragen würde.[17] Laut Wikipedia ist dieser Rekord noch heute aktuell.[18] Dort finden sich auch die Zahl und ihre Primfaktoren.[19] Die *Multiplikation* dieser Primfaktoren kann auf einem handelsüblichen Computer dagegen ohne merkliche Verzögerung

[15] Vgl. etwa Küsters & Wilke 2011, S. 2.
[16] Vgl. Buchmann 2001, S. 119 – 121. Dort führt er aus, dass die Berechnung des privaten Schlüssels äquivalent ist zur Faktorisierung des RSA-Moduls.
[17] (Vgl.) Küsters & Wilke 2011, S.184.
[18] Vgl. *Integer factorization* Art. i.: Wikipedia.
[19] Vgl. *RSA numbers* Art. i.: Wikipedia.

durchgeführt werden.[20]

Ein interessanter Punkt ist die Geschwindigkeit der unterschiedlichen Verfahren. Denn, um eine ausreichende Sicherheit gegen illegitime Entschlüsselungsversuche zu gewährleisten, sind bei asymmetrischen Chiffren die zugrundeliegenden Zahlen derart groß, dass auch die legitimen Rechenvorgänge immerhin um etwa den Faktor 1000 langsamer vonstatten gehen, als dies bei symmetrischen Verfahren der Fall ist.[21] Aus diesem Grund kommen heute häufig sogenannte hybride Verfahren zum Einsatz, bei denen ein Sitzungsschlüssel für ein symmetrisches Verfahren über ein asymmetrisches übermittelt wird, sodass der Großteil der Verschlüsselung symmetrisch stattfinden kann und trotzdem die Vorteile asymmetrischer Systeme hinsichtlich des Schlüsselaustausches zum Tragen kommen.

Es ist aber nicht nur das zugrundeliegende Verschlüsselungs*verfahren* relevant, sondern auch der davon zu unterscheidende *Betriebsmodus*. Ein Verschlüsselungsverfahren verschlüsselt bei einmaliger Anwendung immer einen endlichen Text, oder auch eine endliche Zahl.[22] Bei längeren Texten muss es also mehrfach angewendet werden. *Wie genau* diese Anwendung durchgeführt wird, bezeichnet der Betriebsmodus. Dabei gibt es Betriebsmodi, die als Input Texte fester Länge erhalten und solche, die prinzipiell einen unendlichen Strom von Informationen verarbeiten können. Letztere kommen etwa bei der Verschlüsselung von Echtzeit-Telekommunikation zum Einsatz, bei der auch in Echtzeit verschlüsselt werden muss. In dieser Arbeit wird dagegen nur die erste Variante betrachtet und im Unterricht behandelt.

Der einfachste solche Betriebsmodus ist der ECB-Mode (Electronic Codebook Mode), der einen gegebenen Text entsprechend der Blocklänge des grundlegenden Chiffrierverfahrens aufteilt, gegebenenfalls zu kurze Blöcke durch festgelegte Füllzeichen auffüllt und dann jeden Block nacheinander mit demselben Schlüssel verschlüsselt. Dieser

[20] Getestet auf einem System mit 2,7 GHz i5 Dualcore, 16 GB RAM in Python 3.6.5 und GNU Octave 4.2.2.

[21] Vgl. Swoboda et. al. 2008, S. 28.

[22] Oft beschränkt etwa das Modul des zugrundeliegenden Restklassenrings, in dem gerechnet wird, den verschlüsselbaren Klartext.

Modus ist hinsichtlich statistischer Angriffe unsicher und sollte in realen Anwendungen vermieden werden. In der Unterrichtsreihe soll deshalb der CBC-Mode (Cipherblock Chaining Mode) als ein mögliches Gegenbeispiel behandelt werden. Seine ausführliche Darstellung findet sich wie alle anderen Verfahren auch im übernächsten Abschnitt 3.4.

3.3 Kryptoanalyse und Sicherheit

Die Sicherheit eines Kryptosystems kann durch die Geheimhaltung des Verfahrens selbst, oder hinreichend vieler Anteile davon angestrebt werden. Dieser Ansatz gilt jedoch als veraltet. In der modernen Kryptographie, die Vertraulichkeit in globalen Netzwerk- und Kommunikationssystemen zwischen Milliarden Teilnehmern zu gewährleisten sucht, wird das *Prinzip Kerckhoffs* verfolgt. Dieses fordert, die Sicherheit auf der Geheimhaltung des Schlüssels und nicht auf dem Verfahren zu gründen. Verfahren auf Sicherheitslücken und mögliche Angriffsvektoren hin zu untersuchen ist Aufgabe der *Kryptoanalyse*. Sie unterscheidet verschiedene Angriffsszenarien, gegen die ein Kryptosystem gewappnet sein sollte. Die drei wichtigsten sind:

1. *Ciphertext-only-attack*: Der Angreifer kennt einen, oder mehrere Chiffretexte. Dieser Fall ist immer anzunehmen, denn die Verschlüsselung von Texten dient gerade dazu, sie in chiffrierter Form über unsichere Kanäle zu übertragen.
2. *Known-plaintext-attack*: Der Angreifer kennt zu einem, oder mehreren Chiffretexten die zugehörigen Klartexte. Auch in diesem Fall, wenn etwa einzelne Chiffretexte bereits entschlüsselt wurden, ist es wünschenswert, dass nicht jeder Text, der mit demselben Schlüssel verschlüsselt wurde, kompromittiert ist.
3. *Chosen-plaintext-attack*: Der Angreifer kann zu beliebigen Klartexten zugehörige Chiffretexte erzeugen. Dies ist insbesondere für jede asymmetrische Verschlüsselung der Fall. Ziel ist natürlich auch hier, die Sicherheit anderer, verschlüsselter Texte zu erhalten.

Was aber ist mit dem Begriff Sicherheit gemeint? Wie kann er definitorisch gefasst werden, um ein klares Kriterium zum Beweis der Sicherheit gegebener Systeme zu haben? Der klassische, *informationstheoretische Sicherheitsbegriff* gründet sich auf stochastischen Überlegungen. Naiv ausgedrückt erhöht sich die Sicherheit, je weniger Klartext und Chiffretext zusammenhängen, je weniger Informationen über den Klartext also aus dem Chiffretext abgeleitet werden können. Angenommen auf der Klartextmenge $\mathcal{P}$ ist eine Wahrscheinlichkeitsverteilung Pr gegeben, dann kann die

Wahrscheinlichkeit, dass ein gegebener Chiffretext $c \in C$ und ein möglicher Klartext $p \in \mathcal{P}$ zusammengehören, durch die bedingte Wahrscheinlichkeit $\Pr(p \mid c)$ ausgedrückt werden und ermöglicht so folgende Definition:[23]

Definition 9. *Ein Kryptosystem heißt **perfekt sicher**, wenn $\forall c \in C$ und $\forall p \in \mathcal{P}$ gilt:*

$$Pr(p \mid c) = Pr(p)$$

Perfekt sicher, bedeutet also, dass sich die Wahrscheinlichkeit beliebiger vermuteter Klartexte aus Sicht eines Angreifers nicht durch Kenntnis von Chiffretexten erhöhen beziehungsweise verringern lässt. Mit anderen Worten, verraten Chiffretexte keinerlei Information über den Klartext. Mit dieser Definition gilt:

Satz 15. *Ist das Kryptosystem $\{\mathcal{P}, C, \mathcal{K}, \mathcal{E}, \mathcal{D}\}$ perfekt sicher, so gilt:*

$$|\mathcal{P}| \leq |C| \leq |\mathcal{K}|$$

Beweis. Die Relation $|\mathcal{P}| \leq |C|$ wurde oben bereits gezeigt (Satz 14). Angenommen es existierte ein $p \in \mathcal{P} : \Pr(p) = 0$, so wäre die bedingte Wahrscheinlichkeit $\Pr(p \mid c)$ nicht sinnvoll definierbar. Der Klartextraum $\mathcal{P}$ sei also entsprechend gewählt, so dass die Wahrscheinlichkeit seiner Elemente nicht Null ist.

Perfekte Sicherheit bedeutet dann $\forall c \in C$ und $\forall p \in \mathcal{P}$ gilt: $Pr(p \mid c) = Pr(p) > 0$, das heißt für ein festes p und beliebiges c existiert $k \in \mathcal{K} : e_k(p) = c$, also ist die Funktion $f : \mathcal{K} \to C,\ f(k) = e_k(p) = c$ surjektiv, also gilt $|C| \leq |\mathcal{K}|$.

□

Für perfekte Sicherheit muss es also mindestens so viele Schlüssel, wie Klartexte geben. In Abschnitt 3.4 wird das sogenannte *One-Time-Pad* als Beispiel für ein perfekt

[23] Vgl. Willems 2008, S. 67.

sicheres Kryptosystem vorgestellt und auf seine Eigenschaften hin analysiert. An dieser Stelle soll – ohne Anspruch auf mathematische Exaktheit – die Frage der Schlüsselanzahl genauer betrachtet werden. Offensichtlich ist ein Verfahren, dass nur einen einzigen möglichen Schlüssel hat, absolut unsicher. Angreifer können mit absoluter Sicherheit das Verfahren brechen, indem sie einfach genau diesen Schlüssel verwenden. Wie oben gezeigt wurde, kann das andere Ende der Skala nur erreicht werden, wenn die Schlüsselanzahl die Klartextanzahl erreicht, oder übersteigt. Es liegt die Vermutung nahe, dass die Sicherheit in der Regel also mit steigender Schlüsselanzahl ebenfalls steigt. In jedem Fall ist leicht einzusehen, dass Sicherheit auch graduell erheblich von der Größe des Schlüsselraums abhängt. Je kleiner der Schlüsselraum, desto weniger Klartexte sind potentiell zu einem gegebenen Chiffretext zugehörig, die Wahrscheinlichkeit bestimmter Klartexte muss sich also erhöhen, bis hin zum Extremfall nur eines Schlüssels, in dem Klartexte mit absoluter Sicherheit bestimmbar sind, das System also absolut unsicher ist.

Dieser Umstand ist auch in praktischer Hinsicht einzusehen. Die trivialste Angriffsmethode auf ein Kryptosystem ist bekannt als *Brute-Force-Attacke*, bei der systematisch der Schlüsselraum durchprobiert wird, bis ein sinnvoller Klartext gefunden ist. Je größer der Schlüsselraum, desto länger dauert die Suche. Insbesondere erhöht sich zudem die Wahrscheinlichkeit, *mehrere* sinnvolle Klartexte zu finden bis hin zur perfekten Sicherheit des One-Time-Pads, bei dem zu einem gegebenen Chiffretext für jeden Klartext, also auch für jeden sinnvollen Klartext des Klartextraums ein passender Schlüssel gefunden werden kann.

Vor diesem Hintergrund erschließt sich auch ein praktikablerer Ansatz der Definition von kryptographischer Sicherheit. Obiger Sicherheitsbegriff war auch als informationstheoretischer Sicherheitsbegriff bezeichnet worden. Dagegen gründet sich der *algorithmische Sicherheitsbegriff* auf einem anderen, praxisorientierteren Paradigma: Als sicher wird angesehen, was mit bekannten Algorithmen oder Methoden nicht in relevanter Zeit, auf der Grundlage der Berechnungsmöglichkeiten aktueller Computer ge-

brochen werden kann.[24] In Bezug auf Brute-Force-Attacken muss der Schlüsselraum also ausreichend groß sein, dass einfaches Durchprobieren praktisch zu aufwendig und langwierig ist.

Der algorithmische Sicherheitsbegriff ist maßgeblich bei der Bewertung von asymmetrischen Kryptoverfahren, denn diese basieren ja auf mathematischen Funktionen, die prinzipiell umkehrbar sind, das heißt aus informationstheoretischer Sicht liefert die Kenntnis des öffentlichen Schlüssels zugleich auch Kenntnis über den privaten und somit ist jeder Chiffretext theoretisch entschlüsselbar. Aber in der Tat ist es, bei geschickter Wahl der Funktionen und bestimmten Rahmenbedingungen, praktisch eben nicht möglich den privaten Schlüssel aus dem öffentlichen Schlüssel – oder auch aus gegebenen Klartext-Chiffretextpaaren – zu berechnen. Mit anderen Worten: Es sind keine Algorithmen bekannt, die nach heutigem und für die nahe Zukunft prognostizierten Stand der Technik in der Lage sind, das Verfahren zu brechen – das Verfahren ist algorithmisch sicher.

Ein raffinierteres kryptoanalytisches Angriffsprinzip als die Brute-Force-Attacke ist die *statistische Häufigkeitsanalyse*. Es beruht auf der Tatsache, dass bei üblichen Klartexträumen die einzelnen Klartexte in der Regel nicht gleichverteilt sind. Üblicherweise kann ein Klartextraum aufgefasst werden als eine Menge von Tupeln – den einzelnen Klartexten – über einem Zeichenalphabet, also $\mathcal{P} = \mathcal{A}^n$ mit $\mathcal{A}$ die Menge der Zeichen des Alphabets und n die (maximale) Länge der Klartexte. Betrachtet man etwa das reguläre Schriftalphabet mit seinen 26 Buchstaben und darüber Texte in deutscher Sprache, so ist die unterschiedliche Wahrscheinlichkeit von möglichen Texten leicht einzusehen. In der Tat geht die Wahrscheinlichkeit des Großteils der n-Tupel, die durch Kombinationsmöglichkeiten der Zeichen des Alphabets gebildet werden können, gegen Null.

Konkret können etwa einzelne Buchstaben auf ihre Häufigkeit in deutschen Texten untersucht werden. So tritt der Buchstabe *e* am häufigsten auf mit ungefähr 17,40%, es

[24] Vgl. Küsters & Wilke 2011, S. 2f.

folgen die Buchstaben *n*, *i*, *s*, *r* mit 9,78%, 7,55%, 7,22%, 7,00% und so weiter, die Buchstaben *q*, *x* und *y* bilden wenig überraschend das Ende der Skala.[25] Mit diesem Wissen sind monoalphabetische Chiffren bei hinreichend langen Chiffretexten leicht zu knacken. Im Fall von einfachen Substitutionschiffren kann es sogar genügen, dem häufigsten Buchstaben im Chiffretext das *e* zuzuweisen und daraus unmittelbar den Schlüssel zu berechnen. Bei komplexeren Verschlüsselungsverfahren ersetzt man weitere Buchstaben und errät fragliche Buchstaben aus dem Kontext. Dieses Vorgehen kann verbessert werden durch Hinzunahme weiterer statistischer Eigenschaften, beispielsweise ist auch die Häufigkeitsverteilung von Buchstabenpaaren, sogenannten Bigrammen sehr aussagekräftig. Im Kontext der Unterrichtsreihe kommen jedoch nur die Häufigkeiten einzelner Buchstaben zur Anwendung.

Etwas komplizierter stellt sich die Situation bei Blockchiffren dar. Hier sind alle Zeichen eines Blockes unabhängig voneinander, vorausgesetzt, die einzelnen Teile des Schlüssels sind dies auch. Es können jedoch geeignete Teilmengen der Chiffretexte betrachtet werden, deren Zeichen nicht unabhängig voneinander sind. Dies gilt bei einer Blocklänge von *n* nämlich genau für jedes n-te Zeichen. So lässt sich der Chiffretext in *n* Teiltexte zerlegen, die für sich genommen durch statistische Methoden analysierbar sind. Ein konkretes Beispiel wird in Abschnitt 3.4 vorgeführt.

Interessanterweise zeigt sich hier, wie auch schon im Zusammenhang mit Brute-Force-Attacken, dieselbe Eigenschaft der Sicherheit, abhängig zu sein von der Schlüsselanzahl. Wir hatten gesehen, dass bei steigender Blocklänge durch die steigende Schlüssellänge auch die Größe des Schlüsselraums steigt. Dies erhöht aber nicht nur die Sicherheit gegenüber Brute-Force-Attacken, sondern auch gegenüber statistischen Analysen, denn je stärker die analysierbaren Teile zerstückelt werden, desto geringer ist ihr Umfang und desto geringer die statistische Relevanz der Buchstabenhäufigkeiten.

Der DES ist ein Versuch solche Angriffe durch Verschleierung von statistischen Eigenschaften (hier im Bereich von Bit-Kodierungen) zu verhindern. Die Analyse und

[25] Vgl. Beutelspacher 2002, S. 10.

Bewertung, inwieweit dies gelingt, geht weit über den Rahmen dieser Arbeit und insbesondere über den Rahmen der Schule hinaus. Tatsächlich gilt er heute aber als unsicher aufgrund der zu geringen Schlüsselmenge, das prinzipielle Verfahren, also insbesondere hinsichtlich statistischer Angriffe, wird weiterhin als sicher angesehen.[26]

Im Zusammenhang mit asymmetrischer Verschlüsselung wurde oben von Klartext-Chiffretext-Paaren gesprochen, wodurch auf die Eingangs genannten, modernen kryptoanalytischen Angriffsszenarien verwiesen ist. Das Szenario, abgefangene Chiffretexte zu untersuchen, mit dem Ziel den Klartext zu bestimmen, liegt am nächsten und wird in der Unterrichtsreihe auch zunächst bestimmend sein. Die anderen beiden Szenarien sind aber mit Blick auf die globale Vernetzung nicht außer Acht zu lassen. Bei der folgenden Betrachtung spezifischer Verfahren werden sich die hier betrachteten Verfahren der Klasse der affin (linearen) Chiffren als grundsätzlich angreifbar zeigen, mindestens durch Chosen-Plaintext-Attacken und unter günstigen Bedingungen auch durch Known-Plaintext-Attacken. Daraus begründet sich die Notwendigkeit moderner Verfahren, wobei hier nicht diskutiert werden kann, inwieweit etwa der DES tatsächlich den Anforderungen genügt. Es muss hier genügen, davon auszugehen, dass moderne Verfahren wie DES und RSA zumindest wesentlich sicherer sind und viele einfache Probleme vermeiden, die sich bei den betrachteten, klassischen Verfahren gezeigt haben.

[26] Vgl. Swoboda et. al. 2008, S. 57.

3.4 Darstellung konkreter Verschlüsselungsverfahren

In diesem Abschnitt werden diejenigen Kryptosysteme in Anlehnung an Definition 8 vorgestellt und hinsichtlich ihrer Anwendung, als auch – in gewissem Maße – ihrer Sicherheit analysiert, die in der Unterrichtsreihe vermittelt werden. Dabei handelt es sich um einfache Substitutionschiffren, multiplikative Chiffren und ihre Kombination, die beide der Klasse monoalphabetischer, affiner Chiffren zugehören. Ferner die polyalphabetische Erweiterung der Substitutionschiffre als Beispiel einer Blockchiffre und das perfekt sichere One-Time-Pad, eine weitere Blockchiffre. Beispielhaft für die moderne Kryptographie steht der simplifizierte Data Encryption Standard – stellvertretend für symmetrische Verfahren – und das RSA-Verfahren – stellvertretend für asymmetrische Verschlüsselung. Zudem werden noch die Betriebsmodi ECB und CBC betrachtet.

Im Folgenden bezeichnen $\mathcal{P}, C, \mathcal{K}, \mathcal{E}$ und $\mathcal{D}$ gemäß Definition 8 Klartext-, Chiffretext- und Schlüsselmenge, sowie die Menge der Verschlüsselungs- und Entschlüsselungsfunktionen. Mit $\mathcal{A} = \mathbb{Z}/n\mathbb{Z}$ ist eine geeignete numerische Kodierung des zugrundeliegende Alphabets, also des verwendeten Zeichenvorrats durch einen Restklassenring gemeint, entsprechend ist n gleich der Anzahl der Elemente in $\mathcal{A}$. Beispielsweise ist für das reguläre Alphabet $\mathcal{A} = \mathbb{Z}/26\mathbb{Z}$. Mit E_k und D_k sind jeweils Ver- und Entschlüsselungsfunktionen gemeint, also $\forall k \in \mathcal{K}$ gilt $E_k \in \mathcal{E}, D_k \in \mathcal{D}$ und $E_k : \mathcal{P} \to C,\ D_k : C \to \mathcal{P}$.

Definition 10. ***Monoalphabetische Substitutionschiffren***

- $\mathcal{P} = C = \mathcal{K} = \mathcal{A}$
- $E_e(p) = p + e \bmod n$, *mit* $e \in \mathcal{K}$
- $D_d(c) = c + d \bmod n$, *mit* $d \in \mathcal{K}$, *so dass* $e + d \equiv 0 \bmod n$.

Damit ist ein Kryptosystem gegeben, denn für alle $e \in \mathcal{K}$ existiert $d \equiv -e \bmod n$, $d \in \mathcal{K}$, sodass $D_d(E_e(p)) = p, \forall p \in \mathcal{P}$. Es ist zudem symmetrisch, denn der Zusam-

menhang zwischen Ver- und Entschlüsselungsschlüssel ist sehr stark.

Beispiel 2. *Wähle $\mathcal{A} = \mathbb{Z}/26\mathbb{Z}$ als numerische Repräsentation des regulären Alphabets $\{A, ..., Z\}$. In der Tat besteht der „Klartext-" Raum so nur aus einzelnen kodierten Buchstaben. Längere Texte können durch Anwendung der Chiffre auf jeden Buchstaben des Textes verschlüsselt werden (vergleiche ECB-Modus unten). Nach Definition ist $|\mathcal{K}| = 26$. Wird etwa der Verschlüsselungsschlüssel $e = 7$ gewählt, dann ist entsprechend der Entschlüsselungsschlüssel $d \equiv 19 \equiv -7 \equiv -e \ mod\ 26$.*

Die Schlüsselanzahl dieses Verfahrens ist n und damit selbst für umfangreiche Alphabete ziemlich gering. Insofern ist ein Brute-Force-Angriff selbst ohne Computer aussichtsreich. Ebenso ist ein auf statistischer Häufigkeitsanalyse basierender Angriff schon bei recht kurzen Texten, die durch Hintereinanderausführung (ECB) der Chiffre erzeugt wurden, erfolgversprechend, denn es genügt die Dechiffrierung nur eines Zeichens, um den Schlüssel zu erhalten und so den ganzen Text dechiffrieren zu können. Das bedeutet auch, dass der Schlüssel sofort in einem Known-Plaintext- oder gar Chosen-Plaintext-Szenario berechenbar ist.

Definition 11. ***Multiplikationschiffren***

- *$\mathcal{P}$ und $\mathcal{C}$ analog zur Definition 10,* $\mathcal{K} = \{k \in \mathcal{A} \mid ggT(k, n) = 1\}$
- $E_e(p) = e \cdot p \ mod\ n$
- $D_d(c) = d \cdot c \ mod\ n$, *mit* $e, d \in \mathcal{K}$, *so dass* $ed \equiv 1 \ mod\ n$.

Auch hier ist ein symmetrisches Kryptosystem gegeben, denn mit Satz 9 sind alle $e \in \mathcal{K}$ invertierbar und die Berechnung der Inversen mittels des EEA auch problemlos möglich.

Beispiel 3. *Wähle wieder* $\mathcal{A} = \mathbb{Z}/26\mathbb{Z}$*. Dann ist* $|\mathcal{K}| = \varphi(26) = 11$*. Für* $e = 3$ *ist dann etwa* $d = 9$*, denn derart ist* $ed \equiv 27 \equiv 1 \ mod\ 26$*.*

Die Schlüsselanzahl ist hier noch geringer, im Allgemeinen gilt ja $\varphi(n) \leq n$. Auch statistische Häufigkeitsanalysen und Known-/Chosen-Plaintext-Attacken sind ähnlich erfolgversprechend, wie schon oben. Die Situation verbessert sich, wenn beide Verfahren kombiniert werden:

Definition 12. ***Monoalphabetische, affine Chiffren***

- $\mathcal{P}$ *und* C *analog zu Definition 10,*
  $\mathcal{K} = \{(k_+, k_*) \mid k_+, k_* \in \mathcal{A} \wedge ggT(k_*, n) = 1\}$
- $E_e(p) = E_{(e_*, e_+)}(p) = e_* \cdot p + e_+ \ mod\ n$
- $D_d(c) = D_{(d_*, d_+)}(c) = d_* \cdot (c + d_+) \ mod\ n$*, mit* $(e_*, e_+), (d_*, d_+) \in \mathcal{K}$*, so dass* $e_* \cdot d_* \equiv 1 \ mod\ n$ *und* $e_+ + d_+ \equiv 0 \ mod\ n$*.*

Analog zu den vorigen beiden Chiffren ist leicht einzusehen, dass es sich wieder um ein symmetrisches Kryptosystem handelt. Insbesondere lässt sich jede endliche Kombination von monoalphabetischen additiven und multiplikativen Chiffren auf die hier angegebene Form bringen. Es soll hier der Hinweis genügen, dass sich für $e_*, e_+ \in \mathcal{K}$ immer ein geeignetes $\hat{e}_+ \in \mathcal{K}$ finden lässt, so dass $e_* \cdot (m + e_+) = e_* \cdot m + e_* \cdot e_+ = e_* \cdot m + \hat{e}_+$.

Beispiel 4. *Wähle analog zu den vorigen beiden Beispielen* $\mathcal{A} = \mathbb{Z}/26\mathbb{Z}$*. Dann ist die Schlüsselanzahl* $|\mathcal{K}| = \varphi(26) \cdot 26 = 11 \cdot 26 = 286$*. Wähle ebenso analog* $e = (e_*, e_+) = (3, 7)$*. Dann ist entsprechend* $d = (d_*, d_+) = (9, 19)$*, denn es gilt für alle Klartextzeichen* $m \in \mathcal{A} : m \equiv 9 \cdot ((3m + 7) + 19) = D_d(E_e(m))$*.*

Das Beispiel zeigt, dass die Schlüsselanzahl drastisch ansteigt, da der Schlüssel zwei

unabhängige Komponenten hat und so im Allgemeinen $|\mathcal{K}| = \varphi(n) \cdot n$ gilt. Somit sind Brute-Force-Angriffe zumindest von Hand erschwert, gegen computergestützte Angriffe fällt die Schlüsselmenge dagegen kaum ins Gewicht. Vergleiche hierzu den Schlüsselraum des DES (siehe unten), der heute in annehmbarer Zeit durchsuchbar ist. Im Hinblick auf statistische Analysen lässt sich die Sicherheit durch die Kombination von additiven und multiplikativen Chiffren nicht erhöhen, da es sich weiter um eine monoalphabetische Chiffre handelt. Unter der Voraussetzung von mindestens zwei bekannten Klartext-Chiffretextpaaren führen auch Known-/Chosen-Plaintext-Attacken sicher zum Ziel. Mit dem Hinweis auf die Lösbarkeitsbedingungen linearer Gleichungssysteme, wird hier auf einen formalen Beweis verzichtet.[27]

Definition 13. ***Polyalphabetische Substitutionschiffren***

- $\mathcal{P} = C = \mathcal{K} = \{(m_0, ..., m_s) \mid m_0, ..., m_s \in \mathcal{A}, s \in \mathbb{N}\} = \mathcal{A}^s$
- $E_e(p) = E_{(e_0,...,e_s)}(p_0, ..., p_s) = (p_0 + e_0 \ mod \ n, ..., p_s + e_s \ mod \ n)$
- $D_d(c) = D_{(d_0,...,d_s)}(c_0, ..., c_s) = (c_0 + d_0 \ mod \ n, ..., c_s + d_s \ mod \ n)$, *mit* $e, d \in \mathcal{K}$, *so dass* $e + d \equiv (e_0 + d_0, ..., e_s + d_s) \equiv (0, ..., 0) \equiv 0 \ mod \ n$.

Auch hier liegt ein symmetrisches Kryptosystem vor, denn die fraglichen Eigenschaften in Definition 10 gelten auch für ein s-Tupel. Bei polyalphabetischen Chiffren spricht man auch von Blockchiffren, die allgemein jede Permutation von $\mathcal{P}$ nach C bezeichnen.[28] In der Unterrichtsreihe soll jedoch nur der hier vorgestellte Spezialfall behandelt werden.

Beispiel 5. *Wähle* $\mathcal{A} = \mathbb{Z}/2\mathbb{Z}$ *und als Blocklänge* $s = 8$. *Dann ist die Schlüsselanzahl* $|\mathcal{K}| = 2^s = 2^8 = 256$. *Wähle etwa als Schlüssel* $k = (11100110)_2$. *In der Tat sind*

[27] Vgl. Buchmann 2001, S. 80f.
[28] Vgl. Buchmann 2001, S. 62f.

Ver- und Entschlüsselungsschlüssel gleich, denn es gilt $k + k \equiv (00000000)_2$ *mod n. Ein Ver- und Entschlüsselungsvorgang eines Blocks* $p = (00101101)_2 \in \mathcal{P}$ *sieht dann wie folgt aus:*

$$\begin{aligned} D_k(E_k(p)) &= D_k(E_k(00101101)_2) = D_k((00101101)_2 + (11100110)_2) \\ &= D_k(11001011)_2 = (11001011)_2 + (11100110)_2 \\ &= (00101101)_2 = p \end{aligned}$$

Die Schlüsselanzahl ist im gegebenen Beispiel von der gleichen Größenordnung, wie in Beispiel 12, kann aber leicht vergrößert werden und zwar unabhängig vom betrachteten Alphabet, exponentiell mit wachsender Blockgröße. Damit kann prinzipiell jeder Brute-Force-Angriff in der Praxis unterbunden werden. Auch statistische Angriffe werden erschwert, da statistische Regelmäßigkeiten nur noch auftreten bei Texten mit der vielfachen Länge der Blocklänge s. Ist die Länge des Gesamttextes etwa $l = t \cdot s, t \in \mathbb{N}$, also ein Vielfaches der Blocklänge s, dann gibt es s Teile der Länge t, die untereinander statistisch unabhängig sind, für sich jedoch auf Regelmäßigkeiten untersucht werden können. Das heißt, eine Vergrößerung von l führt zu größerer statistischer Angreifbarkeit, eine Vergrößerung von s wirkt diesem Effekt entgegen. Mit Blick auf Known-/Chosen-Plaintext-Attacken ist festzuhalten, dass analog zur monoalphabetischen Transposition bereits ein Klartext-Schlüsseltext-Paar genügt, das Verfahren zu brechen.

Es wurde mehrfach, insbesondere hinsichtlich monoalphabetischer Chiffren, die wiederholte Anwendung des Verfahrens für längere Texte angesprochen. In der Tat ist die Länge von einem Zeichen für einen Text wenig befriedigend und auch beliebig große Blockchiffren können nicht garantieren, dass sie im Allgemeinen ausreichend für jeden Anwendungsfall sind. Aus diesem Grund werden Chiffren auf der Basis bestimmter Betriebsmodi befähigt, beliebig lange Texte als Eingabe zu verarbeiten. In dieser Arbeit sollen zwei solche Modi vorgestellt werden. Jeder Modus erhält als

Eingabe einen Klartext, der ein Vielfaches der Blocklänge der zugrundeliegenden Chiffre beträgt. (Dieser Zustand kann immer etwa durch Anfügung von vereinbarten Füllzeichen erreicht werden.) Er zerlegt den Text in Blöcke der entsprechenden Länge und verschlüsselt diese in bestimmter Weise hintereinander.

Definition 14. ***Betriebsmodi***

Es sei eine polyalphabetische Substitutionschiffre gegeben,[29] *mit einem Schlüssel* $k \in \mathcal{K}$*, einer Verschlüsselungsfunktion* E_k *und einer Entschlüsselungsfunktion* D_k*. (Gegebenenfalls sind zwei verschiedene Schlüssel* $e, d \in \mathcal{K}$ *zu verwenden.) Der Klartext bestehe aus* $t \in \mathbb{N}$ *Blöcken, also* $p = (p_0, ..., p_t) \in \mathcal{P}^t$*. Entsprechend sei der resultierende Chiffretext bezeichnet durch* $c = (c_0, ..., c_t) \in C^t$

- ***ECB-Mode*** *(Electronic Code Book Mode)*

  Die zugrundeliegende Chiffre wird hintereinander auf alle Blöcke angewendet:

  Verschlüsselung: $c = (c_0, ..., c_t) = (E_k(p_0), ..., E_k(p_t))$

  Entschlüsselung: $p = (p_0, ..., p_t) = (D_k(c_0), ..., D_k(c_t))$.

- ***CBC-Mode*** *(Cipher Block Chaining Mode)*

  Der erste Block wird zunächst mit einem Initialisierungsvektor $i \in \mathcal{A}^s$ *verschlüsselt – im Fall binärer Verfahren also eine XOR-Verknüpfung mit* $i \in \{0,1\}^s$ *– und dann regulär mit der Chiffre verschlüsselt. Alle folgenden Blöcke werden mit dem jeweils vorigen, verschlüsselten Block verschlüsselt (XOR-verknüpft) und dann mit der Chiffre verschlüsselt. Dies zeigt folgende, rekursive Definition:*

  Verschlüsselung: $c_0 = E_k(p_0 + i), \qquad \forall j \in \{1, ..., t\} : c_j = E_k(c_{j-1} + p_j)$

  Entschlüsselung: $p_0 = E_k(c_0) - i, \qquad \forall j \in \{1, ..., t\} : p_j = D_k(c_j) - c_{j-1}$

Der ECB-Mode gilt als unsicher, unter anderem aufgrund der bereits dargelegten, statistischen Angriffsmöglichkeiten. Der CBC-Mode ist eine Weiterentwicklung, die die-

sem Problem Rechnung tragen soll. Eine dezidierte Analyse des CBC-Modes wird in dieser Arbeit nicht vollzogen, da er in der Unterrichtsreihe nur als Lösung für die einfachen statistischen Angriffsmöglichkeiten diskutiert werden soll. In jedem Fall ist leicht einzusehen, dass die hier vorgestellten, simplen, statistischen Angriffe durch den CBC-Mode zunächst verhindert werden.

Die oben durchgeführten Überlegungen zu Abhängigkeit der Sicherheit vom Verhältnis der Blocklänge und der tatsächlichen Textlänge basieren auf der Idee des ECB-Modes. Wird dieser angewendet so vergrößern sich durch den Faktor t die effektiven Klartext- und Chiffretexträume zu $\mathcal{P}^t$ und C^t und enthalten so sicherlich mehr Elemente, als $\mathcal{K}$. Dadurch sind sie nicht perfekt sicher, was etwa Raum für die diskutierten, statistischen Möglichkeiten eröffnet. Wenn nun aber Vorkehrungen getroffen werden, dass dieser Fall nicht eintritt und tatsächlich für die effektiven Räume gilt $\mathcal{P} \leq C \leq \mathcal{K}$, dann ist das Verfahren nach Definition 9 perfekt sicher. Diese Vorkehrungen sind in folgendem Verfahren realisiert.

Definition 15. ***Das One-Time-Pad***

Das One-Time-Pad ist eine polyalphabetische Substitutionschiffre auf dem Alphabet $\mathcal{A} = \mathbb{Z}/2\mathbb{Z}$, es sind also $\mathcal{P} = C = \mathcal{K} = \{0,1\}^s$, wobei s wieder die Blocklänge angibt. Die Schlüsselwahl erfolgt zufällig und gleichverteilt über $\mathcal{K}$ und wird für jeden Verschlüsselungsvorgang erneut und völlig zufällig durchgeführt.

Zunächst handelt es sich nur um einen Spezialfall polyalphabetischer Substitutionschiffren. Die Besonderheit liegt darin, dass über die Eigenschaften des Kryptosystems hinaus, gefordert wird, jeden Schlüssel nur einmal zu verwenden. Darin und in der Forderung der gleichverteilten Schlüsselwahl begründet sich folgender Satz:

Satz 16. *Das One-Time-Pad ist perfekt sicher.*

Beweis. Nach Definition 15 ist der Schlüssel $k \in \mathcal{K}$ für ein Klartext-Chiffretext-Paar

$p \in \mathcal{P},\ c \in C$ gegeben durch $k = p + c$. Es gibt also für jedes solche Paar genau einen Schlüssel k, der im Übrigen zugleich der Entschlüsselungsschlüssel ist. Folglich gilt für die Wahrscheinlichkeit, dass p, c zusammen auftreten:

$$\Pr(p, c) = \frac{\Pr(p)}{|\mathcal{K}|}$$

Da die Schlüssel gleichverteilt sind, gilt ferner für die Summe über alle p:

$$\sum_{\lambda \in \mathcal{P}} \Pr(\lambda, c) = \Pr(c) = \frac{1}{|\mathcal{K}|}$$

Damit gilt für die bedingte Wahrscheinlichkeit:

$$\Pr(p \mid c) = \frac{\Pr(p, c)}{\Pr(c)} = \frac{\Pr(p) \cdot |\mathcal{K}|}{|\mathcal{K}|} = \Pr(p)$$

Mit Definition 9 folgt dann die Behauptung.

□

In der Praxis wird das One-Time-Pad trotz seiner perfekten Sicherheit selten angewendet, da es sehr aufwendig umzusetzen ist. Für jede Nachricht, muss ein eben so langer Schlüssel über einen geheimen Kanal ausgetauscht werden. Für die Kommunikation in Rechnernetzwerken ist dies kaum praktikabel. In Geheimdienstkreisen hat das One-Time-Pad aber offenbar Verwendung gefunden. So beschreibt Beutelspacher, wie die Briten ihre Kommunikation hinsichtlich abgefangener Enigma-Nachrichten durch das One-Time-Pad verschlüsselten, um zu garantieren, dass den Deutschen die Kompromittierung der Enigma verborgen bliebe. Auch soll das One-Time-Pad bei der besonders gesicherten, telefonischen Verbindung zwischen dem Kreml und dem Weißem Haus Anwendung gefunden haben.[30]

Hinsichtlich moderner Rechnernetzwerke dagegen kommen heute andere symmetrische Verfahren zum Einsatz. Als Urvater ist vermutlich der DES (Data Encryption

[30] Vgl. Beutelspacher 2001, S. 52f.

Standard) anzusehen. Wie bereits dargelegt, soll er die klassischen Angriffsszenarien – also insbesondere statistische Angriffe – verhindern. Heute ist er durch die Entwicklung der Rechengeschwindigkeit von Computern durch Brute-Force relativ leicht zu brechen. Dennoch ist er, beziehungsweise in dieser Arbeit seine simplifizierte Form, ein nachvollziehbares Exempel, an dem der heute notwendige Komplexitätsgrad nachvollzogen werden kann. Es wird also im folgenden der Simplified DES (SDES) algorithmisch dargestellt und ein Beispiel durchgerechnet. Dagegen wird nicht die Übereinstimmung mit der Definition von Kryptosystemen nachgewiesen und auch seine Sicherheit nicht im Detail analysiert.

Definition 16. ***Simplified Data Encryption Standard*** *(SDES)*[31]

Der SDES ist eine polyalphabetische Substitutionschiffre mit Alphabet $\mathcal{A} = \mathbb{Z}/2\mathbb{Z}$. Er bildet 12-Bit-Eingabeblöcke mit einem 9-Bit-Schlüssel auf wiederum 12-Bit-Ausgabeblöcke ab und zwar in mehreren Runden, in denen je ein vom 9-Bit-Schlüssel abgeleiteter 8-Bit-Rundenschlüssel verwendet wird.

- *Das heißt es ist $\mathcal{P} = C = \mathcal{A}^{12}$ und $\mathcal{K} = \mathcal{A}^9$.*
- *Verschlüsselung: Sei $t \in \mathbb{N}$ die Anzahl der Runden, dann wird in der Runde $j \in \{1, ..., t\}$ der Rundenschlüssel*

$$k_j = (k_j^{(0)}, ..., k_j^{(7)}), \quad k_j \in \mathcal{A}^8$$

gebildet aus den Komponenten des Hauptschlüssels

$$k = (k^{(0)}, ..., k^{(8)}) \in \mathcal{K}$$

[31] Vgl. Trappe & Washington 2002, S. 98 – 101 zitiert nach: Computer Science at University of Rhode Island 2018.

durch die Vorschrift

$$k_j = (k^{(j-1 \bmod 8)}, k^{(j-1+1 \bmod 8)}, ..., k^{(j-1+7 \bmod 8)})$$

Mit anderen Worten werden der Reihe nach 8 Bits aus dem Hauptschlüssel gewählt, beginnend beim j-ten Bit.

Die Eingabe-Bitfolge $p = (p_0, ..., p_{11})$ *wird initial aufgeteilt in die Hälften* $L_0 = (p_0, ..., p_5)$ *und* $R_0 = (p_6, ..., p_{12})$. *In den folgenden Runden* $j \in \{1, ..., t\}$ *werden* L_j, R_j *rekursiv bestimmt durch*

$$L_j = R_{j-1}, \qquad R_j = L_{j-1} + f(R_{j-1}, k_j) \in \{0,1\}^6$$

Nach der letzten Runde t wird dann der Chiffretext aus L_t *und* R_t *zusammengesetzt. (Man beachte, dass* R_t *und* L_t *in diesem letzten Schritt vertauscht werden):*

$$c = (R_t, L_t) \in \{0,1\}^{12} = C$$

- *Die Funktion* $f : \{0,1\}^6 \times \{0,1\}^8 \to \{0,1\}^6$ *berechnet sich wie folgt: Die 6 Eingabe-Bits werden durch eine Expansionsfunktion e auf 8 Bit erweitert und anschließend mit dem Rundenschlüssel* k_j *XOR-verknüpft. Das resultierende 8-Bit-Tupel*

$$k_j + e(R_{j-1}) = x_j = (x_j^{(0)}, ..., x_j^{(7)}) \in \{0,1\}^8$$

wird aufgeteilt in zwei 4-Bit-Tupel

$$l_j = (x_j^{(0)}, ..., x_j^{(3)}), \; r_j = (x_j^{(4)}, ..., x_j^{(7)}) \in \{0,1\}^4$$

Auf die 4-Bit-Tupel werden nun die sogenannten S-Boxen angewendet, das sind Funktionen die auf 3 Bit reduzieren und diese zugleich durcheinan-

der würfeln. Schließlich ergibt die Zusammensetzung der resultierenden 3-Bit-Tupel das Ergebnis von f, es ist also

$$f(R_{j-1}, k_j) = (S_1(l_j),\ S_2(r_j)) \in \{0,1\}^6$$

Die Expansionsfunktion hat folgende Form:

$$e : \{0,1\}^6 \to \{0,1\}^8, \qquad (x_0, ..., x_5) \mapsto (x_0, x_1, x_3, x_2, x_3, x_2, x_4, x_5)$$

Die Funktionen $S_1, S_2 : \{0,1\}^4 \to \{0,1\}^3$ bilden ab auf Einträge zweier Tabellen (Die S-1-Box und die S-2-Box) und zwar bestimmt das erste Bit des Eingabetupels die Reihe ($0 \to$ 1. Reihe, $1 \to$ 2. Reihe) und die folgenden drei Bit die Spalte ($000 \to$ 1. Spalte, $001 \to$ 2. Spalte, ..., $111 \to$ 8. Spalte).

S-1-Box:

101	*010*	*001*	*110*	*011*	*100*	*111*	*000*
001	*100*	*110*	*010*	*000*	*111*	*101*	*011*

S-2-Box:

100	*000*	*110*	*101*	*111*	*001*	*011*	*010*
101	*011*	*000*	*111*	*110*	*010*	*001*	*100*

- *Entschlüsselung: Hier wird genauso vorgegangen, nur die Reihenfolge der Rundenschlüssel wird umgekehrt, es wird also in der j-ten Entschlüsselungsrunde der Schlüssel k_{t+1-j} verwendet.*

Der Hauptschlüssel ist sowohl für Ver-, als auch für Entschlüsselung derselbe und auch die Rundenschlüssel sind dieselben, sie werden nur in unterschiedlicher Reihenfolge

angewendet. Der SDES ist also ein symmetrisches Verfahren. In der Tat ist er auch ein symmetrisches Kryptosystem, welcher Nachweis hier aber nicht unternommen wird. Gleiches gilt für den regulären DES. Dieser unterscheidet sich vom SDES in der Hauptsache in der Blockgröße und der Menge der Schlüssel. Für den DES sind $\mathcal{P} = C = \mathcal{K} = \{0,1\}^64$, wobei nur 56 Bit der 64 Bits des Schlüssels frei wählbar sind, die anderen dienen der Fehlerkorrektur. Damit ist die Größe des Schlüsselraums $|\mathcal{K}| \approx 7,206 \cdot 10^{16}$, ein Raum, der bereits 1999 durch spezielle Hardware in ungefähr 22 Stunden durchsucht wurde. Auch beim DES wird der Eingabeblock aufgeteilt, hier in 32-Bit-Blöcke. Die interne Funktion f Expandiert zunächst auf 48 Bit, die auf acht 6-Bit-Blöcke aufgeteilt werden, die dann durch acht verschiedene S-Boxen durchmischt und auf 4-Bit-Blöcke abgebildet werden. Zusätzlich werden noch einige weitere Permutationen durchgeführt und die Ableitung der Rundenschlüssel ist etwas komplizierter.[32]

Beispiel 6. *Anwendung des SDES*

Im folgenden werden der Übersichtlichkeit halber die Bit-Tupel durch Interpunktion entweder in Dreier- oder Vierergruppen geordnet. Die Rundenanzahl und der Schlüssel seien

$$t = 2, \quad k = (011.010.111)_2$$

Damit sind die Rundenschlüssel

$$k_1 = (0110.1011)_2, \quad k_2 = (1101.0111)_2$$

Ferner sei die zu verschlüsselnde Nachricht m und dadurch die initialen L_j, R_j gegeben durch

$$m = (101.110.001.011)_2 \quad \Longrightarrow \quad L_0 = (101.110)_2, \quad R_0 = (001.011)_2$$

[32] Vgl. insb. Buchmann 2001, S. 96 – 103 u. Beutelspacher 2002, S. 18f.

- *Runde 1:*

  Expansion und XOR-Verknüpfung mit dem Rundenschlüssel:

  $$e(R_0) = (0001.0111)_2, \quad e(R_0) + k_1 = (0111.1100)_2$$

  Anwendung der S-Boxen und Ausgabe von f:

  $$S_1((0111)_2 = (000)_2, \quad S_2((1100)_2) = (110)_2 \quad \Longrightarrow \quad f(R_0, k_1) = (000.110)_2$$

  Es ergeben sich

  $$L_1 = R_0 = (001.011)_2, \quad R_1 = L_0 + f(R_0, k_1) = (101.000)_2$$

- *Runde 2:*

  $$e(R_1) = (1001.0100)_2, \quad e(R_1) + k_2 = (0100.0011)_2 \quad \Longrightarrow$$

  $$S_1((0100)_2 = (011)_2, \quad S_2((0011)_2) = (101)_2 \quad \Longrightarrow \quad f(R_1, k_2) = (011.101)_2$$

  $$\Longrightarrow \quad L_2 = R_1 = (101.000)_2, \quad R_2 = L_1 + f(R_1, k_2) = (010.110)_2$$

Damit ist also der Chiffretext im Vergleich zum Klartext

$$c = (010.110.101.000)_2, \quad m = (101.110.001.011)_2$$

Die umgekehrte Anwendung der Rundenschlüssel entschlüsselt den Chiffretext wieder:

$$c = (010.110.101.000)_2, \quad \Longrightarrow L_0 = (010.110)_2, \quad R_0 = (101.000)_2$$

- *Runde 1:*

  $$e(R_0) = (1001.0100)_2, \quad e(R_0) + k_2 = (0100.0011)_2 \quad \Longrightarrow$$

$$S_1((0100)_2) = (011)_2, \quad S_2((0011)_2) = (101)_2 \quad \Longrightarrow \quad f(R_0, k_2) = (011.101)_2$$

$$\Longrightarrow \quad L_1 = R_0 = (101.000)_2, \quad R_1 = L_0 + f(R_0, k_2) = (001.011)_2$$

- *Runde 2:*

$$e(R_1) = (0001.0111)_2, \quad e(R_1) + k_1 = (0111.1100)_2 \quad \Longrightarrow$$

$$S_1((0111)_2) = (000)_2, \quad S_2((1100)_2) = (110)_2 \quad \Longrightarrow \quad f(R_1, k_1) = (000.110)_2$$

$$\Longrightarrow \quad L_2 = R_1 = (001.011)_2, \quad R_2 = L_1 + f(R_1, k_1) = (101.110)_2$$

Und es ergibt sich durch L_2 und R_2 wieder $m = (101.110.001.011)_2$.

Nachdem anhand des SDES ein Einblick in moderne, symmetrische Kryptographie gegeben wurde, soll abschließend das RSA-Verfahren als Beispiel für asymmetrische Kryptographie dargestellt werden:

Definition 17. ***RSA-Verfahren***

- *Klartext- und Chiffretextraum hängen bei RSA ab von der Wahl des Schlüssels. Bei der Schlüsselerzeugung wird ein RSA-Modul n gebildet. Es können dann alle natürlichen Zahlen* $p \in \{0, ..., n-1\}$ *verschlüsselt werden. Alle Berechnungen werden in* $\mathbb{Z}/n\mathbb{Z}$ *durchgeführt, also liegt auch der Chiffretext in derselben Menge, wie p.*
- *Schlüsselgenerierung:*

  Wähle zwei Primzahlen $p, q \in \mathbb{P}$, $p \neq q$ *und berechne* $n = p \cdot q$. *Wähle dann*

$$e \in \mathbb{N}, \ 1 < e < \varphi(n), \qquad \textit{so dass} \qquad ggT(e, \varphi(n)) = 1$$

Berechne nun

$$d \in \mathbb{N},\ 1 < d < \varphi(n), \qquad \textit{so dass} \qquad e \cdot d \equiv 1 \ mod\ \varphi(n)$$

Der öffentliche Schlüssel ist das Paar (e, n), der private Schlüssel ist d. Die Primzahlen p, q, sowie $\varphi(n)$ werden nicht mehr benötigt und sollten vergessen werden.

- *Verschlüsselung:*

  Es lassen sich nun Zahlen $0 \leq p < n$ verschlüsseln, es ist also $\mathcal{P} = \{0, ..., n-1\}$. Der Chiffretext $c \in C = \{0, ..., n-1\}$ berechnet sich durch:

$$c \equiv p^e \ mod\ n$$

- *Entschlüsselung:*

  Der Klartext p kann mit d (und n) aus dem Chiffretext c berechnet werden durch

$$p \equiv c^d \equiv (p^e)^d \ mod\ n$$

Bemerkung. *Da p, q prim sind, lässt sich mit deren Kenntnis aufgrund von Satz 12 $\varphi(n)$ leicht berechnen:*

$$\varphi(n) = \varphi(pq) = (p-1)(q-1)$$

Ferner sind p und q in der Praxis sehr groß, also insbesondere ungleich 2. Nun wird e üblicherweise zufällig gewählt und mit dem Euklidischen Algorithmus auf die geforderte Teilerfremdheit getestet. Die Auswahl kann im Vorhinein eingeschränkt werden auf ungerade Zahlen, da p, q ungerade und also $\varphi(n)$ gerade.

Die Möglichkeit der Berechnung von d und die Korrektheit des Verfahrens liefert der folgende Satz:

Satz 17. *Das RSA-Verfahren ist wohldefiniert, das heißt d lässt sich berechnen, wie angegeben, und es ist ein Kryptosystem, die Entschlüsselungsvorschrift erzeugt also immer den ursprünglichen Klartext.*

Beweis. Seien also $p, q \in \mathbb{P}, n = p \cdot q$ und $1 < e < \varphi(n)$, so dass $\text{ggT}(e, \varphi(n)) = 1$. Daraus folgt mit Satz 7: $\exists s, t \in \mathbb{Z}$:

$$1 = s \cdot e + t \cdot \varphi(n) \quad \Longrightarrow \quad t \cdot \varphi(n) = 1 - s \cdot e$$

$$\overset{\text{(Satz 8)}}{\Longrightarrow} \quad \varphi(n) \mid (1 - s \cdot e) \quad \overset{\text{(Satz 8)}}{\Longrightarrow} \quad s \cdot e \equiv 1 \bmod \varphi(n)$$

Wähle also $d = s$.

Sei nun $p \in \mathcal{P}$. Mit $e \cdot d \equiv 1 \bmod \varphi(n) \implies \exists k \in \mathbb{Z}$:

$$e \cdot d = 1 + k \cdot \varphi(n) = 1 + k(p-1)(q-1)$$

Also gilt:

$$(m^e)^d = m^{ed} = m^{(1+k(p-1)(q-1))} = m \cdot \left(m^{(p-1)(q-1)}\right)^k$$

Damit gilt:

$$(m^e)^d \equiv m \cdot \left(m^{(p-1)}\right)^{(q-1)\cdot k} \equiv m \bmod p$$

denn entweder $p \mid m \implies$

$$(m^e)^d \equiv 0 \equiv m \bmod p$$

oder $p \nmid m \implies$

$$m^{(p-1)} \equiv m^{\varphi(p)} \overset{\text{(Satz 13)}}{\equiv} 1 \bmod p \quad \Longrightarrow \quad (m^e)^d \equiv m \cdot 1^{(q-1)\cdot k} \equiv m \bmod p$$

Analog gilt:

$$(m^e)^d \equiv m \cdot \left(m^{(q-1)}\right)^{(p-1)\cdot k} \equiv m \bmod q$$

Das bedeutet aber nach Satz 8:

$$p \mid \left((m^e)^d - m\right) \quad \wedge \quad q \mid \left((m^e)^d - m\right)$$

Nun sind $p \neq q$ Primzahlen, das heißt:

$$(pq) \mid \left((m^e)^d - m\right) \quad \Longrightarrow \quad n \mid \left((m^e)^d - m\right) \quad \Longrightarrow \quad (m^e)^d \equiv m \bmod n$$

Mit dem privaten Schlüssel d lässt sich also aus dem Chiffretext $c \equiv m^e \bmod n$ der Klartext m rekonstruieren.

□

Bemerkung. *Die Existenz von d sichert Satz 7, die Berechnung ist mit dem erweiterten Euklidischen Algorithmus möglich. Zur Berechnung der Potenzen m^e und c^d kann die in Abschnitt 3.1 dargestellte Methode der schnellen Potenzierung angewendet werden.*

Beispiel 7. *RSA-Verfahren mit sehr kleinem Modul (9 Bit)*

- *Schlüsselgenerierung:*

  Seien $p = 17,\ q = 19 \implies$

  $$n = 17 \cdot 19 = 323 \quad \textit{und} \quad \varphi(n) = \varphi(323) = \varphi(17 \cdot 19) = 16 \cdot 18 = 288$$

  Teste zufällig gewählte, ungerade $1 < e < 288$*:*

  $$\begin{array}{llll} \textit{Sei} \quad e = 9 & \overset{(EA)}{\Longrightarrow} \quad 288 = 32 \cdot 9 + 0 & \Longrightarrow & ggT(9, 288) \neq 1 \\ \textit{Sei} \quad e = 11 & \overset{(EA)}{\Longrightarrow} \quad 288 = 26 \cdot 11 + 2 \quad (*) & & \\ & \qquad\quad 11 = 5 \cdot 2 + 1 \quad (**) & \Longrightarrow & ggT(11, 288) = 1 \end{array}$$

  Sei also $e = 11$.

  Berechne $1 < d < 288$ *mit* $ed \equiv 1$ *mod* 288*, das heißt finde mit EEA* $x, y \in \mathbb{Z}$:

$ggT(11, 288) = 1 = x \cdot 11 + y \cdot 288$. Betrachte dazu $(*)$ und $(**)$ im vorigen Schritt. Damit gilt:

$$(*) \quad 2 = 288 - 26 \cdot 11 \qquad \wedge \qquad (**) \quad 1 = 11 - 5 \cdot 2$$

$$\Longrightarrow \qquad 1 = 11 - 5 \cdot (288 - 26 \cdot 11) = -5 \cdot 288 + 131 \cdot 11$$

Damit ist $d = 131$, denn es gilt $11 \cdot 131 - 1 = 5 \cdot 288$, also $11 \cdot 131 \equiv 1$ mod 288. Öffentlicher Schlüssel (e, n) und privater Schlüssel d sind also gegeben durch:

$$(e, n) = (11, 323) \qquad d = 131$$

Die beiden Primzahlen p, q, ebenso wie $\varphi(n)$ werden nicht mehr gebraucht und sollten vergessen werden.

- *Verschlüsselung:*

  Es sei $p = 42$ der zu verschlüsselnde Klartext. Es ist also $p^e \equiv 42^{11}$ mod 323 zu berechnen. Betrachte die 2-adische Darstellung von e:

  $$e = 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$$

  Interpretiert man die Koeffizienten als Bit-Tupel, so kann e übrigens kürzer durch $(1011)_2$ repräsentiert werden. Es werden also die Potenzen 42^{2^i} mod 323 mit $i \in \{0, ..., 3\}$ benötigt:

  $$42^2 \equiv 1764 \equiv 149 \text{ mod } 323$$

  $$42^4 \equiv 149^2 \equiv 22.201 \equiv 237 \text{ mod } 323$$

  $$42^8 \equiv 237^2 \equiv 56.169 \equiv 290 \text{ mod } 323$$

Damit lässt sich der Chiffretext $c \equiv p^e \bmod n$ *leicht berechnen:*

$$p^e \equiv 42^{11} \equiv 42^{2^3} \cdot 42^{2^1} \cdot 42^{2^0} \equiv 42^8 \cdot 42^2 \cdot 42^1 \equiv 290 \cdot 149 \cdot 42 \equiv 1.814.820$$
$$\equiv 206 \; mod \; 323 \quad \Longrightarrow \quad c = 206$$

- *Entschlüsselung:*

  Hier zeigt sich besonders deutlich der Nutzen des schnellen Potenzierens, denn ohne dieses würde zunächst $c^d = 206^{131}$ *berechnet, eine Dezimalzahl mit* 304 *Stellen* ($\approx 1,31 \cdot 10^{303}$)*. Betrachte also die* 2*-adische Darstellung von* d*:*

$$d = 1 \cdot 2^7 + 0 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$$

  Als Bit-Tupel also $(1000.0011)_2$*. Berechnung aller nötigen Potenzen von* 206*:*

$$206^2 \equiv 42.436 \equiv 123 \; mod \; 323$$
$$206^4 \equiv 123^2 \equiv 15.129 \equiv 271 \; mod \; 323$$
$$206^8 \equiv 271^2 \equiv 73.441 \equiv 120 \; mod \; 323$$
$$206^{16} \equiv 120^2 \equiv 14.400 \equiv 188 \; mod \; 323$$
$$206^{32} \equiv 188^2 \equiv 35.344 \equiv 137 \; mod \; 323$$
$$206^{64} \equiv 137^2 \equiv 18.769 \equiv 35 \; mod \; 323$$
$$206^{128} \equiv 35^2 \equiv 1225 \equiv 256 \; mod \; 323$$

  Damit gilt

$$c^d \equiv 206^{131} \equiv 206^{128} \cdot 206^2 \cdot 206 \equiv 256 \cdot 123 \cdot 206 \equiv 6.486.528$$
$$\equiv 42 \; mod \; 323 \quad \Longrightarrow \quad 42 \equiv (42^{11})^{131} \; mod \; 323$$

  Der Chiffretext wurde wieder entschlüsselt.

Zur Sicherheit von asymmetrischen Verfahren wurden bereits der algorithmische Sicherheitsbegriff thematisiert und einige allgemeine Informationen geliefert. Bereits hier hatte sich gezeigt, dass Aussagen über die Sicherheit nicht so leicht zu treffen sind. In Bezug auf das RSA-Verfahren ist zwar beispielsweise bekannt, dass die Berechnung des privaten Schlüssels d aus dem öffentlichen Schlüssel (e, n) äquivalent zum Problem der Faktorisierung des RSA-Moduls n ist, jedoch ist bis heute unbekannt, ob die Faktorisierung tatsächlich schwer ist, oder nur kein effizienter Algorithmus bekannt ist. Auch die Frage ob es prinzipiell schwer ist, ohne Berechnung von d aus Chiffretexten direkt den zugehörigen Klartext zu berechnen, oder lediglich kein praktikables Verfahren gefunden wurde, ist bis heute nicht zu beantworten.[33]

Obige Definition des RSA-Verfahrens hat die Struktur des Schlüsselraums offen gelassen, denn dieser ist nicht trivial zu bestimmen, zudem hängt er von der Wahl der Primzahlen p und q ab. Hinsichtlich dieser Wahl gibt es einige Richtlinien, die für die Sicherheit von Relevanz sind. Zunächst sollten p und q gleichverteilt zufällig und ungefähr gleich groß gewählt werden. Zufällig, da mit ihnen – und im Übrigen auch mit $\varphi(n)$ – der private Schlüssel leicht berechnet werden kann. Da alle drei Zahlen nach der Schlüsselgenerierung nicht mehr benötigt werden, erklärt sich der mehrfache Hinweis, sie anschließend zu vergessen. Je kleiner der private Schlüssel ist, desto aussichtsreicher sind Brute-Force-Angriffe, aber auch sehr kleine öffentliche Schlüssel sind ein Sicherheitsrisiko (Low-Exponent-Attack), weshalb beide ungefähr dieselbe Größenordnung haben sollten.[34]

Die Größenordnung selbst ist ein ungefähres Maß für die Sicherheit, je größer die Primzahlen und damit der RSA-Modul, desto sicherer die Verschlüsselung. Es wurde bereits der Faktorisierungsrekord angesprochen, der bei einer 768-Bit-Zahl liegt. Daraus erklärt sich auch die Einschätzung, dass der RSA-Modul mindestens 512 Bit, besser 1024 Bit oder mehr betragen sollte.[35]

[33] Vgl. Buchmann 2001, S. 115 – 121.
[34] Vgl. Buchmann 2001, S. 122f.
[35] Vgl. Buchmann 2001, S. 121 u. Swoboda et al. 2008, S. 121.

Swoboda et al. führen aus, dass im Bereich von 512 Bit ungefähr $\frac{1}{256}$ aller ungeraden Zahlen Primzahlen sind.[36] Das heißt ungefähr $\frac{2^{512}}{2 \cdot 2^8} = 2^{503} \approx 2,619 \cdot 10^{151}$ Zahlen. Diese Anzahl ist im Vergleich zum Schlüsselraum des DES ($\approx 7,206 \cdot 10^{16}$) unfassbar groß, die Gefahr des Durchprobierens aller Möglichkeiten also im Vergleich zur Gefahr der Faktorisierung offensichtlich zu vernachlässigen. Und in der Tat ziehen Swoboda et al. auch hinsichtlich der Sicherheit einen vorsichtigen Vergleich zwischen 56 Bit symmetrischer, und 512 Bit asymmetrischer Verschlüsselung.[37] Die Anzahl aller Primzahlen ist zwar nicht dasselbe, wie die Anzahl aller privaten Schlüssel, aufgrund der Äquivalenz des Faktorisierungsproblems mit dem Problem der Berechnung von d aus e ist diese Anzahl aber dennoch ein vergleichbarer Indikator zur gewohnten Schlüsselmenge. Diese Anmerkungen zum RSA-Verfahren schließen nicht nur den Abschnitt über Verschlüsselungsverfahren, sondern insgesamt den theoretischen Teil, um im nächsten Teil zur Kryptographie-Unterrichtsreihe zu kommen.

[36] Swoboda et al. 2008, S. 124.
[37] Swoboda et al. 2008, S. 126f.

4. Die Unterrichtseinheiten im Einzelnen

4.1 Jahrgangsstufe 5 – Einführung

4.1.1 Lernziele und Vernetzung

Die erste Unterrichtseinheit muss zunächst eine Heranführung der Kinder an die Kryptographie und ihren Themenbereich, an ihre Idee, Nützlichkeit und Notwendigkeit leisten und zentrale Begriffe und Konzepte einführen. Dabei soll die mathematische Theorie auf ein Minimum beschränkt bleiben und der phänomenale Erlebnisraum für die Kinder so offen, wie möglich gestaltet werden.

Es werden folgende Begriffe eingeführt: Kryptographie (unter Umständen die Abgrenzung zur Steganographie), Geheimschrift, Klartext, Chiffretext, Verschlüsseln und Entschlüsseln. Und weniger zentral: Nachricht, Sender und Empfänger. Konzeptuell lernen die Kinder die mit den obigen Begriffen unmittelbar verbundenen Ideen der geheimen Nachrichtenübermittlung durch Ver- und Entschlüsselung kennen, darüber hinaus die Notwendigkeit der Umkehrbarkeit des Verschlüsselungsverfahrens, die Idee der Trennung von öffentlichem Verfahren und geheimen Schlüssel und das Problem der Schlüsselübermittlung. Auch das Konzept der Kodierung wird zumindest implizit angewendet.

Die Kinder lernen in einfacher Weise das Rechnen mit Kongruenzen. Sie werden mittels des Uhrmodells in elementarer Weise an das Konzept der Restklassenäquivalenz herangeführt und lernen auch die Notation $a \equiv b \bmod n$ mit konkreten Beispielen kennen. Ferner ver- und entschlüsseln sie Texte mit der einfachen Verschiebechiffre, indem das Uhrmodell auf das Alphabet angewendet wird und versuchen bereits spielerisch andere Chiffren zu „knacken“.

Insbesondere ist in dieser ersten Einheit das „Kryptographie-Handbuch“ zu etablieren, das als Lerntagebuch und Ergebnissicherungsheft die Kinder durch alle geplanten Unterrichtseinheiten begleiten soll und zu Beginn einer Einheit die Rekapitulierung der Ergebnisse vergangener Einheiten erlaubt. In dieser Einheit werden gegen Ende exemplarisch einige Vorschläge für die Ergebnissicherung angeführt. In den folgenden Einheiten wird davon abgesehen, da durch die gegebenen Beispiele die Idee des Kryptographie-Handbuchs ausreichend expliziert zu sein scheint und weitere Wiederholungen in dieser Arbeit vermieden werden sollen.

Entsprechend der oben angeführten Zielsetzungen beschränken sich die mathematischen Grundlagen auf Äquivalenzklassen beziehungsweise Kongruenzrechnung, sowie auf genannte, kryptographische Begriffe und die Notwendigkeit der Umkehrbarkeit der Verschlüsselungsfunktion nach Definition 8.

Die Lernvoraussetzungen der Kinder beschränken sich auf einfaches Addieren, Subtrahieren und Dividieren natürlicher Zahlen. Diese sind in der Regel zum Ende der 5. Jahrgangsstufe anzunehmen.[38] Zwar beherrschen die Kinder bereits die Division als Rechenoperation, dennoch scheint die Etablierung der Kongruenzrechnung zunächst auf der Basis der Addition für das phänomenale Verstehen angemessener. Die Erweiterung auf Divisionsreste soll erst im Anschluss erfolgen. Da es sich um die erste Unterrichtseinheit handelt, sind keine Voraussetzungen die Kryptographie betreffend gegeben.

[38] Vgl. Lehrplan Mathematik (Sek I), 10f.

4.1.2 Ausführliche Unterrichtsstruktur

Der Begriff der *Kryptographie* ist ein geeigneter Ausgangspunkt, den Themenkomplex der Unterrichtsreihe zu eröffnen und die erste Aufgabe einzuleiten. Die Kinder können unmittelbar mit dem Begriff konfrontiert werden. Unter Umständen ist er bereits einigen bekannt, andernfalls kann er in seiner Bedeutung als „geheimes Schreiben“ aufgeklärt werden. Dadurch lässt sich unmittelbar das folgende Spiel motivieren:

> *Überlegt euch zusammen, in eurer Gruppe eine Geheimschrift. Verschlüsselt mit dieser Geheimschrift jeweils alleine einen kurzen, einfachen Satz mit höchstens 4 Wörtern und schreibt ihn auf ein eigenes Blatt Papier. Tauscht dann eure Chiffretexte (das sind die verschlüsselten Klartexte) mit euren Gruppenmitgliedern untereinander aus und versucht den jeweils getauschten Chiffretext zu entschlüsseln, also wieder lesbar zu machen.*

Eine kleinere Gruppengröße von zwei bis drei Kindern erscheint angemessen, um die Gruppenkommunikation übersichtlich zu halten und so produktives Arbeiten zu befördern. Die Aufgabenstellung ist vermutlich im Detail zu besprechen, insbesondere die Begriffe *Verschlüsseln*, *Entschlüsseln*, *Klartext* und besonders *Chiffretext* sind erklärungsbedürftig und können in der direkten Anwendung der Aufgabe sinngebend erlernt werden. Die Aufgabe ist hinsichtlich der zu entwickelnden Chiffre absichtlich offen gehalten, in der Hoffnung ein möglichst breites Spektrum an Ergebnissen zu erhalten. Mögliche und erwartbare Ansätze der Geheimschriften der Kinder sind:

- Isomorphe Abbildungen des normalen Alphabets auf andere bekannte Zeichen, beziehungsweise unbekannte Fantasiezeichen.
- Beliebige affine Chiffren. Dabei sind Substitutionschiffren, die im Unterricht einfacher als Verschiebechiffren adressiert werden sollten, eher zu erwarten, oder auch unsystematische, festgelegte Permutationen.

- Steganographische Ansätze, also das Verstecken des Klartextes, beispielsweise in den Anfangsbuchstaben eines Trägertextes. Auch Lochkarten, die nur bestimmte Teile von Textblöcken etwa aus Büchern sichtbar machen, sind als quasi-steganographische Ansätze möglich.
- Geometrische Umordnungen von definierten Textblöcken, also Permutationen von Zeichen- oder Zeichenblockpositionen.

Gegebenenfalls sind einzelne Gruppen durch geeignete Hinweise in der Ideenfindung zu unterstützen, wobei obige Ansätze herangezogen werden können. Ziel ist eine anwendbare, also hinsichtlich der Ver- und Entschlüsselung eindeutige und zudem bezüglich des „Rechenaufwands“ durch die Kinder zu bewältigende Geheimschrift, die im folgenden Teil der Aufgabe untersucht werden kann:

> *Wählt einen eurer Chiffretexte aus, von dem ihr sicher seid, dass er mit dem Wissen über eure Geheimschrift entschlüsselbar ist und gebt ihn der Lehrperson. Jede Gruppe bekommt dann einen Chiffretext einer anderen Gruppe und versucht in der eigenen Gruppe den dazu gehörenden Klartext heraus zu bekommen, das heißt, die Geheimschrift zu „knacken“.*

Auch in diesem zweiten Teil der spielerischen Aufgabe ist die Vorgehensweise offen gehalten. Die Kinder können unbedarft experimentieren und das Phänomen des Spiels zwischen Kryptographie und Kryptoanalyse kennenlernen. Es geht in erster Linie nicht um eine Lösung, sondern um die Erfahrung des Spiels und der beiden grundlegenden Anliegen von Geheimhaltung und Geheimnisaufklärung. Dennoch mag es sich anbieten, je nach Situation, Hinweise hinsichtlich grundlegender Geheimschriftansätze zu geben, oder gar das genaue Verfahren aufzudecken und die Kinder lediglich den Schlüssel finden zu lassen.

Im Anschluss können in einer offenen Diskussion verschiedene, sich im Spiel gezeigte

Aspekte und Probleme vergegenwärtigt und so weitere Ziele der Unterrichtseinheit im Dialog fixiert werden. Eine dezidierte Ergebnissicherung sollte erst zum Ende der Einheit erfolgen, um so zunächst den spielerischen Freiraum offenzuhalten, in dem die Kinder ihr eigenes, freies Verhältnis zur Kryptographie entwickeln können.

Wie auch bei der Gruppenaufgabe selbst, geht es in der Diskussion wieder darum, das Phänomen der Kryptographie als Spiel zwischen Geheimhaltung und Aufklärung näher zu beleuchten und zwar durch phänomenale Beschreibung dessen, was im Verlauf der Gruppenaufgabe beobachtet und erlebt wurde. Die Umkehrbarkeit der Verschlüsselungsfunktion ist dabei ein Konzept, dass in seiner Notwendigkeit und ganz konkret am Beispiel zur Sprache gebracht werden sollte und sich unter Umständen von selbst aus Problemen ergibt, die aus nicht-umkehrbaren Geheimsprachen erwachsen sind. In Bezug etwa auf eine isomorphe Abbildung des Alphabets auf Fantasiezeichen kann gesagt werden:

> *Damit die Geheimsprache sinnvoll zu gebrauchen ist, muss jeder Buchstabe in ein eigenes Zeichen umgewandelt werden. Kein Geheimzeichen darf doppelt verwendet werden und ein Buchstabe darf auch nicht zwei Geheimzeichen bekommen, zwischen denen man wählen kann.*

Eine allgemeinere Formulierung ergibt sich möglicherweise im Unterrichtsgespräch, ist zu diesem Zeitpunkt aber nicht zwingend erforderlich. Weitere Begriffe und Schlüsselkonzepte ergeben sich optional aus der Unterrichtssituation und können in die Diskussion eingebracht werden: Die Unterscheidung des Kryptoverfahrens vom Schlüssel ist möglicherweise anhand der verschiedenen, entwickelten Geheimschriften erläuterbar und aufgrund des Begriffs des Schlüssels kann das Problem der Schlüsselübermittlung und überhaupt das Problem der Praktikabilität angesprochen werden. Auch die Abgrenzung der Kryptographie von etwa steganographischen Verfahren mag sich aus dem Gespräch ergeben. Ein Beispiel einer allgemeineren Formulierung ist etwa:

> *Ein kryptographisches Verfahren dient zur Geheimhaltung von Texten.*

Dabei ist die grundsätzliche Idee meist allen bekannt. Zum Entschlüsseln braucht es aber noch einen Schlüssel, wodurch der Text vor den anderen geschützt ist. Das ist so ähnlich, wie bei einer Schatztruhe mit Schloss: Jeder kann wissen, wie die Truhe und das Schloss funktionieren, nämlich im Prinzip immer gleich. Aber zum Öffnen braucht man trotzdem einen ganz bestimmten Schlüssel.

Das zentrale mathematische Verfahren der Kryptographie ist das Rechnen mit Kongruenzen. Es kann auch ohne Kenntnis über Teilbarkeit oder der Teilung mit Rest, einzig mittels Addition (und Subtraktion), in seinen Grundzügen vermittelt und geübt werden, etwa ausgehend von folgender Frage:

Wenn es jetzt 2h ist, wie viel Uhr ist es dann 11 Stunden später?

Je nach verwendetem Uhrmodell – also 12h- oder 24h-Format – und je nach Interpretation der gegenwärtigen Uhrzeit als 2h Nachts oder 14h Nachmittags, kann hier unterschiedlich gerechnet werden. Diese Offenheit ist beabsichtigt und bringt bereits die Möglichkeit der Verschiedenartigkeit des Moduls der Kongruenzrechnung in Stellung.[39] Werden die verschiedenen Lösungen in Abhängigkeit der Voraussetzungen betrachtet und gewürdigt, ist anzunehmen, dass die Kinder recht schnell das grundlegende Konzept begreifen und *im Kreis* rechnen lernen. Denn dies befördert das Uhrmodell insbesondere: Die Vorstellung einer endlichen Zahlenreihe, deren Ende an den Anfang zurück gebunden ist. Dergestalt ist ein Addieren über das Ende der Zahlenreihe hinaus möglich, da sich die Reihe in der Kreisform unendlich fortsetzt.

Es bietet sich an, einige weitere, einfache Kopfrechenaufgaben im Klassenplenum zu stellen, die sich des Uhrmodells bedienen, und je nach Leistungsspektrum der

[39] Zudem erscheint es erstrebenswert, den Kindern Freiräume in der Interpretation zu ermöglichen, um erstens die Bedeutung von Voraussetzungen erfahrbar zu machen und zweitens Beweglichkeit und nicht Kalkülfixierung im Denken zu fördern.

Kinder dann mit steigendem Schwierigkeitsgrad in einen schriftlichen Übungsteil überzugehen. Dabei ist der Schwierigkeitsgrad einerseits durch größere Zahlen und damit einhergehendem, mehrfachen „Umrunden“ steigerbar, andererseits durch die Wahl anderer Module:

> *Wenn ein Tag 17 statt 24 Stunden hätte und es jetzt 13 Uhr wäre. Wie spät wäre es 35, 42 oder 99 Stunden später?*

Im Anschluss kann die Vorstellung der im Kreis angeordneten, endlichen Menge auf das Alphabet erweitert werden, sodass auf dieser Grundlage Verschiebechiffren in den Blick genommen werden können. Die folgende Aufgabenstellung geht davon aus, dass das Konzept der Verschiebechiffre noch nicht durch die Kinder entdeckt wurde, andernfalls wäre diese Entdeckung natürlich ein Anknüpfungspunkt, der nicht außer Acht gelassen werden sollte.

> *Das „Kreisrechnen“ können wir für Geheimschriften verwenden. Stellt euch vor nicht die Uhrzeiten wären im Kreis angeordnet, sondern die Buchstaben des Alphabets. Wie könnten wir diese Idee für eine Geheimschrift nutzen?*

In der Folge entwickeln die Kinder die Verschiebechiffre im Unterrichtsgespräch soweit möglich selbst und werden soweit nötig durch die Lehrkraft durch Hinweise unterstützt. Sie lernen, dass alle Buchstaben „im Kreis“ um die gleiche Zahl verschoben werden. Konkret kann die als Caesar-Chiffre bekannte Verschiebung um 3 gewählt werden und an Beispielen probiert werden.[40] Anschließend sind auch andere Schlüssel in geeigneter Weise zu erproben, wobei der Begriff des Schlüssels zugleich etabliert

[40] Der Beispielklartext „Caesar“ etwa kann einerseits als Anknüpfungspunkt für die Anekdote um Caesars Chiffre dienen und erfordert kein Überschreiten des Alphabets; „Zebra“ oder gar „Xylophon“ sind dagegen Beispiele, die ein Überschreiten notwendig machen.

werden kann. Auf der Basis eines soliden Verständnisses des Verfahrens, ist mit den Kindern zu hinterfragen, ob das bereits besprochene Erfordernis der Umkehrbarkeit der Verschlüsselungsfunktion erfüllt wird.

Ferner sollte die konzeptuelle Trennung von Verfahren und Schlüssel hier – soweit bereits angesprochen, wieder aufgegriffen, und – anhand der Caesar-Chiffre verdeutlicht und verinnerlicht werden. Daraus ergibt sich auch die Möglichkeit, die Schlüssellänge und das Problem der Schlüsselübertragung zu betrachten. Unter Umständen können auch schon der Schlüsselraum und seine Mächtigkeit ganz naiv angesprochen werden:

> *Wie viele verschiedene Schlüssel gibt es denn? Ist es gut, wenn wir viele Schlüssel haben, oder eher schlecht?*

Unabhängig davon, wie tief obige Konzepte erforscht werden, sollte nun das erlernte Verfahren aus einer kryptoanalytischen Perspektive fokussiert werden:

> *Schreibt eine kurze Nachricht (4 – 5 Sätze) an eine Freundin oder einen Freund. Verschlüsselt diesen Klartext mit dem Verschiebeverfahren, wobei ihr einen Schlüssel auslost.*[41] *Danach erhaltet ihr einen Chiffretext einer anderen Gruppe. Versucht diesen zu entschlüsseln! Bedenkt, wenn ihr einmal den Schlüssel herausbekommen habt, ist der Rest nicht mehr schwer.*

Das Augenmerk dieser Gruppenarbeit liegt erneut weniger auf Vermittlung theoretischer Konzepte, denn auf der unmittelbaren Anwendung des Verfahrens der Verschiebechiffre durch die Kinder, die so einerseits *im Kreis rechnen*, als auch das Verfahren

[41] Es erscheint günstig, die Kinder nicht wählen zu lassen, um eine Häufung einfach zu berechnender Schlüssel zu vermeiden und allgemein die Entropie groß zu halten. Vorbereitete Lose, die von den Kindern gezogen werden, sind eine praktikable Möglichkeit.

selbst üben, und sich zugleich mit zentralen Begriffen und Konzepten der Kryptographie im phänomenalen, theoriefreien Erleben vertraut machen können, etwa Ver- und Entschlüsselung, Klartext und Chiffretext, sowie Verfahren, Schlüssel und in gewisser Weise die Schlüsselübermittlung. Insbesondere lernen die Kinder implizit die Idee der Kodierung von Buchstaben durch zugeordnete Zahlen kennen. Wenn dies auch noch nicht bewusst angesprochen, oder erkannt wird, so kann später darauf zurückgegriffen werden.

Nachdem kryptographische Konzepte und mathematische Grundlagen derart phänomenal erfahren wurden, kann zuletzt noch eine abstraktere Zuspitzung durch Verallgemeinerung der Kongruenzrechnung mittels der Idee der Restklassen beziehungsweise dem Rechnen mit Divisionsresten erfolgen. Es kann etwa von folgender Aufgabe ausgegangen werden:

> *Es ist 0h. Wie spät ist es 41.353 Stunden später?*

Die Berechnung im bekannten Uhrmodell mittels Addition ist äußerst mühselig. Sie kann aber als Ausgangspunkt für die Kinder dienen, den Zusammenhang zwischen etwa fortwährendem Subtrahieren von 24, bis ein Zahl kleiner 24 übrig bleibt, und dem Rest der Division 41353 : 24 = 1723 Rest 1 selbst herzustellen, beziehungsweise durch Anleitung der Lehrkraft kennenzulernen.

Weitere Übungsaufgaben sind in geeigneter Weise anzuschließen, wobei verschiedene Herausforderungen fokussiert werden können: Erstens natürlich – wie in obiger Aufgabe bereits geschehen – Aufgaben mit großen Zahlen, um schriftliches Rechnen zu üben und so Vertrautheit mit der Sache, sowie das Vertrauen in die Rechenfähigkeiten zu fördern. Wie schon vorher, können zweitens unterschiedliche Kongruenzmodule gewählt werden. Drittens ist insbesondere auch die Addition zweier Restklassen mit Blick auf die neue Technik eine Herausforderung. In diesem Zusammenhang kann die übliche Schreibweise beim Rechnen mit Kongruenzen eingeführt werden und so Aufgaben folgenden Typs ermöglichen:

$$a + b \equiv c \ (mod)\ n, \ \textit{mit gegebenen } a, b, n \in \mathbb{N}$$

Je nach den Fähigkeiten der Lerngruppe und den zeitlichen Rahmenbedingungen können auch $a, b \in \mathbb{Z}$, oder a beziehungsweise b anstatt c als unbekannt gewählt werden und im Verlauf der Rechenübungen auch Teile der Rechengesetze (Satz 2) etabliert und expliziert werden.

Abschließend ist eine diskursive Rückbindung der Rechentechniken an die bekannte Verschiebechiffre sinnvoll, um das Kalkül durch einen Sinn zu bereichern und eine Anbindung an die Kryptographie zu erhalten. Ferner bietet sich an, den Begriff der Kodierung einzuführen, indem die implizite Anwendung dieser Idee im Zusammenhang mit Verschiebechiffren expliziert wird.

Zum Ende jeder Einheit ist eine geeignete Ergebnissicherung vorzunehmen, in der die in den Zielsetzungen genannten Begriffe und Konzepte etwa im fragenden Gespräch rekapituliert und anschließend im Kryptographie-Handbuch festgehalten werden. Dabei können für diese Einheit folgende Formulierungen nützlich sein:

> *Kryptographie beschäftigt sich mit Geheimschriften. Dabei geht es darum, Klartexte so in Chiffretexte zu verändern, dass nicht jeder den Klartext erkennen kann. Der Empfänger aber soll den Chiffretext wieder in Klartext umwandeln können.*
>
> *Wir unterscheiden das Verfahren und den Schlüssel. Es ist praktisch, wenn das Verfahren nicht geheim sein muss, sondern nur der Schlüssel. Dann brauchen Sender und Empfänger nur den Schlüssel geheim auszutauschen, was viel einfacher ist, als sich immer wieder ein neues Verfahren auszudenken.*
>
> *Durch eine sinnvolle Geheimschrift muss ein Klartext immer genau in* ***einen*** *Chiffretext umgewandelt werden, egal wer sie benutzt. Und andersherum muss daraus beim Entschlüsseln genau wieder der ursprüngliche*

Text herauskommen und nicht etwas anderes möglich sein.

4.2 Jahrgangsstufe 6 – Restklassenarithmetik

4.2.1 Lernziele und Vernetzung

Diese zweite Unterrichtseinheit dient der Erweiterung und Vertiefung der Kongruenzrechnung. Es wird die Multiplikation eingeführt, sowie die Wohldefiniertheit derselben und auch der Addition in elementarer Weise diskutiert. Das Konzept der Kongruenz wird expliziert durch Erlernen der Zusammenhänge in Satz 8, also insbesondere durch die Regel, dass a und $\hat{a}$ genau dann kongruent modulo n sind, wenn $n \mid (a - \hat{a})$.

Die Überlegungen zur Wohldefiniertheit und damit einhergehend zur Vertreterunabhängigkeit in Restklassen fördern dabei algebraisches Strukturdenken und zwar nicht durch Fixierung auf formale Darstellung, sondern durch argumentative Abstraktion, durch welche sich bekanntes Wissen in andere Bereiche übertragen lässt. Damit werden Restklassen in einer Weise kennengelernt, die als Grundlage für die folgende Einheit dienen kann, in der die äußerst komplexe Methode der Berechnung multiplikativer Inverser modulo n mittels des EEA besprochen werden soll.

Die Addition in Bezug auf Buchstaben des Alphabets konnte noch als Verschiebung in einem kreisförmigen Alphabet vorgestellt werden, die Anwendung der Multiplikation dagegen ist derart kaum zu denken und erfordert die Idee der Kodierung, also der Identifizierung der einzelnen Buchstaben mit Zahlen ($A \leftarrow 0, B \leftarrow 1, ...$).

Nachdem sich die kryptographische Notwendigkeit der *Umkehrung* der Verschlüsselung in der vorigen Einheit noch nicht als großes Problem dargestellt hat, rückt sie in dieser Einheit in den besonderen Fokus, denn die Invertierung der Multiplikation modulo n ist weder garantiert noch trivial. Die Kinder lernen diesen Umstand spielerisch kennen, stellen Vermutungen über Bedingungen der Existenz eines Inversen auf und versuchen Inverse durch Raten und Prüfen zu berechnen.

Die zweite Unterrichtseinheit knüpft unmittelbar an die erste an. Alle erlernten Begriffe werden weiterverwendet, die mathematische Methode der Kongruenzrechnung wird

weiter vertieft und die bekannte, auf der Addition beruhende Verschiebechiffre wird mittels der Multiplikation weiter entwickelt.

Die Begriffe der Teilbarkeit und des Teilers, die im Lehrplan der sechsten Jahrgangsstufe[42] vorgesehen sind, finden in dieser Unterrichtseinheit besondere Anwendung, einerseits ganz explizit in der Rechenregel von Satz 8, als auch mittelbarer hinsichtlich der abstrakteren Auseinandersetzung mit der Kongruenzrechnung. Unter Umständen kann der, im Lehrplan fakultativ vorgesehene Euklidische Algorithmus[43] als Vorbereitung auf die nächste Einheit thematisiert oder aufgefrischt werden.

[42] Vgl. Lehrplan Mathematik (Sek I), S. 14f.
[43] Vgl. Lehrplan Mathematik (Sek I), S. 15.

4.2.2 Exemplarische Unterrichtsstruktur

Im Rückblick auf die vorige Unterrichtseinheit lässt sich aus der geringen Schlüsselanzahl der einfachen Verschiebechiffre die Suche nach zusätzlichen Rechenoperationen motivieren. Die Multiplikation ist hier naheliegend und soll entsprechend in den Blick genommen werden. Dabei stellt sich vor der mathematischen Präzisierung zunächst die Frage, wie Buchstaben multipliziert werden können. Es bietet sich an, hier die Verschiebechiffre der vorigen Einheit mit Blick auf die Kodierung ($A \leftarrow 0, B \leftarrow 1, ...$) in Stellung zu bringen und die Kinder in einer Übung oder einem Spiel Kodierung, Verschlüsselung, Entschlüsselung und abschließende Dekodierung erproben zu lassen, so dass sie die Inhalte der vorigen Einheit erinnern können und sich zugleich mit dem Konzept der Kodierung vertraut machen.

Dergestalt sind die Methoden der Kongruenzrechnung für Addition, als auch Multiplikation motiviert, so dass die zugrundeliegende Mathematik sinnhaft in den Blick genommen werden kann. Die bereits bekannte Schreibweise $a \equiv b \bmod n$ kann gegebenenfalls durch einfache Rechenübungen aufgefrischt werden, um dann die Wohldefiniertheit zu thematisieren.

In dieser Hinsicht ist anzumerken, dass in dieser Arbeit die Kongruenzschreibweise vorgezogen wird, insbesondere als maßgebliche Notation für die Kinder, um die Tatsache hervorzuheben, dass zwei verschiedene Zahlen *nicht* gleich, sondern nur kongruent sind bezüglich eines Moduls. Die im Zusammenhang mit Definition 6 ebenfalls verwendete Schreibweise der Restklassen per Balkennotation ($\overline{a} \in \mathbb{Z}/n\mathbb{Z}$) *kann* an dieser Stelle jedoch gewinnbringend angewendet werden. Es ist im Einzelfall abzuschätzen, ob der Vorteil etwaige, durch die zusätzliche Notation bedingte Verwirrungen überwiegt. In der folgenden Darstellung wird die Balkennotation der Übersichtlichkeit halber verwendet. Im Unterricht kann durch graphische Hilfsmittel, etwa verschiedene Teile von Gleichungen verknüpfende Umrandungen und Pfeile, auch einheitlich die Kongruenzschreibweise verwendet werden.

Wie würdet ihr vorgehen, wenn ihr mehr als nur zwei Zahlen modulo zusammen rechnen wollt – zum Beispiel $7 + 19 + 2 + 23 \equiv$ *? mod n. — Kommt dabei immer Dasselbe heraus, egal wie ihr rechnet?*

Es können ganz konkret etwa folgende Rechenwege ausprobiert werden:

1) $\overline{7 + 19 + 2 + 23} = \overline{51} = \overline{1}$
2) $\overline{7} + \overline{19} + \overline{2} + \overline{23} = \overline{2} + \overline{4} + \overline{2} + \overline{3} = \overline{2 + 4 + 2 + 3} = \overline{11} = \overline{1}$
3) $\overline{7 + 19} + \overline{2 + 23} = \overline{26} + \overline{25} = \overline{1} + \overline{0} = \overline{1 + 0} = \overline{1}$

Die sehr abstrakte Vorstellung der Restklassen als Äquivalenzklassen, die Äquivalenzeigenschaften und die Gleichheit als ein Spezialfall einer Äquivalenzrelation sind für das schulische Umfeld vermutlich zu abstrakt, um gewinnbringend eingebracht werden zu können. Dennoch lohnt ein Versuch, auf einer konkreteren Ebene die Restklassen als etwas kennen zu lernen, dass in einem gewissen Sinne gleich ist und trotzdem nicht dasselbe.

1 *und* 13 *haben modulo* 12 *denselben Rest. Für welche anderen Zahlen gilt das noch? — Wie viele solche Zahlen gibt es denn? — Sagen wir mal, wir werfen alle diese Zahlen, auch wenn es unendlich viele sind, in einen großen Topf und schauen uns dann Zahlen an, die nicht im Topf sind, zum Beispiel* 3.

So kann schrittweise die Vorstellung von verschiedenen Töpfen etabliert werden, deren Inhalte bezüglich eines – dies zu betonen ist wichtig – bestimmten Moduls in gewisser Weise gleich sind, sie haben denselben Rest. Auch die Anzahl aller dieser Töpfe ist dann vermutlich nicht schwer zu bestimmen. Das Bild der Töpfe kann jederzeit die Vorstellungsgabe in Richtung des adäquaten Mengenauffassung der Rest-

klassen erweitert werden, so dass Problemen, die aus der Vorstellung der Restklassen als denjenigen Zahlen mit dem kleinsten Rest erwachsen, begegnet werden kann. Insbesondere kann so sogar unter Umständen die Frage nach der Wohldefiniertheit von Addition und Multiplikation gestellt werden:

> *Jetzt haben wir einfach die Zahlen mit gleichem Rest in unsere Töpfe geworfen. Können wir mit diesen Töpfen denn etwas anfangen? Können wir vielleicht mit ihnen rechnen, und wenn ja, wie? — Wie sind wir denn vorher vorgegangen, da haben wir doch mit solchen Resten gerechnet, oder? — Bei der Uhr haben wir gesagt, dass* 3 *Uhr und* 27 *Uhr irgendwie gleich sind, sie gehören also in einen Topf. Und wenn wir da jetzt eine Stunde dazu rechnen, welche Zahl nehmen wir,* 3 *oder* 27*? — Macht das einen Unterschied?*

So kann das Topf-Modell weiter ausgenutzt werden, um den Begriff des Vertreters zu etablieren und zur Frage der Vertreterunabhängigkeit zu kommen. Diese in Bezug auf beide Grundrechenarten zumindest exemplarisch zu überprüfen und so festzustellen, dass beide tatsächlich weiter so funktionieren, wie gewohnt, ist eine schöne Übungsaufgabe, die zugleich algebraisches Strukturdenken fördert.

Auf der anderen Seite ist hier auch große Vorsicht angebracht, um nicht zu große Verwirrung anzustiften. Ein Gegengewicht können feste Rechenregeln sein, die gewissermaßen wieder festen Boden unter den Füßen erzeugen. Eine Regel, die zu diesem Zeitpunkt einzubringen ist, findet sich in Satz 8. Eine Möglichkeit diese Eigenschaften zu thematisieren, sind sehr große Zahlen:

> *Fällt euch eine einfache und schnelle Methode ein, heraus zu bekommen, ob diese beiden ziemlich großen Zahlen*
>
> 738.046 *und* 738.085

kongruent sind modulo 13*?*

Diese und ähnliche Aufgaben können als Optimierungsproblem angegangen werden. Die Kinder versuchen ihren Lösungsprozess zu optimieren, um mit möglichst wenigen Rechenschritten zum Ziel zu kommen. Die intendierte Lösung ist natürlich, die Differenz auf Teilbarkeit durch 13 hin zu prüfen. Im Zusammenhang mit dem vertieften Verständnis der Restklassen sollten dann alle Zusammenhänge von Satz 8 altersgerecht kennengelernt, nachvollzogen und ihre Anwendung eingeübt werden.

Nachdem nun die sinnvolle Definition der Addition und der Multiplikation durchdacht worden ist und die Idee der Kongruenz weiter verinnerlicht wurde in Verbindung mit obiger Rechenregel und so insgesamt ein angemessener Rahmen geschaffen wurde, um grundlegende arithmetische Berechnungen zu ermöglichen und zu legitimieren, ist das Problem der Invertierbarkeit in den Blick zu nehmen.

Anhand der naiven Erfahrungen aus der vorangegangenen Jahrgangsstufe mit additiven Verschiebechiffren kann die Notwendigkeit der Umkehrbarkeit der Verschlüsselung erneut vergegenwärtigt, und die Realisierung derselben durch das additiv Inverse nachvollzogen werden. Daraus lässt sich die Frage nach dem multiplikativ Inversen motivieren, übrigens ohne dass das Konzept des Inversen zwingend im Detail expliziert werden muss.

> *Um die Verschlüsselung mit einer Verschiebechiffre, bei der ja eine bestimmte Zahl – der Schlüssel – addiert wurde, umzukehren, ziehen wir sie einfach wieder ab. Wir nehmen also denselben Schlüssel nur mit einem Minus. Wie gehen wir beim Multiplizieren vor?*

Die naheliegende Idee der Umkehrung durch Teilung, oder der Multiplikation mit dem multiplikativ Inversen in $\mathbb{Q}$ kann durchaus probiert werden, um die Problematik darzustellen. Folgende Tabelle zeigt das Rechenschema. Auf der linken Seite als

Referenz eine additive Verschiebechiffre mit dem Schlüssel $k = 3$ und auf der rechten Seite analog eine multiplikative Chiffre mit demselben Schlüssel, wobei zur Entschlüsselung versucht wird einfach durch den Schlüssel zu teilen. (Die Schreibweise *aRr* bezeichnet „*a* Rest *r*“.)

Klartext:	H	A	L	L	O	H	A	L	L	O
Kodierung:	7	0	11	11	14	7	0	11	11	14
Verschlüsselung:	10	3	14	14	17	21	0	33	33	42
(kongruent):						21	0	7	7	16
Chiffretext:	K	D	O	O	R	V	A	H	H	Q
Entschlüsselung:	7	0	11	11	14	7	0	2*R*1	2*R*1	5*R*1
Dekodierung:	H	A	L	L	O	H	A	C/D?	C/D?	F/G?

Es wird so das Problem deutlich, dass durch Teilung – selbst wenn man sie zulässt – keine Umkehrung möglich ist, jedenfalls im allgemeinen Fall nicht, wenn durch die vorherige Multiplikation über den „Rand“ hinausgelangt wurde.

Damit stehen die Kinder vor der Frage, wie sonst der Schlüssel für die Entschlüsselung (also das multiplikativ Inverse) gefunden werden kann. Anhand der folgenden Aufgaben, die den Umständen entsprechend erweitert werden sollten, können sie durch freies Ausprobieren ein Gefühl für die Schwierigkeit des Problems bekommen und schrittweise erstens die Unabhängigkeit der Invertierung vom betrachteten Klartext beziehungsweise Chiffretext erkennen, sowie schlussendlich bemerken, dass ein Inverses nicht zwingend gegeben sein muss:

> *Versucht für die folgenden Verschlüsselungsszenarien jeweils genau eine ganze Zahl zu finden, mit der ihr die Verschlüsselung durch Multiplikation mit eurer Zahl rückgängig machen könnt. Versucht also einen Entschlüsselungsschlüssel zu finden:*
>
> 1) *Das Szenario aus obiger Tabelle. — Ergebnis:* $(k_e, k_d) = (3, 9)$.

2) *Ein wie oben kodierter Text ist mit dem Schlüssel* 11 *verschlüsselt worden und der Chiffretext ist „*OSZSKCBSTB*“. — Ergebnis:* $(k_e, k_d) = (11, 19)$*, Klartext: „*GEHEIMTEXT*“.*

3) *In einem speziellen Alphabet gibt es nur* 13 *Buchstaben und der Verschlüsselungsschlüssel ist* 6*. — Ergebnis:* $(k_e, k_d) = (6, 11)$*, Entschlüsselungsschlüssel unabhängig von verschlüsseltem Text.*

4) *Das Alphabet ist wieder das Bekannte, der Verschlüsselungsschlüssel ist nun* 2*. — Ergebnis: Es lässt sich nicht immer ein Inverses finden.*

Die beiden Themengebiete dieser Einheit, Restklassen und ihre Arithmetik, sowie naive Umkehrung der Multiplikation, sollten durch ausreichende Übungen vertieft werden. Sind die Möglichkeiten gegeben, so ist es vorteilhaft den Euklidischen Algorithmus in seiner einfachen Form zu thematisieren, denn in der nächsten Unterrichtseinheit sollen dann Inverse modulo n auf einem abstrakteren Niveau besprochen, und natürlich ihre Berechnung mit dem EEA erlernt werden.

4.3 Jahrgangsstufe 7 – Inverse und der EEA

4.3.1 Lernziele und Vernetzung

Die dritte Unterrichtseinheit zum Ende der 7. Jahrgangsstufe erfordert ein hohes Abstraktionsvermögen. In der vorigen Einheit wurde im Bereich der Kongruenzarithmetik bereits eine Grundlegung im Bereich der Vorstellung der Restklassen, als auch im Bereich von einigen Rechenregeln erreicht. Darüber hinaus wurde bereits die Problematik der Invertierung problemorientiert thematisiert. Nun soll diese Problematik abstrahiert werden, das heißt, losgelöst von dem ursprünglichen Problem, auf das Wesentliche reduziert, betrachtet werden. Die Frage, wie die Multiplikation umgekehrt werden kann, wird überführt in die Frage nach Zahlenpaaren, die multipliziert 1 ergeben. So lernen die Kinder eine fundamentale Methodik der Mathematik kennen, die wissenschaftliche Mathematik erst möglich macht: Abstraktion.

Der Euklidische Algorithmus soll, falls nötig kennengelernt werden. Anschließend wird er erweitert zum EEA, um die Linearfaktordarstellung des ggT zu konstruieren. Falls der ggT des Moduls und einer Zahl gleich 1 ist, kann so durch geschickte Umformungen das Inverse der Zahl gefunden werden. Während diese Umformungen aus theoretischer Sicht wenig spektakulär sind, ist anzunehmen, dass sie für die Kinder dennoch sehr schwer zu verstehen sind, da der Weg zum Ziel erst am Ziel, wie von Zauberhand plötzlich funktioniert. Dieser Eindruck ist in mathematischen Beweisen häufig anzutreffen, für Schulkinder aber eher ungewohnt und nur schwer zu verstehen.

Die zweite, weniger umfangreiche Zielsetzung dieser Einheit ist die gewonnene Möglichkeit multiplikative Chiffren zu analysieren und mit den bekannten Substitutionschiffren zu kombinieren. Dabei wird sich, während nebenher die später benötigte φ-Funktion eingeführt wird, herausstellen, dass multiplikative Chiffren noch weniger mögliche Schlüssel aufweisen, als vergleichbare Substitutionschiffren. Erst die Kombination der beiden Grundrechenarten bringt einen relevanten Mehrwert.

Die Einheit baut auf beide vorigen Einheiten auf, wobei der Schwerpunkt sich stärker

in die algebraische Theorie verschiebt und die kryptographischen Konzepte in den Hintergrund rücken. Dennoch gibt es hinreichend Gelegenheiten, die vorigen Einheiten in Erinnerung zu rufen und so die interne Vernetzung der Unterrichtsreihe zu stärken.

Aus dem regulären Mathematikunterricht wird der für die 6. Jahrgangsstufe fakultativ genannte Euklidische Algorithmus benötigt. Ferner können kombinatorische Kenntnisse aus der Stochastik zum Einsatz gebracht werden. Darüber hinaus hat diese Einheit allerdings wenige Überscheidungspunkte mit dem Lehrplan.[44]

[44] Vgl. Lehrplan Mathematik (Sek I), S. 17 –22.

4.3.2 Exemplarische Unterrichtsstruktur

In Anbindung an die Übungen und Ergebnisse der letzten Kryptographie-Einheit zu multiplikativen Inversen, die sich noch an das konkrete Problem der Umkehrung der Verschlüsselung gehalten hat, kann das Konzept des Inversen nun auf einen höheren Abstraktionsgrad gehoben werden. Das bereits kennengelernte Ergebnis der Unabhängigkeit des Entschlüsselungsschlüssels von Klar- beziehungsweise Chiffretext bei gegebenem Verschlüsselungsschlüssel führt auf die grundlegende Idee des Inversen, welche sich im Zusammenhang $a + \hat{a} \equiv 0 \bmod n$ beziehungsweise $a \cdot \hat{a} \equiv 1 \bmod n$ darstellt, und so erstens zeigt, dass das Inverse nur von der Zahl a selbst und vom Modul n abhängt und zweitens die definitorische Eigenschaft gerade ist, dass die Verknüpfung je nachdem 0 oder 1 ergibt.

> *Die Umkehrung der Verschlüsselung geschieht durch sogenannte* ***Inverse****. Bei der Addition sind zwei Zahlen* ***invers****, wenn sie zusammen addiert* 0 *ergeben, bei der Multiplikation sind sie* ***invers****, wenn sie multipliziert* 1 *ergeben.*
>
> *Ist eine der Verschlüsselungsschlüssel und die andere der Entschlüsselungsschlüssel, dann bewirken sie nacheinander angewendet keine Veränderung, das heißt wir erhalten den ursprünglichen Klartext. Denn bei der Addition rechnen wir insgesamt* 0 *dazu und bei der Multiplikation nehmen wir mit* 1 *mal.*

Derart abstrahiert kann die Frage nach der Existenz und der Berechnung von Inversen nachgegangen werden. Es bietet sich in diesem Zusammenhang an, wie auch schon zuvor, immer wieder additiv Inverse als intuitiv zugängliches Vergleichsmittel heranzuziehen. Die Darstellung derselben Vergleiche im Einzelnen erscheint trivial, weshalb sie hier nicht weiter ausgeführt sind. Im Folgenden ist mit Inversen immer die multiplikative Variante gemeint.

Die Berechnung von Inversen ist bereits als Problem bearbeitet worden, wobei sich unter Umständen bereits der Zusammenhang aus Satz 9, dass Inverse genau dann existieren, wenn Zahl und Modul teilerfremd sind, als aussichtsreiche Hypothese gezeigt hat. Falls nicht können eine Reihe von Aufgaben des Typs *Berechne das Inverse zu a modulo n* Grundlage sein, diese Hypothese zu fassen und zugleich das Interesse an einem handhabbaren Kalkül zu wecken.

Obiger Zusammenhang von Inversen mit dem größten gemeinsamen Teiler verweist auf die üblicherweise in der 6. Jahrgangsstufe behandelte Teilbarkeitstheorie. Während diese kanonisch ist, ist der Euklidische Algorithmus, mit dem sich der ggT berechnen lässt, nur fakultativer Teil des Lehrplans.[45] Es wird im Folgenden im Detail direkt der erweiterte Euklidische Algorithmus adressiert. Je nach Lernstand und Fähigkeiten der Kinder mag es angezeigt erscheinen, zunächst den einfachen Euklidischen Algorithmus zu erforschen. Darüber hinaus kann es notwendig sein, algorithmisches Vorgehen überhaupt erst anhand einfacherer Beispiele zu vermitteln. Hier bietet sich etwa an, das wohl bekannte Verfahren der schriftlichen Division algorithmisch zu beschreiben und erst dann den Euklidischen Algorithmus zu betrachten.

Ist der Euklidische Algorithmus den Kindern in seiner einfachen Form vertraut, kann die Darstellung des ggT als Linearkombination nach Satz 7 in den Blick genommen werden. Hier soll ein mathematik-wissenschaftlicher Blickwinkel eingenommen werden und so die Gelegenheit genutzt werden, die Kinder wissenschafts-propädeutisch in elementarer Weise mit Arbeitsweisen der Mathematiker zu einem gewissen Grade bekannt zu machen. Das heißt, es wird ausgegangen von der Aussage von Satz 7 und seine Nützlichkeit hinsichtlich der Berechnung von Inversen angedeutet. Dann wird an konkreten Beispielen von teilerfremden Zahlen die Linearkombination berechnet und daraus dann das Inverse abgeleitet:

Wir suchen Inverse in der Modulo-Rechnung, das heißt doch wir wollen

[45] Vgl. Lehrplan Mathematik (Sek I), S. 15.

mit etwas multiplizieren, so dass 1 plus beliebig oft unsere Modulo-Zahl herauskommt. Also zum Beispiel so etwas: $42 \cdot ? \equiv 1$ *mod* 31 *oder auch* $42 \cdot ? = 1 +$ *beliebig viele* 31*. Jetzt haben wir schon die Vermutung, dass wir Inverse nur dann finden können, wenn* 42 *und* 31 *keinen gemeinsamen Teiler zusammen haben, der nicht* 1 *ist, also der ggT gleich* 1 *ist. Vielleicht hat ja der ggT, der* 1 *ist etwas mit unserer* 1 *zu tun, die wir mit dem Inversen bekommen wollen? Dazu schauen wir uns den Euklidischen Algorithmus noch einmal genau an. Er berechnet uns ja den ggT. – Wir wollen versuchen, ihn zu erweitern, um den ggT nur mit Vielfachen von den Anfangszahlen* 42 *und* 31 *auszudrücken. Das heißt eine bestimmte Anzahl mal* 42 *plus oder minus eine bestimmte Anzahl* 31*. Wenn der ggT gleich* 1 *ist, können wir so vielleicht das Inverse finden.*

An dieser Stelle können die Kinder unter Umständen zunächst so versuchen die Linearkombination vom ggT$(42, 31)$, oder anderer Beispiele, zu finden. Dadurch kann sich eine grundlegende Vorstellung von deren Beschaffenheit entwickeln, insbesondere die Notwendigkeit, dass es sich um eine Differenz handeln muss. Anschließend ist der einfache Euklidische Algorithmus nach dem folgenden Muster zu erweitern:

$$
\begin{aligned}
42 &= 1 \cdot 31 + 11 && \Longrightarrow && 11 &= 42 - 1 \cdot 31 && \text{(I)}\\
31 &= 2 \cdot 11 + 9 && \Longrightarrow && 9 &= 31 - 2 \cdot 11 && \text{(II)}\\
11 &= 1 \cdot 9 + 2 && \Longrightarrow && 2 &= 11 - 1 \cdot 9 && \text{(III)}\\
9 &= 4 \cdot 2 + 1 && \Longrightarrow && 1 &= 9 - 4 \cdot 2 && \text{(IV)}\\
2 &= 2 \cdot 1 + 0 && && && \text{(V)}
\end{aligned}
$$

Wir wissen also schon einmal, dass der ggT gleich 1 *ist. Jetzt schaut euch die Gleichungen und besonders ihre Umformungen genau an: In der Vorletzten wird der ggT – die* 1 *– mit Vielfachen von* 2 *und* 9 *dargestellt. Diese beiden Zahlen werden darüber aber mit Vielfachen von* 11 *und* 9 *bezie-*

hungsweise 31 *und* 11 *dargestellt. Und auch die* 11 *können wir ersetzen durch Vielfache von* 42 *und* 31. *Wir können also solange ersetzen, bis wir nur noch Vielfache von* 42 *und* 31 *haben, unsere Anfangszahlen. Das ist unser Ziel, probiert es selbst!*

(II) / (III) in (IV):	$1 = (31 - 2 \cdot 11) - 4 \cdot (11 - 1 \cdot 9)$	
	$= 31 - 2 \cdot 11 - 4 \cdot 11 + 4 \cdot 9$	
	$= 31 - 6 \cdot 11 + 4 \cdot 9$	(VI)
(I) / (II) in (VI):	$1 = 31 - 6 \cdot (42 - 1 \cdot 31) + 4 \cdot (31 - 2 \cdot 11)$	
	$= 31 - 6 \cdot 42 + 6 \cdot 31 + 4 \cdot 31 - 8 \cdot 11$	
	$= 11 \cdot 31 - 6 \cdot 42 - 8 \cdot 11$	(VII)
(I) in (VII):	$1 = 11 \cdot 31 - 6 \cdot 42 - 8 \cdot (42 - 1 \cdot 31)$	
	$= 11 \cdot 31 - 6 \cdot 42 - 8 \cdot 42 + 8 \cdot 31$	
	$= 19 \cdot 31 - 14 \cdot 42$	(VIII)
Probe:	$= 589 - 588 = 1$	

Es ist sicherlich vorteilhaft hier eine geeignete Farbkodierung zu nutzen, um die Übersichtlichkeit zu erhöhen, da davon auszugehen ist, dass die notwendigen Umformungen sehr ungewohnt und schwierig für die Kinder sind. Beispielsweise können alle zu ersetzenden Zahlen (11, 9, 2) in roter Farbe und die angestrebten Zielzahlen (42, 31) in grüner Farbe geschrieben werden.

Nun kann das Problem der Inversen wieder in den Blick genommen werden. Ist eine Darstellung $1 = \text{ggT}(a, n) = ax + ny$ für die fragliche Zahl a und das Modul n mit ganzen x, y gefunden, so lässt sich durch die Umformung $ax = 1 - nx$ leicht erkennen, dass a und x invers sind. Dieser äußerst anspruchsvolle Themenkomplex sollte durch umfangreiche Übungen, die einerseits das Verständnis der Zusammenhänge, als auch das

Kalkül der Inversenbestimmung adressieren, abgerundet werden. Anschließend kann die nächste Thematik in den Blick genommen werden:

In der 5. Jahrgangsstufe war bereits die Anzahl aller Schlüssel als Maß für die Sicherheit angedacht worden. Diese Idee ist in Bezug auf die Multiplikation in Erinnerung zu rufen. Dadurch kann erstens der Inhalt von Satz 9 verinnerlicht werden, also die Äquivalenz von der Existenz Inverser und der Teilerfremdheit, und zugleich die eulersche φ-Funktion eingeführt werden. Der Funktionsbegriff kann dabei außer Acht gelassen werden, wenn er den Kindern nicht bekannt ist, es genügt die Schreibweise zu definieren als „Anzahl aller teilerfremden Zahlen, die kleiner als die vorgegebene Zahl in Klammern ist“.

Es stellt sich heraus, dass $\varphi(26) = |\{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}| = 11$ und somit noch weniger Schlüssel existieren, als für die Addition, die Sicherheit für allein multiplikative Verfahren demnach nicht besser ist. Die Kombination von Addition und Multiplikation dagegen erhöht die Schlüsselanzahl drastisch. Dazu ist zu untersuchen, *wie* die Kombination aussehen kann und davon ausgehend, kann die Schlüsselanzahl berechnet werden.

> *Überlegt verschiedene Kombinationsmöglichkeiten, wie Addition und Multiplikation von einer Klartextzahl beziehungsweise einem kodierten Klartextbuchstaben vorgenommen werden können. Schaut dann welche der Möglichkeiten wirklich verschieden voneinander sind.*

Ziel ist es, festzustellen, dass weder die Reihenfolge von Addition und Multiplikation, noch beliebige Häufigkeiten von verschiedenen Schlüsseln (additiv und multiplikativ) einen relevanten Unterschied machen, da sich alle diese Formen auf die affine Form $c = a \cdot m + b$ zurückführen lassen. Auf der Grundlage der ersten stochastischen und also kombinatorischen Inhalte des Mathematikunterrichts der 7. Jahrgangsstufe ist dann die Anzahl aller Schlüssel für affin lineare Verschlüsselungen bezüglich des Alphabets leicht nachzuvollziehen: $26 \cdot \varphi(26) = 286$ und so aus Sicht des Kenntnisstandes der

Kinder eine drastische Verbesserung der Sicherheitssituation erreicht.

4.4 Jahrgangsstufe 8 – Häufigkeit und Sicherheit

4.4.1 Lernziele und Vernetzung

Der Begriff der Sicherheit dient in dieser Unterrichtseinheit als Einstieg und schließt sie zugleich ab. Es soll einerseits die Idee der Blockbildung in der Chiffrierung thematisiert werden und andererseits Kryptoanalyse als legitimer und notwendiger Forschungszweig der Kryptographie dezidiert kennengelernt werden und mit statistischen Methoden ein Angriffsvektor in der unmittelbaren Anwendung erfahren werden. Darauf gründend kann das Verhältnis von Blocklänge, Schlüsselanzahl und Sicherheit und die absolute Sicherheit des One-Time-Pads analysiert werden.

Die Unterrichtseinheit greift damit insbesondere das freie Spiel von Geheimhaltung und Geheimnisaufklärung in der 5. und 6. Jahrgangsstufe in methodisch strukturierterer Weise wieder auf und verortet es als wissenschaftliches Anliegen. Dabei liegt das Augenmerk der Einheit auf dem Sicherheitsbegriff und stützt sich weniger auf die Methoden und Ergebnisse der vorigen beiden Jahrgangsstufen die Restklassenarithmetik betreffend.

Aus dem regulären Mathematikunterricht kommen in ausgezeichneter Weise Inhalte der Stochastik zur Anwendung, die im Lehrplan der Jahrgangsstufen 5 – 8 mit geringem Anteil, aber kontinuierlich Bestandteil sind. Die Kinder kennen absolute und relative Häufigkeiten, Wahrscheinlichkeiten und Zufallsversuche. Dagegen ist der Begriff der bedingten Wahrscheinlichkeit nicht Teil des Lehrplans – dies ist mit Blick auf die Diskussion der Sicherheit zu beachten.[46]

[46] Vgl. Lehrplan Mathematik (Sek I), S. 10 – 27.

4.4.2 Exemplarische Unterrichtsstruktur

Der Umstand, dass Computer nur mit „Nullen und Einsen rechnen“, ist den Kindern sicherlich als Allgemeinplatz geläufig. Wie genau 2-adische Darstellung von Zahlen umgesetzt wird, ist zu diesem Zeitpunkt noch nicht zwingend zu thematisieren, mag sich aber in ungezwungener Form aus dem Unterricht ergeben. Es in ausführlicher Form nur die Vorstellung von Bit-Tupeln als „Blöcken“und die XOR-Verknüpfung benötigt. Die grundlegende, binäre Arbeitsweise von Computern dient hier nämlich in der Hauptsache lediglich als Ausgangspunkt, erneut die Schlüsselanzahl und die damit verbundene Sicherheit in den Blick zu nehmen.

> *Computer haben also im Gegensatz zu uns mit unseren 26 Buchstaben nur ein „Alphabet“ mit zwei „Buchstaben“. Wie ist es da mit der Sicherheit bestellt, wenn wir so verschlüsseln, wie wir es in den letzten Jahren kennengelernt haben?*

In der hier intendierten Interpretation der Bits als einzelne Buchstaben ergibt sich ein sehr kleiner Schlüsselraum von nur zwei Schlüsseln für affine Chiffren. Additiv kann Nichts 0 oder 1 verwendet werden, multiplikativ nur die 1. Mit anderen Worten, gibt es nur einen sinnvollen Schlüssel – also abgesehen vom leeren Schlüssel 0 –, nämlich +1. Dieses Problem kann einzig durch Blockbildung umgangen werden. Diese lässt sich auch aus der Kodierung etwa von echten Buchstaben im Computer motivieren: Diese werden im Computer durch eindeutige Folgen von Bits in bestimmter, festgelegter Länge repräsentiert. Kommt nun ein Schlüssel aus mehreren „Buchstaben“, also Bits zur Anwendung, liegt ein Beispiel für eine Blockchiffre vor.

> *Verschlüsselt den „Text“* 00001010001001110010 *mit dem Schlüssel* 01111*, indem ihr den Chiffretext in Blöcke aufteilt, die genauso lang sind, wie der Schlüssel und dann den Schlüssel jeweils auf die einzelnen Blöcke*

anwendet. — Wie genau könntet ihr denn den Schlüssel auf die einzelnen Blöcke anwenden? — Wenn ihr dann einen Chiffretext habt, wie würdet ihr ihn nun wieder entschlüsseln?

Je nach Lerngruppe und zeitlichen Möglichkeiten kann dieses Beispiel vertieft werden, so dass die Kinder vertrauter werden im Umgang mit Bitfolgen und der XOR-Verknüpfung, also der Bit-weisen Addition in $\mathbb{Z}/2\mathbb{Z}$, indem die Kodierung des regulären Alphabets durch 5 Bits beginnend bei A gleich 00000, B gleich 00001, bis hin zu Z gleich 11001 eingeführt wird und so zugleich ein Beispiel für binäres Zählen, also der Idee des Übertragens in die nächste Stelle: $00, 01, 10...$, kennengelernt wird. Obiger Klartext ergibt so in dekodierter Form das Wort „BITS“. Eine Dekodierung der verschlüsselten Form ist übrigens nicht vollständig möglich, da die letzten beiden Fünfergruppen 11100 und 11101 keine Entsprechung im Alphabet haben. Dies zu diskutieren mag Ansatzmöglichkeiten zum vertieften Verständnis bieten.

In jedem Fall erscheint es sinnvoll, Blockchiffren (oder exakter polyalphabetische Substitutionschiffren) ebenfalls unmittelbar auf dem regulären Alphabet zu betrachten, um das Konzept an bekanntere Verfahren zu knüpfen. Zudem kann so der nächste Teil eingeleitet werden, in dem die Kinder die kryptoanalytische Methode der Häufigkeitsanalyse kennenlernen:

Durch die Erinnerung an die ersten, naiven Versuche des „Knackens“ von Chiffren in den ersten Einheiten können nun Begriff und Anliegen der Kryptoanalyse dezidiert eingeführt und diskutiert werden. Dabei lohnt es sich die Frage nach der moralischen Legitimität, als auch der Sinnhaftigkeit in Bezug auf das ureigene Geheimhaltungsanliegen der Kryptographie zu stellen.

Ist es in Ordnung, Chiffren zu „knacken“, oder sollte Kryptoanalyse sogar gesetzlich verboten werden? — Wozu ist Kryptoanalyse – außer für Angreifer – überhaupt nützlich, wenn sie doch nur Chiffren unbrauchbar macht, indem sie Schwachstellen aufdeckt?

Gründe für die Daseinsberechtigung und Legitimität der Kryptoanalyse liegen etwa in dem Ansinnen der Kryptographie als Wissenschaft, die eigenen Verfahren auf ihre Möglichkeiten und Beschränkungen hin testen zu wollen. Darüber hinaus sollte das Argument, dass immer nach Schwachstellen gesucht werden wird und deshalb die Vogel-Strauß-Taktik nicht genügt, ausreichend wiegen, um guten Gewissens in ein statistische Kryptoanalyse einzusteigen.

Die naivste kryptoanalytische Methode kennen die Kinder vermutlich selbst und haben sie zumindest implizit bereits angewendet. Zu diesem Zeitpunkt sollte sie expliziert und benannt werden, wenn dies sich nicht schon vorher im Unterrichtsgeschehen ergeben hat, etwa im Zusammenhang mit Überlegungen zur Menge der Schlüssel eines Verfahrens. Der Begriff „Brute-Force“ zu deutsch rohe oder brachiale Gewalt beschreibt sehr gut diese naive kryptoanalytische Methode. Sie nutzt nicht ausgefeilte Techniken, sondern eben rohe Rechengewalt. Ihre Erfolgsaussichten werden verringert durch die Menge der Schlüssel eines Kryptosystems.

Vor dem Hintergrund dieser Methode kann dann kontrastierend die Methode der statistischen Häufigkeitsanalyse in den Blick genommen werden. Deren grundlegende Idee ist vermutlich nur sehr geführt zu entdecken. Folgende, simplifizierte Frage-Antwort-Skizze mag als Erläuterung, sowie als Anregung für den Unterricht genügen:

> *Wenn ihr einen Chiffretext von eurem Banknachbarn abfangt, was könnt ihr **vor** jeder Kryptoanalyse bereits wissen? — Ihr wisst, wer den Text verschlüsselt hat und dass derjenige wahrscheinlich deutsch schreibt.*
>
> *Wenn es ein deutscher Text ist, kennen wir das Alphabet, also alle Zeichen, die vorkommen. Was wisst ihr über die einzelnen Buchstaben? Welche Buchstaben kennt ihr selbst sehr gut und welche eher nicht? Und warum?*
>
> *X oder Y schreibt man also sehr selten, welche Buchstaben dafür sehr oft?*
>
> *Wir haben im Unterricht schon **Häufigkeiten** kennengelernt. Wie steht es mit den relativen Häufigkeiten der einzelnen Buchstaben in deutschen*

Texten?

Es bietet sich eine Gruppenarbeit an, für die das Alphabet wie schon gewohnt auf die 26 Standard-Buchstaben beschränkt wird. Für Umlaute und Ähnliches sind entsprechend Substitutionsmöglichkeiten zu erörtern. Die einzelnen Gruppen wählen sich aus ihren Schulbüchern und Unterrichtsmaterialien frei einen deutschen Text aus. Die Länge ist den Umständen entsprechend anzupassen, sollte aber eine handgeschriebene Seite nicht unterschreiten, um statistisch brauchbare Ergebnisse erzielen zu können. Die Aufgabe ist, die relativen Häufigkeiten aller 26 Buchstaben im Text zu bestimmen. Die Gruppengröße ist mit zwei Kindern ideal, so kann eines den Text durchgehen und das andere die Häufigkeiten notieren.

Im Anschluss können die Ergebnisse verglichen, und lerngruppenübergreifende Häufigkeitswerte bestimmt werden. Gegebenenfalls ist die Gültigkeit unterschiedlicher Ergebnisse zu thematisieren, je nachdem, wie weit das Konzept der Wahrscheinlichkeit im regulären Unterricht behandelt wurde. Der Abgleich mit Werten aus größer angelegten Messungen ist zwar verlockend, das Vertrauen in die Werte der Kinder und die damit einhergehende Anerkennung ihrer Arbeit sind aber höher zu gewichten. Bei einer durchschnittlichen, schulischen Lerngruppe und der angegebenen Textgröße, ist eine ausreichende Stichprobe anzunehmen.

Mit diesen Ergebnissen ist einem spielerischen Wettkampf zwischen einzelnen Gruppen der Boden bereitet. Die Kinder können mit den besprochenen Chiffren und beliebigen anderen monoalphabetischen Verfahren Chiffretexte erzeugen und diese dann gegenseitig per statistischer Analyse versuchen zu brechen. Vorerst sollten polyalphabetische Chiffren ausgeklammert werden mit dem Hinweis, dass hier die Lage etwas schwieriger ist. Möglicherweise entwickeln besonders leistungsstarke Kinder unter Festlegung der Blocklänge den nun folgenden Punkt aber auch von allein.

Denn natürlich stellt sich die Frage, ob das vorher kennengelernte Konzept der Blockchiffren statistische Analysen verhindert. Dazu kann etwa folgende Aufgabe bearbeitet werden:

Ihr habt ein einen Chiffretext vorliegen, von dem ihr wisst, dass er durch eine Blockchiffre mit Blocklänge gleich 2 verschlüsselt wurde. Wie könnt ihr hier eine statistische Häufigkeitsanalyse so ansetzen, dass ihr den Klartext herausfinden könnt?

Die Antwort ist natürlich, den Text in zwei Teile zu zerlegen – in diesem Fall in einen Teil bestehend aus allen Buchstaben mit ungerader beziehungsweise gerader Positionsnummer – und diese separat einer Häufigkeitsanalyse zu unterziehen. Geeignete Schlüsselkandidaten oder auch nur geeignete Buchstabenkandidaten müssen dann verständlicherweise am Gesamttext getestet werden. Dieses Verfahren ist prinzipiell für jede beliebige Blocklänge anwendbar. Für jede beliebige Blocklänge n wird die Nachricht entsprechend in n kleinere Teile zerlegt. Trotzdem erhöht sich mit steigender Blocklänge die Sicherheit bis hin zur absoluten Sicherheit des One-Time-Pads, einerseits aus stochastischer Sicht – die verwertbare Stichprobe hinsichtlich eines Schlüsselanteils wird verkleinert – und andererseits mit Blick auf die Schlüsselanzahl – je größer die Blöcke, desto länger der Schlüssel und desto mehr verschiedene Schlüssel gibt es.

Im Unterricht ist zunächst der Umstand zu diskutieren, dass statistische Angriffe nur gegen hinreichend lange Nachrichten möglich sind, deren Buchstabenhäufigkeiten also gegen erwartbare Werte gehen. Als Gegenbeispiel können ganz konkret kurze Sätze auf ihre Buchstabenhäufigkeiten hin betrachtet werden. Ist das Verfahren bei Blockchiffren nachvollzogen, ergibt sich unmittelbar der Nutzen großer Blöcke hinsichtlich der Sicherheit gegenüber statistischer Methoden. Im Hinblick auf die bereits mehrfach diskutierte Schlüsselanzahl ist auch der Einfluss des längeren Schlüssels auf die Sicherheit leicht herauszuarbeiten. Ein letzter wichtiger Punkt ist der Umstand, dass auch mehrmalige Verwendung gleicher Schlüssel denselben Effekt hat, wie die Verlängerung einer einzigen Nachricht. Es steht mehr Material zur Verfügung, das statistisch ausgewertet werden kann.

Aus diesen Überlegungen heraus kann ganz ohne mathematischen Formalismus die

Idee des One-Time-Pads und der mathematisch perfekten Sicherheit nachvollzogen werden: Sie ergibt sich im Grunde von allein, denn im Wesentlichen ist nur gefordert, dass die Blocklänge die Länge der Nachricht übersteigt und so jedes Zeichen separat, das heißt stochastisch unabhängig, verschlüsselt wird. Einzig das Erfordernis der gleichverteilten Wahl des Schlüssels bleibt so offen. Es muss im Einzelfall abgewägt werden, ob und in wie weit diese Thematik für und im Unterrichtskontext nötig und möglich ist.

4.5 Jahrgangsstufe 9 – Moderne Kryptographie

4.5.1 Lernziele und Vernetzung

In der Unterrichtseinheit zum Ende der 9. Jahrgangsstufe sollen die Jugendlichen die Betriebsmodi ECB und CBC, als Lösung des Problems statistischer Methoden kennenlernen und diskutieren. Ferner soll das kryptoanalytische Szenario von Known-, beziehungsweise Chosen-Plaintext-Angriffen eingeführt werden, vor dessen Hintergrund die bekannten, affinen Chiffren, aufgrund der Eigenschaften linearer Gleichungssysteme, als grundsätzlich unsicher erscheinen (Chosen-Plaintext), beziehungsweise unter bestimmten Voraussetzungen unsicher sind (Known-Plaintext). Darüber hinaus soll die Unterscheidung von symmetrischer und asymmetrischer Verschlüsselung bereits begrifflich eingeführt werden.

Damit geht einher, dass statistische Häufigkeitsanalysen und insbesondere die verschiedenen Formen affiner Chiffren wiederholt werden. Auch der Umgang mit Bit-Tupeln ist erneut gefragt. Dadurch bietet sich die Gelegenheit, die Ergebnisse der letzten vier Einheiten zu rekapitulieren und zu bündeln. Gerade die Kryptoanalyse affiner Chiffren verankert die Einheit im regulären Mathematikunterricht, der in der 9. Jahrgangsstufe lineare Gleichungssysteme in herausragender Stellung behandelt.[47] Ferner wird, mit Blick auf die Wiederholung der Häufigkeitsanalysen, an die umfangreicheren Inhalte der Stochastik in der 9. Jahrgangsstufe angeknüpft werden können.[48]

[47] Vgl. Lehrplan Mathematik (Sek I), S. 28f.
[48] Vgl. Lehrplan Mathematik (Sek I), S. 35.

4.5.2 Kurzer Unterrichtsverlauf

In den vorigen beiden Unterrichtseinheiten haben Überlegungen zur Sicherheit einerseits, und der Umgang mit Bit-Tupeln, beziehungsweise das Rechnen in $\mathbb{Z}/2\mathbb{Z}$, andererseits, eine zentrale Rolle eingenommen. Insbesondere statistische Angriffe haben sich als problematisch herausgestellt, auch im Hinblick auf Blockchiffren. Das One-Time-Pad ist nur in besonderen Fällen eine Alternative, gerade für globale Netzwerke sind andere Lösungen notwendig. Ein solcher Lösungsansatz ist der CBC-Betriebsmodus für Blockchiffren. Die Explikation des, vermutlich zuvor implizit angewendeten ECB-Modus und die (erneute) Vergegenwärtigung der einhergehenden Probleme, sind der Ausgangspunkt, die beiden Betriebsmodi zu formulieren, zu vergleichen und die Vor- und Nachteile zu diskutieren.

Eine Möglichkeit den CBC-Modus anzuwenden, liefert die Aufgabe zu Blockchiffren aus Jahrgangsstufe 8. Wählt man als Initialvektor $i = (10101)_2$, dann ergibt sich für die Chiffretextblöcke $(c_0.c_1.c_2.c_3)_2$, wenn der Klartext die Form $(p_0.p_1.p_2.p_3)_2 = (00001.01000.10011.10010)_2$ hat und der Schlüssel gegeben ist durch $k = (01111)_2$, zum Beispiel:

$$c_0 = p_0 + i + k = (00001)_2 + (10101)_2 + (01111)_2 = (01011)_2$$

$$c_1 = p_1 + c_0 + k = (01000)_2 + (01011)_2 + (01111)_2 = (01100)_2$$

$$c_2 = p_2 + c_1 + k = (10011)_2 + (01100)_2 + (01111)_2 = (10000)_2$$

$$c_3 = p_3 + c_2 + k = (10010)_2 + (10000)_2 + (01111)_2 = (01101)_2$$

Doch auch dieses Verfahren hilft nicht weiter, unter der Voraussetzung von Chosen-Plaintext-Angriffen. Diese kryptoanalytischen Szenarien sind, mit Blick auf moderne Anforderungen an kryptographische Systeme, die etwa im Internet eingesetzt werden sollen, leicht zu motivieren. Mit Hilfe, in der 9. Jahrgangsstufe erlernter, algebraischer Methoden zur Lösung linearer Gleichungssysteme lässt sich nun ganz abstrakt, ohne notwendige Rechnungen zeigen, das alle kennengelernten affinen Chiffren und Blockchiffren diesem Szenario nicht standhalten können, denn es lassen sich durch die frei

wählbaren Klartext-Chiffretext-Paare beliebig viele Gleichungen erzeugen, so dass jede Unbekannte bestimmt werden kann. Beim One-Time-Pad greift diese Argumentation übrigens nicht, da hier jeder Schlüssel nur einmal verwendet wird und demnach, nach jedem erzeugten Klartext-Chiffretext-Paar, vernichtet wird. Das Known-Plaintext-Szenario nimmt eine hybride Stellung ein. Es greift unter günstigen Bedingungen, wenn die bekannten Paare gerade hinreichend für oben genanntes Vorgehen sind. Als Lösung dieses Problems kann bereits der DES angeführt werden, um so bereits vernetzend in die folgende Einheit zu verweisen.

Die genannten, kryptoanalytischen Szenarien können ein Ausgangspunkt sein, den Begriff der asymmetrischen Kryptographie zu motivieren. Eine weitere Möglichkeit ist das in Abschnitt 3.2 dargelegte Problem der Schlüsselanzahl für n Teilnehmer eines Netzwerkes, die insgesamt $\frac{n(n-1)}{2}$ Schlüssel benötigen, oder auch das Problem der geheimen Schlüsselübertragung. In jedem Fall sollten in dieser Einheit das Begriffspaar *symmetrisch* – in exemplarischer Anbindung an die bekannten Verfahren – und *asymmetrisch* behandelt werden. Zur Konkretisierung der Vorstellung können symmetrische Verfahren etwa bildlich dargestellt werden durch eine Schatzkiste. Wer den Schlüssel zum Einschließen des Geheimnisses besitzt, ist auch in der Lage, die Kiste wieder zu öffnen und an das Geheimnis zu gelangen. Im Kontrast zur Schatzkiste kann das Bild des Briefkastens hinsichtlich asymmetrischer Verschlüsselung in Anschlag gebracht werden, in den jeder Post einwerfen kann, den aber nur derjenige mit dem (Entschlüsselungs-) Schlüssel leeren kann.[49] Ein anderes eingängiges Bild ist das Prinzip des Telefonbuchs, in dem zwar nach Namen gesucht werden kann, und so die zugehörige Telefonnummer ‚entschlüsselt' werden kann, nicht aber umgekehrt.

[49] Vgl. Stohr 2007, S. 103.

4.6 Jahrgangsstufe 10 – DES und RSA-Grundlagen

4.6.1 Lernziele und Vernetzung

Die Einheit zum Ende der 10. Jahrgangsstufe hat zum Ziel einerseits, den Data Encryption Standard als modernen Algorithmus zu thematisieren, der die behandelten Probleme der Häufigkeitsanalyse und der Lösbarkeit auf Basis bekannter Klartext-Chiffretext-Paaren vermeidet, und andererseits die Grundlagen zu legen, um in der verbleibenden Einheit das RSA-Verfahren behandeln zu können. Dazu gehören die Idee der Einwegfunktionen und der algorithmische Sicherheitsbegriff, sowie – als mathematisches Handwerkzeug – die Methode des schnellen Potenzierens modulo n.

Die Inhalte der Einheit fokussieren sich somit vollständig auf die moderne Kryptographie und verweisen die Chiffrierverfahren der vorigen Einheiten auf ihren historischen Platz. Dennoch sind einerseits alle erlernten Begriffe und Konzepte, als andererseits auch die mathematischen Methoden (Restklassen, Bit-Manipulationen) weiterhin relevant. Im Mathematikunterricht der 10. Jahrgangsstufe sind Potenz- und Wurzelfunktionen zentral,[50] Kenntnisse, die in dieser Unterrichtseinheit gewinnbringend angewendet werden können. Ferner wird der Einsatz „elektronischer Werkzeuge“[51] im Lehrplan vorgeschlagen, ein Umstand, dem in der Auseinandersetzung mit dem (S)DES hervorragend Rechnung getragen werden kann. Bemerkenswert ist auch die lehrplanmäßige Thematisierung von Umkehrfunktionen,[52] die ja im Kontext der Entschlüsselung von affinen Chiffren bereits kennengelernt wurden. Hier bietet sich also eine Vernetzung in umgekehrter Richtung an. Zugleich ist der Begriff der Umkehrfunktion Voraussetzung, um die Idee der Einwegfunktion nachvollziehen zu können.

[50] Vgl. Lehrplan Mathematik (Sek I), S. 36f.
[51] Vgl. Lehrplan Mathematik (Sek I), S. 36.
[52] Vgl. Lehrplan Mathematik (Sek I), S. 36f.

4.6.2 Kurzer Unterrichtsverlauf

In der letzten Einheit war die klassische Kryptographie gewissermaßen abgeschlossen und die moderne Kryptographie zumindest begrifflich eröffnet worden. In dieser Einheit soll mit der Erprobung des SDES der Bereich der symmetrischen Kryptographie zu seinem krönenden Abschluss kommen. Die in den Abschnitten 3.2, 3.3 und 3.4 dargelegten Eigenschaften des DES können besprochen werden. Ausführlichere kryptoanalytische Untersuchungen sind – wie gesagt – nicht vorgesehen, da hier die schulischen Möglichkeiten, angesichts des gesetzten Zeitrahmens, bereits ausgereizt sind. Aber eine Auseinandersetzung mit der Funktionsweise anhand des SDES ist durchaus möglich. Es kann etwa das in Abschnitt 3.4 angeführte Beispiel durchgerechnet werden, um eine Ahnung des rechnerischen Aufwandes moderner, kryptographischer Verfahren zu vermitteln. Wie bereits in den Ausführungen zur Vernetzung angedeutet, gibt es hier vielfältige Möglichkeiten computergestützt zu arbeiten.

Mit diesem Abschluss der symmetrischen Kryptographie kann nun die volle Aufmerksamkeit ihrem asymmetrischen Gegenpart gewidmet werden. Dazu bietet es sich an, vom algorithmischen Sicherheitsbegriff auszugehen. Dieser findet sich ja bereits in der Idee, Schlüsselräume ausreichend groß zu gestalten, dass Brute-Force-Angriffe algorithmisch aussichtslos sind. Aus diesen Überlegungen heraus, kann der Begriff der Einwegfunktion, in Anbindung an die Inhalte des regulären Unterrichts, aber insbesondere auch in Erinnerung an die prinzipielle Notwendigkeit der Umkehrung symmetrischer Verfahren, motiviert und vernetzt werden. Als Einstiegsbeispiel eignet sich in ausgezeichneter Weise sicherlich das Faktorisierungsproblem und zwar aus mehreren Gründen: Erstens ist es ein klassisches und insbesondere jedem Schulkind bekanntes Problem der Mathematik. Zweitens ist es ja äquivalent zum RSA-Problem und bietet so zukünftige Anschlussmöglichkeiten. Und drittens kann es sehr leicht auch auf jedweder Form von Computer nachvollzogen werden, etwa auf graphischen Taschenrechnern. Es sei hier auf die Testmultiplikation der Faktoren der 768 Bit langen Zahl in Abschnitt 3.2 verwiesen, deren Faktorisierung als aktueller Weltrekord gilt.

Das RSA-Verfahren basiert – zumindest unmittelbar – dagegen auf der Potenzierung modulo n. Die Hinzunahme der Multiplikation zur Addition im Verlauf der Unterrichtsreihe kann als Vorbild dienen, es nun mit Potenzen zu versuchen, zumal sie aus dem regulären Unterricht gegenwärtig sein sollten. Mit kleinen Zahlen kann erprobt werden, dass Wurzelziehen modulo n, problematisch ist, etwa mit der Aufgabe

> *Welche Zahl ist* $a^5 \equiv 5$ *mod* 7*?*
> *—Lösung* $a = 3$*, denn* $3^5 \equiv 9 \cdot 9 \cdot 3 \equiv 243 \equiv 5$ *mod* 7

Diese Aufgabe ist per Hand noch recht einfach durch systematisches Probieren zu lösen, bei etwas größeren Zahlen wird es sehr schnell sehr aufwendig. Das Beispiel zum RSA-Verfahren in Abschnitt 3.4 liefert hier eine Potenzgleichung, deren Lösung von Hand die meisten abschrecken wird. Und anders als beim Problem der multiplikativen Inversen, gibt es hier keinen bequemen Algorithmus, was ja gerade Grundlage der Sicherheit von RSA ist. Diese Offenbarung ist nicht nur für die spätere Auseinandersetzung mit dem RSA-Verfahren relevant, sondern für sich auch eine wertvolle Erkenntnis. Häufig erfahren Jugendliche im Mathematikunterricht ihre eigene Unwissenheit. Hier aber, wie auch beim Faktorisierungsproblem, haben sie Gelegenheit einen Ansporn durch ein ungelöstes, aber verständliches Problem zu erhalten.

Selbst Computer kommen hier – wie auch bei der Faktorisierung – an die Grenzen ihrer Möglichkeiten, wenn die Zahlen ausreichend groß sind. Soll dieser Umstand für asymmetrische Verschlüsselung ausgenutzt werden, so bedarf es der Potenzierung großer Zahlen. Und dies in angemessen kurzer Laufzeit, sonst ist nichts gewonnen. Derart ist die Methode der schnellen Potenzierung motiviert, die sich die Jugendlichen zum Abschluss der Einheit aneignen sollen. Damit sind alle Grundlagen für die abschließende Unterrichtseinheit gelegt.

4.7 Jahrgangsstufe 11 – Das RSA-Verfahren

4.7.1 Lernziele und Vernetzung

Die folgende und letzte Einheit Ende der 11. Jahrgangsstufe fokussiert sich vollständig auf das RSA-Verfahren mit Schlüsselgenerierung und Verschlüsselungsverfahren mittels schnellem Potenzieren, als auch auf den Nachweis der Gültigkeit von Schlüsselgenerierung und Verschlüsselungsverfahren (Satz 17). Darüber hinaus bietet sich an, zum Abschluss der Unterrichtsreihe verschiedenste Aspekte moderner Kryptographie zu diskutieren (der theoretische Teil dieser Arbeit liefert in dieser Hinsicht sicherlich einige Anregungen).

Im Kontext der Unterrichtsreihe muss sich diese Einheit besonders auf die Vorarbeiten der vorigen Einheit stützen. Aber wie auch schon zuvor, kommen die über die Jahre erlernten und verfeinerten Methoden der Restklassenarithmetik anhand einer faszinierenden Idee zu einer sinnvollen Anwendung. Bezüglich der Inhalte des regulären Mathematikunterrichts in der 11. Jahrgangsstufe, welche sich ausschließlich mit der Analysis befassen,[53] sind hier keine unmittelbaren Vernetzungsmöglichkeiten gegeben. Mit Blick auf den Anspruch der „wissenschaftspropädeutische[n] Orientierung“[54] kann diese Einheit mit dem Nachweis der Gültigkeit des RSA-Verfahrens gewiss methodische Relevanz beanspruchen.

Sicherlich kann diese Einheit auch auf zwei Jahrgangsstufen aufgeteilt werden, insbesondere, wenn noch tiefer in Themen der modernen Kryptographie eingestiegen wird. Wie gesagt ist die vorliegende Konzeption größtenteils auf die Sekundarstufe eingeschränkt, um der Stofffülle der Oberstufe gerecht zu werden. Einige Anschluss- beziehungsweise Erweiterungsmöglichkeiten werden in Abschnitt 5 diskutiert.

[53] Vgl. Lehrplan Mathematik (Sek II), S. 43f.
[54] Lehrplan Mathematik (Sek II), S. 3.

4.7.2 Kurzer Unterrichtsverlauf

In dieser letzten Unterrichtseinheit lernen die Jugendlichen das RSA-Verfahren gemäß Definition und Beispiel in Abschnitt 3.4 kennen und erarbeiten sich darüber hinaus die Nachweise, dass Schlüsselgenerierung und Entschlüsselung, wie angegeben funktionieren. Hier sind die Anforderungen in formalistischer Hinsicht und mit Blick auf die Abstraktionsfähigkeit der Jugendlichen sicherlich am höchsten gesteckt.

Im Sinne der wissenschaftspropädeutischen Zielsetzung wird hier vorgeschlagen, gerade den Beweis in einer Form vorzustellen, der an den Vorlesungscharakter an Universitäten angelehnt ist. Im Anschluss wird dann mit tatkräftiger Unterstützung der Lehrperson die „Vorlesung“ nachbereitet. Derart haben die Jugendlichen Gelegenheit, einen ersten Eindruck von der universitären Lehrmethodik zu erhalten. Wichtig ist hier, sie dennoch nicht allein zu lassen, sondern im Nachgang genügend Hilfsangebote und Anleitung zum gemeinsamen Nachbereiten in Kleingruppen zu geben. Darüber hinaus können verschiedenste Zusatzinformationen zum RSA-Verfahren diskutiert und auch getestet werden, wie etwa die Empfehlung, die Primzahlen p und q etwa gleichgroß zu wählen.

5. Kritische Reflexion der Zielsetzungen und Ausblick

In Abschnitt 2 die Leitlinien und die Methodik dieser Arbeit betreffend, hatten sich aus dem generellen Anliegen die Kryptographie als Teil des Mathematikunterrichts des Gymnasium zu erproben – um sie einerseits in der Sache als Beitrag zur schulischen Allgemeinbildung der sogenannten Informationsgesellschaft hervorzuheben und andererseits ihre Chancen auf Bereicherung des kanonischen Stoffs im Mathematikunterricht auszuloten – verschiedene, teils abgeleitete Intentionen ergeben. Diese sollen nun kritisch hinterfragt werden, um dann, daran anknüpfend, Ausblicke in zweierlei Hinsicht zu unternehmen, erstens bezogen auf die Inhalte der Unterrichtsreihe und ihre Erweiterungs- und Anknüpfungspunkte und zweitens, weitere didaktische (Anschluss-) Forschung betreffend.

Insgesamt ist sicher ein mehr als ausreichender Einblick in die Kryptographie gelungen – wenn überhaupt hat sich der Einblick als zu umfangreich gestaltet. Auch die damit verbundene Zielsetzung der Verflechtung des Themengebiets der Kryptographie durch sinnhafte, interne Bezüge konnte umgesetzt werden. Obwohl die anfänglichen, klassischen Chiffren durch kryptoanalytische Methoden als unbrauchbar deklassiert wurden, konnten die erlernten, mathematischen Werkzeuge gewinnbringend weiter verwendet werden, und so schließlich in den Bereich moderner Kryptographie vorgedrungen werden. Auch die konkreten inhaltlichen Zielsetzungen sind umgesetzt worden, nämlich der Einblick in die moderne Kryptographie mit der Unterscheidung in symmetrische und asymmetrische Verschlüsselungsverfahren, beispielhaft durch SDES und RSA in der Anwendung erfahrbar gemacht, sowie das Wechselspiel von kryptographischen Verfahren und deren Erprobung durch kryptoanalytische Methoden. Insofern wurde eines der zentralen Anliegen verwirklicht.

Dagegen hat die Vernetzung mit dem kanonischen Stoff an zwei Stellen Probleme bereitet, wenn sie auch sonst sehr gut gelungen ist. Die Auseinandersetzung mit den recht abstrakten Restklassen und ihrer Arithmetik bereits in der 6. Jahrgangsstufe und die daran anschließende Behandlung multiplikativer Inverser in $\mathbb{Z}/n\mathbb{Z}$ in der 7. Jahrgangsstufe ist für Lerngruppen durchschnittlichen Leistungsniveaus vermutlich nur schwer realisierbar. Der gewählte Weg ergab sich aus dem Umstand, dass die statistische Häufigkeitsanalyse als Argument für moderne, symmetrische Verfahren nachfolgen musste, gleichzeitig aber die mathematische Theorie der Restklassenarithmetik sich als Voraussetzung für alle anderen anschließenden Betrachtungen dargestellt hat.

Eine alternative Verschiebung in höhere Jahrgangsstufen hätte hier mehr Möglichkeiten bei der abstrakten Betrachtung der Restklassen gebracht und gegebenenfalls sogar die Option, die generelle Klasse affin linearer Chiffren (Multiplikation mit Vektoren) mit Methoden der linearen Algebra in der Oberstufe zu behandeln, um so auch ihre generelle Angreifbarkeit mit Known-Plaintext-Attacken zu beweisen. Dies hätte jedoch den Anspruch der Ausrichtung auf die moderne Kryptographie konterkariert, denn in den unteren Jahrgangsstufen hätte so vermehrt auf veraltete Chiffrierverfahren gesetzt werden müssen. Ein solches Vorgehen kann durchaus gewinnbringend sein – weiter unten werden diesbezüglich noch Vorschläge erörtert –, mit Blick auf die Zielsetzungen dieser Arbeit war aber der gegebene Weg einzuschlagen.

Zwei weitere, eng mit der obigen zusammenhängende Zielsetzungen waren der Anspruch, die Zahlentheorie beziehungsweise die Algebra im Mathematikunterricht stärker zu verankern und der Anspruch, einen wissenschaftspropädeutischen Beitrag zu leisten. Die erste Zielsetzung ist, abzüglich oben genannter Schwierigkeiten, gelungen. Sieht man von den Problemen ab, so haben die Jugendlichen am Ende der Unterrichtseinheit einen bedeutenden Einblick in die genannten zwei mathematischen Teilgebiete erlangt, insbesondere in Relation zu den regulär vorgesehenen, kanonischen Inhalten. Hinsichtlich der Wissenschaftspropädeutik ist eine stärkere Einübung von Beweismethoden und deduktiver Denk- und Argumentationsweise wünschenswert. Nicht zuletzt im Bereich der Vertreterunabhängigkeit und der Invertierung mittels des EEA ist ur-

sprünglich ein stärkerer, diesbezüglicher Fokus geplant gewesen, von dem aber, aus den angeführten Gründen, abgesehen wurde.

Damit ist auch erörtert, inwiefern zwei der drei Grundaspekte des Mathematikunterrichts aus den Lehrplänen verwirklicht werden konnten. Der Anwendungsaspekt ist uneingeschränkt zur Geltung gekommen, die Geistesschulung dagegen, die ja insbesondere durch die abstrakten Restklassen gefördert werden sollte, muss mit einem Fragezeichen versehen werden. Unter der Voraussetzung, dass die problematischen Stellen der Unterrichtsreihe in der 6. und 7. Jahrgangsstufe erfolgreich durchführbar sind, ist ein enormer Beitrag getan.

Der dritte Aspekt der Vermittlung der deduktiven Struktur der Mathematik hat in der Unterrichtsreihe keinen ausreichenden Raum gefunden. Zwar ist im theoretischen Teil die geplante, ambivalente Linie gefahren worden und in gewissem Maße dem deduktiven Aufbau gerecht geworden, doch konnte dies aufgrund des Projektumfangs in den Unterrichtselementen nicht eingebracht werden.

Die strukturellen Zielsetzungen der Unterrichtsreihe wurden im Wesentlichen umgesetzt. Es hat sich jedoch im Verlauf der Ausarbeitungen das Ausmaß des geplanten Unterfangens gelegentlich auf die Details ausgewirkt. Sicherlich wäre eine Beschränkung auf ein weniger umfassendes Projekt – etwa eine Unterrichtsreihe allein zum RSA-Verfahren – der detaillierten Ausarbeitung einzelner Unterrichtselemente, als auch der Genauigkeit der Ausführungen entgegen gekommen. Derart wäre jedoch die Gesamtkonzeption, insbesondere hinsichtlich des angestrebten, thematischen Gesamtzusammenhanges, verloren gegangen.

Eine weiterer, zu hinterfragender Punkt ist die Sinnhaftigkeit der Aufteilung der Unterrichtsreihe auf sieben Klassenstufen. Die hier dargestellte Strukturierung der Kryptographie kann gewiss in anderer Form in den Unterricht eingebracht werden, solange die einzelnen Themen nicht in noch frühere Jahrgangsstufen verortet werden. In dieser Arbeit ist vermutlich die untere Altersgrenze ausgelotet, und insgesamt ist ein sehr hohes Leistungsniveau angesprochen worden. Mit Blick auf etwaige Integration der Kryptographie in der hier angestrebten Form in den Lehrplan muss deshalb festge-

halten werden, dass sich dies wohl nur mit einem erheblich umfangreicheren und vor allem kleinschrittigeren Unterrichtspensum verwirklichen ließe. Inwiefern dies machbar, und in Relation zu anderen wichtigen Themen der Allgemeinbildung gerechtfertigt ist, muss hier offen bleiben. Gleichzeitig verweist die Frage auf mögliche, allgemein didaktische Anschlussforschungen.

Zunächst sollen aber konkretere, stoffdidaktische Erweiterungspotentiale angesprochen werden. Die Optionen sind zahlreich, besonders im fächerübergreifenden Bereich zwischen Mathematik und Informatik, jeder Versuch einer Aufzählung somit sicherlich unvollständig. Es ergeben sich aber aus Sicht des Autors drei Bereiche. Wie bereits erwähnt, können in den unteren Jahrgangsstufen verschiedenste, historische Verschlüsselungsverfahren in ausführlicher Weise untersucht werden. Hier sei die Onlineplattform *Cryptool Portal* empfohlen, die verschiedenste Lehrmaterialien und Lehralgorithmen zur Verfügung stellt. Der Link findet sich im Literaturverzeichnis unter den Empfehlungen.

Der zweite Bereich umfasst Anschlüsse an die gegebene Unterrichtsreihe. Hier können, wie schon gesagt, affin lineare Chiffren durch Methoden der linearen Algebra umfassender und allgemeiner analysiert werden. Daran anschließend stellt sich die Frage, warum der (S)DES nicht affin linear ist. Darüber hinaus kann dieser auch hinsichtlich seiner, statistische Angriffe verhindernden, Mechanismen untersucht werden. Analog kann die RSA-Thematik, in Bezug auf empfohlene Randbedingungen und Sicherheit, beliebig vertieft werden. Ein letztes Beispiel sind die Möglichkeiten statistischer Methoden. Sie werden zwar nach aktuellem Stand durch moderne Verfahren verhindert, doch kann dies durchaus problematisiert werden, zudem eröffnet sich hier ein Übergang zu den Bereichen *Big Data* und *Machine Learning*, die beide wohl eine ähnliche Relevanz für die digitale Bildung inne haben, wie die Kryptographie.

Es wurde bereits auf Möglichkeiten des fächerübergreifenden Unterrichts hingewiesen. Angesichts des informationstechnologischen Charakters der Kryptographie, rückt hier wenig überraschend der Informatikunterricht in den Fokus. Grundsätzlich alle besprochenen Algorithmen und Verschlüsselungsverfahren können, unter förderlichen Rah-

menbedingungen, in der Schule implementiert werden. Aber auch binäre Zahldarstellungen bieten sich an, um ein Gebiet aus der theoretischen Informatik aufzuführen.

In allgemein didaktischer Hinsicht, war bereits die Frage der Abwägung der Notwendigkeit der Kryptographie gegenüber anderen (mathematischen Themen) angesprochen worden. Die in dieser Arbeit zu Beginn angeführten Argumente für kryptographische Inhalte sind sicher einleuchtend, eine differenziertere Abwägung ist in der Debatte aber durchaus wünschenswert. Darüber hinaus ist wohl deutlich geworden, dass diese Arbeit nur eine Grundlegung hinsichtlich der Etablierung kryptographischer Themen im Mathematikunterricht leistet und leisten konnte. Insofern gibt es mannigfaltigen Forschungsbedarf hinsichtlich den Fragen ob, warum und wie Kryptographie im Mathematikunterricht verankert werden soll.

Dazu wäre es zu begrüßen, auch empirische Untersuchungen anzustellen. Monika Stohr hat in ihrer Dissertation einige Praxiserfahrungen ausgewertet. Nach ihren Befragungen, bezogen auf ihre Unterrichtskonzeption, scheint das Thema Kryptographie durchaus das Interesse der Jugendlichen geweckt zu haben.[55] Zuletzt sind auch ergänzende, kompetenztheoretische Forschungen wünschenswert, denn Mathematik und Mathematikunterricht leben durch die Verflechtung von Inhalten und Kompetenzen.

Damit können dieser Ausblick und zugleich diese Arbeit abgeschlossen werden. Es bleibt, zu hoffen, dass die faszinierende Thematik der Kryptographie in der Mathematikdidaktik und im Mathematikunterricht in Zukunft vermehrt Beachtung erfährt.

[55] Vgl. Stohr 2007, S. 144 – 148.

6. Literaturverzeichnis

Quellenangaben:

Beutelspacher, Albrecht: *Kryptologie. Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen*, 6. Aufl., Braunschweig/Wiesbaden: Vieweg 1987/2002.

Buchmann, Johannes: *Einführung in die Kryptographie*, 2. Aufl., Berlin/Heidelberg: Springer 1999/2001.

Küster, Ralf & Wilke, Thomas: *Moderne Kryptographie. Eine Einführung*, Wiesbaden: Vieweg+Teubner 2011.

Swoboda, Joachim; Spitz, Stephan; Pramateftakis, Michael: *Kryptographie und IT-Sicherheit. Grundlagen und Anwendungen*, Wiesbaden: Vieweg+Teubner 2008.

Trappe, Wade; Washington, Lawrence C.: *Introduction to Cryptography with Coding Theory*, (o.O.): Prentice Hall 2002.

Willems, Wolfgang: *Codierungstheorie und Kryptographie*, Basel: Birkhäuser 2008.

Online-Quellen:

Computer Science at University of Rhode Island: *Simplified DES*, URL: https://www.cs.uri.edu/cryptography/dessimplified.htm, letzter Zugriff:

23.5.2018, 16h.

HLbGDV, URL: https://www.uni-kassel.de/einrichtungen/fileadmin/datas/einrichtungen/zlb/Referat_SPS/Webseite_Ref_SPS/03_SPS_I/HLBGDV_vom_28.09.2011.pdf, letzter Zugriff: 30.3.2018, 20h.

Kerncurriculum Informatik, URL: https://kultusministerium.hessen.de/sites/default/files/media/kcgo-in.pdf, letzter Zugriff: 25.5.2018, 14:20h.

Kerncurriculum Mathematik Sek I, URL: https://kultusministerium.hessen.de/sites/default/files/media/kerncurriculum_mathematik_gymnasium.pdf, letzter Zugriff: 25.5.2018, 14:25h.

Kerncurriculum Mathematik Sek II, URL: https://kultusministerium.hessen.de/sites/default/files/media/kcgo-m.pdf, letzter Zugriff: 25.5.2018, 14:30h.

Lehrplan Mathematik. Gymnasialer Bildungsgang. Gymnasiale Oberstufe, (Sek II), URL: https://kultusministerium.hessen.de/sites/default/files/media/go-mathematik.pdf, letzter Zugriff: 27.5.2018, 15h.

Lehrplan Mathematik. Gymnasialer Bildungsgang. Jahrgangsstufen 5 bis 13, (Sek I), URL: https://kultusministerium.hessen.de/sites/default/files/media/g9-mathematik.pdf, letzter Zugriff: 27.5.2018, 11:20h.

reddit.com, URL: https://www.reddit.com/r/IAmA/comments/36ru89/just_days_left_to_kill_mass_surveillance_under/, 2015, letzter Zugriff: 25.5.2018, 21:30h.

Spiegel Online: *Die Kanzlerin entdeckt #Neuland*, URL: http://www.spiegel.de/netzwelt/netzpolitik/kanzlerin-merkel-nennt-bei-obama-besuch-das-internet-neuland-a-906673.html, letzter Zugriff: 25.5.2018, 12h.

Stohr, Monika: *Unterricht in Kryptologie*, Diss. a. d. Ludwig-Maximilian-Universität München, URL: https://edoc.ub.uni-muenchen.de/8456/1/Stohr_Monika.pdf, letzter Zugriff: 27.5.2018, 23h.

Wikipedia: *Integer factorization*, URL: https://en.wikipedia.org/wiki/

Integer_factorization, letzter Zugriff: 17.5.2018, 12:30h.

Wikipedia: *RSA numbers*, URL: https://en.wikipedia.org/wiki/RSA_numbers, letzter Zugriff: 17.5.2018, 12:45h.

Weiterführende Empfehlungen:

Artin, Michael: *Algebra*, Basel: Birkhäuser 1998.

Cryptool Portal, URL: https://www.cryptool.org/de/, letzter Zugriff: 28.5.2018, 20:30h.

Fischer, Gerd: *Lineare Algebra. Eine Einführung für Studienanfänger*, 18. Aufl., Wiesbaden: Springer Spektrum 2014.

Forster, Otto: *Analysis 1. Differential- und Integralrechnung einer Veränderlichen*, 12. Aufl., Wiesbaden: Springer Spektrum 2016.

7. Eidesstaatliche Versicherung

Ich versichere hiermit, dass ich die Arbeit selbstständig verfasst, keine anderen als die angegebenen Hilfsmittel verwandt und die Stellen, die anderen benutzten Druck- und digitalisierten Werken im Wortlaut oder dem Sinn nach entnommen sind, mit Quellenangaben kenntlich gemacht habe.[56]

Kassel, 29. Mai 2018

(Manuel Matting)

[56] Insbesondere ist diese Formulierung entsprechend §33 Abs. 7 HLbGDV.