universität wien

DIPLOMARBEIT / DIPLOMA THESIS

Titel der Diplomarbeit / Title of the Diploma Thesis

„Kryptologie im Mathematikunterricht – Mögliche Inhalte für ein Wahlpflichtfach und fachdidaktische Analysen“

verfasst von / submitted by

Julia Poiß

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Magistra der Naturwissenschaften (Mag. rer. nat.)

Wien, 2017 / Vienna, 2017

Studienkennzahl lt. Studienblatt / degree programme code as it appears on the student record sheet:	A 190 884 406
Studienrichtung lt. Studienblatt / degree programme as it appears on the student record sheet:	Lehramtsstudium UF Mathematik, UF Informatik und Informatikmanagement
Betreut von / Supervisor:	Univ.-Prof. Mag. Dr. Johann Humenberger
Mitbetreut von / Co-Supervisor:	Mag. Dr. Andreas Ulovec

Danksagung

Ich möchte mich an dieser Stelle bei allen Personen, die mich während meinem Studium und dem Verfassen der vorliegenden Diplomarbeit unterstützt und begleitet haben, bedanken.

Ganz herzlich bedanken möchte ich mich bei meinen Betreuern Mag. Dr. Andreas Ulovec und Univ.-Prof. Mag. Dr. Hans Humenberger, die maßgeblich an der Entstehung der Arbeit beteiligt und mir bei allen Problemen und Fragen stets behilflich waren.

Danke sage ich auch meinen Mathemädels Andrea, Anna, Elisabeth, Katja, Sophie und Valerie und meinem Studienkollegen Michael für die Begleitung durch das Studium, die sich immer als motivierend und hilfreich erwies.

Ohne die Unterstützung meiner Familie und meinen Freundinnen und Freunden sei es finanzieller oder anderer Art, wäre mein Studium nicht möglich gewesen – vielen Dank dafür. Ein besonderer Dank geht außerdem an Vera und Max für die Hilfe bei meiner Arbeit.

Danke Philipp, dass du in der Zeit der Entstehung der Diplomarbeit so verständnisvoll und geduldig für mich da warst.

Inhaltsverzeichnis

1. Wahlpflichtfach Mathematik

Im ersten Kapitel der Arbeit geht es um das Wahlpflichtfach Mathematik allgemein. Dazu werden die gesetzlichen Aspekte eines Wahlpflichtfaches, wie und in welchen Schulen es diese gibt und wie der Lehrplan dazu aussieht, dargelegt. Den Abschluss des Kapitels bildet eine kurze Abhandlung darüber, anhand welcher Kriterien Themen für das Wahlpflichtfach Mathematik ausgewählt werden könnten.

1.1 Gesetzliches

Was ist überhaupt ein Wahlpflichtfach? In welchen Schulen gibt es das? Und was lernt man da? Grundlegende Fragen wie diese sollen im folgenden Abschnitt beantwortet und die rechtliche Lage dazu aufgezeigt werden.

Was sind Wahlpflichtfächer?

Unter Wahlpflichtfächern bzw. alternativen Pflichtgegenständen versteht man „jene Unterrichtsgegenstände, deren Besuch zur Wahl gestellt wird, wobei einer von mehreren Unterrichtsgegenständen gewählt werden kann und der gewählte Unterrichtsgegenstand wie ein Pflichtgegenstand gewertet wird“. (Schulorganisationsgesetz, 1962, §8)

Ähnliche Arten von Unterrichtsgegenständen, mit denen Wahlpflichtfächer nicht verwechselt werden sollten, sind verbindliche Übungen, Freigegenstände und unverbindliche Übungen.

Verbindliche Übungen sind für alle Schülerinnen und Schüler[1] der Schule verpflichtend, werden jedoch nicht beurteilt. Zum Beispiel wird in der Sekundarstufe I an vielen Schulen die verbindliche Übung „Berufsorientierung“ angeboten. Für Freigegenstände können sich die Schülerinnen und Schüler freiwillig anmelden. Obwohl diese Gegenstände benotet werden, können sie einen erfolgreichen Abschluss einer Schulstufe nicht verhindern. Unverbindliche Übungen sind weder verpflichtend, noch werden sie beurteilt. (Vgl. Schulorganisationsgesetz, 1962, §8)

Welche Stundenanzahl haben Wahlpflichtfächer?

Wahlpflichtgegenstände sollen in der Oberstufe in der 6., 7. Und 8. Klasse in solchen Stundenanzahlen vorgesehen werden, dass für alle Schülerinnen und Schüler der Schule das Gesamtstundenausmaß, also die Summe der Stundenanzahlen der Pflichtgegenstände und der Wahlpflichtgegenstände, dasselbe ist. (Vgl. Schulorganisationsgesetz, 1962)

Wie viele Schüler und Schülerinnen sind in einem Wahlpflichtfach?

Für den Unterricht in den Wahlpflichtfächern werden Schülergruppen gebildet, die aus mindestens fünf Schülerinnen und Schüler bestehen müssen. Diese Schülergruppen dürfen auch klassenüberreifend geführt werden. Das würde aber heißen, dass ein Wahlpflichtgegenstand nicht abgehalten werden kann, wenn sich weniger als fünf Schülerinnen und Schüler für dieses Fach anmelden. Um diesem Problem zu entgehen, dürfen bei einer zu niedrigen Anmeldezahl auch Schülergruppen schulübergreifend gebildet werden. Dazu müssen die Schulleiterinnen bzw. Schulleiter der betroffenen Schulen zustimmen.

[1] Ausgenommen sind vom Besuch befreite Schüler und Schülerinnen

Allgemein ist auch zu beachten, dass es nicht mehr als viermal so viele Schülergruppen wie Klassen ab der 10. Schulstufe geben darf. (Vgl. Schulorganisationsgesetz, 1962, §43 Abs. 2)

In welchen Schulen in Österreich gibt es Wahlpflichtfächer?

Außer in Allgemeinbildenden höheren Schulen gibt es auch in Polytechnischen Schulen Wahlpflichtfächer. Dort sind „im Hinblick auf die Berufsgrundbildung sowie zur Erweiterung und Vertiefung der Allgemeinbildung erforderliche Unterrichtsgegenstände“ (Schulorganisationsgesetz, 1962, §29 Abs. 1b) als Wahlpflichtfächer anzubieten.

In anderen Schulformen wie Volksschulen, Hauptschulen, Neuen Mittelschulen, Berufsschulen, Berufsbildenden mittleren Schulen, Berufsbildenden höheren Schulen sind keine Wahlpflichtfächer vorgesehen. (Vgl. Schulorganisationsgesetz, 1962, §9 - §82)

Was gibt es sonst noch zu wissen?

Genaue gesetzliche Regelungen zu Fragestellungen über ein Versäumnis der Wahl eines Wahlpflichtfaches und zum Wechsel eines solchen aufgrund eines Schulwechsels oder dem Wunsch einer Schülerin oder eines Schülers sind unter (Schulunterrichtsgesetz, 1986, §11) zu finden.

Was soll im Wahlpflichtfach Mathematik gelehrt werden?

„Das Ziel des Wahlpflicht-Unterrichts ist, den Schülerinnen und Schülern gemäß ihrer Interessen eine Erweiterung bzw. Vertiefung ihres Bildungshorizontes zu bieten.“ (Lehrplan Mathematik WPF, 2004)

Der Lehrstoff für das Wahlpflichtfach Mathematik ist folgendermaßen auszuwählen:

„Wie Lehrplan des Pflichtgegenstandes Mathematik. Die Schülerinnen und Schüler sollen im Rahmen der ausgewählten Themen mit instruktionaler Anleitung selbsttätig Fragen stellen, die sich daraus ergebenden Probleme mit mathematischen Methoden analysieren und gegebenenfalls lösen sowie die Ergebnisse der Arbeit mit zeitgemäßen Hilfsmitteln präsentieren können.

Im Zuge der Erweiterung sind folgende zusätzliche Bereiche möglich: Klassische Probleme der Mathematik; geometrische Probleme; Kongruenzen und Teilbarkeit; zahlentheoretische Probleme; Kryptologie, Codierung; numerische Methoden; Programmierung mathematischer Verfahren; Approximations- und Interpolationsverfahren; Differenzengleichungen und Differentialgleichungen; spezielle Anwendungsprobleme aus Naturwissenschaften, Wirtschaftswissenschaften und anderen Bereichen; Fraktale; Chaostheorie; algebraische Strukturen; Matrizen; Anwendungen komplexer Zahlen; analytische Behandlung von geometrischen Abbildungen; ebene Kurven und Raumkurven; Bogenlänge und Krümmung von Kurven; Darstellungen von Flächen; Differentialrechnung für Funktionen in zwei Variablen; Integralrechnung für Funktionen in zwei Variablen; lineare Optimierung; Graphentheorie; Netzpläne; Spieltheorie; Regression und Korrelation; Wahrscheinlichkeitsverteilungen; statistische Testverfahren; Schätzen von statistischen Parametern; sphärische Trigonometrie.“ (Lehrplan Mathematik WPF, 2004)

1.2 Vorschläge für Kriterien zur Themenauswahl

Der Lehrplan für das Wahlpflichtfach Mathematik besteht nur aus einer Aufzählung von Themen. Alle diese Themen können zeitlich nicht in die zur Verfügung stehenden Unterrichtsstunden gefasst werden. Welche dieser Themen soll man nun unterrichten? Zur Erleichterung der Themenauswahl ist hier eine Kriterien-Sammlung angeführt, die aber keinesfalls auf Vollständigkeit abzielt, sondern Inspiration und Denkanstöße geben soll.

- **Studienrelevanz:**

„Das Ziel der AHS ist die Vermittlung einer umfassenden und vertieften Allgemeinbildung und damit die Schaffung der nötigen Voraussetzungen für ein Universitätsstudium." (Bundesministerium für Bildung, 2015), lautet der erste Satz der Beschreibung der allgemein bildenden höheren Schulen auf der Website des Bundesministeriums für Bildung.

Da speziell im Fach Mathematik der Umstieg zwischen Schul- und Universitätsebene sehr groß und deshalb schwierig für viele Studienanfängerinnen und -anfänger ist, wird hier die Relevanz des Wahlpflichtfachstoffes im Mathematikstudium besonders wichtig sein.

Um bei der Auswahl der Themen für das Wahlpflichtfach auf Studienrelevanz Rücksicht zu nehmen, können z.B. aktuelle Studienpläne und Curricula der österreichischen Universitäten online abgerufen werden. Ein besonderes Augenmerk kann im Fach Mathematik, außer auf das Studium Mathematik, auch auf naturwissenschaftliche, technische und wirtschaftswissenschaftliche Fächer gelegt werden.

- **Anwendungsorientierung:**

<u>Warum Anwendungsorientierung?</u>

Das Verständnis von Mathematik wird durch Anwendungen oft gefördert. (Vgl. Humenberger, 1996, S. 5) Bei einer Befragung von 174 Lehrerinnen und Lehrern hatten folgende Argumente für Anwendungsorientierung einen Zuspruch von über 50%:

„1. Die [Schülerinnen und] Schüler erkennen dadurch besser die Bedeutung, den Sinn von Mathematik („Wozu braucht man das?"), sind dadurch i.a. besser motiviert und arbeiten besser mit. (71%)

2. Explizit genannte Lehrplanziele wie *Argumentieren und exaktes Arbeiten, Darstellen und Interpretieren, produktives geistiges Arbeiten, kritisches Denken und Anwenden von Mathematik* können durch die Einbeziehung von Realitätsbezügen besser erreicht werden. (58%)

3. Viele mathematische Bereiche haben ihren Ursprung eindeutig in der „Praxis" (z.B. Stochastik, Numerik, Lineare Optimierung, Differenzengleichungen, etc.), daher sind mit ihnen sozusagen *naturgemäß* Anwendungen verbunden, die im Unterricht nicht verdrängt werden sollen. (55%)" (Humenberger, 1996, S. 34f)

Das „Lernen in anwendungsorientierten Kontexten" ist auch im Lehrplan Mathematik explizit gewünscht und gefordert. (Vgl. Bundesministerium für Bildung, 2004, S. 2)

Welche Themen sind anwendungsorientiert?

Bei jener bereits genannten Befragung von (Humenberger, 1996), wurden von 202 Mathematikstudentinnen und -studenten, die nach anwendbaren mathematischen Gebieten gefragt wurden, die Gebiete *Prozentrechnung* (53[2]), *Statistik* (49), *Wahrscheinlichkeitsrechnung* (45) und *Zins*- u. *Zinseszinsrechnung* (45) am häufigsten gewählt. Bei den 491 befragten Schülerinnen und Schülern[3] wurden *Wahrscheinlichkeitsrechnung* (151), *Prozentrechnung* (106), *Rechnen*, *insbesondere Grundrechnungsarten* (105), *Extremwertaufgaben* (87) und *Statistik* (85) am öftesten genannt.

- **Fächerübergreifende Vernetzungen:**

Argumente für Fächerübergreifenden Unterricht sind z.B. in (Mastny, 2009, S. 31-35) aufgezählt und dort auch genauer erläutert: Wissen neu ordnen und strukturieren, Verbindung von Wissen und problemlösendes Denken, Eigenverantwortung und Selbstständigkeit, Kommunikation, Ergänzung und Fachunterricht.

Von dem im Lehrplan des Wahlpflichtfaches angeführten Themenpool lassen sich z.B. die Gebiete Kryptologie, Codierung, Programmierung mathematischer Verfahren und spezielle Anwendungsprobleme aus Naturwissenschaften, Wirtschaftswissenschaften und anderen Bereichen gut in fächerübergreifende Zusammenhänge bringen.

- **Interessen der Schülerinnen und Schüler:**

Vielmehr als hier Studien über die mathematischen Interessen von Schülerinnen und Schülern aufzuzählen und so zu vermeintlich „interessanten" Gebieten zu kommen, sind mit diesem Punkt die Interessen der speziellen Schülerinnen und Schüler der zu unterrichtenden Gruppe gemeint. Die Interessen können leicht erfragt werden. Es kann wahrscheinlich helfen, verschiedene Gebiete vorzuschlagen und evtl. kurz zu erklären, worum es geht, da Schülerinnen und Schüler i.A. hauptsächlich die Mathematik aus dem regulären Unterricht kennen. Dieser Punkt könnte auch zusätzlich fächerübergreifend gehandhabt werden, wenn die Schülerinnen und Schüler z.B. besonderes Interesse an Sport, Musik oder anderen Fächern, die sich gut mit Mathematik verbinden lassen, haben.

[2] In den Klammern ist die Anzahl der Nennungen angeführt
[3] 11.Schulstufe: 403, 10. Schulstufe: 88

2. Warum Kryptographie?

Anhand der im vorigen Kapitel vorgeschlagenen Kriterien, soll die Sinnhaftigkeit von Kryptographie als Thema im Wahlpflichtfach untersucht werden.

2.1 Innermathematische Relevanz

Um der Frage, ob die im Rahmen dieser Arbeit behandelten mathematischen Themen auch innermathematisch relevant sind, nachzugehen, wurden ao. Univ-Prof. Mag. Dr. Günther Hörmann, Studienprogrammleiter der Mathematik, und Univ.-Prof. Mag. Dr. Andreas Cap, die beide im Wintersemester 2016 die Einführungsvorlesung des Mathematikstudiums der Universität Wien gehalten haben, dazu befragt.

Cap meint auf die Frage, ob die besprochenen Themen als wichtig für die Mathematik an sich sind, dass sie zwar schon wichtig, von wirklicher Mathematik aber noch weit entfernt seien. Er vergleicht es mit der Wichtigkeit von Schreibschrift für die deutsche Literatur. Ohne Schreibschrift könne man nicht schreiben. Die Themen seien eben noch sehr grundlegend und für manche Gebiete der Mathematik wichtiger als für andere.

Für Hörmann sind diese im Zuge der Arbeit behandelten mathematischen Grundlagen innermathematisch absolut wichtig, „weil sie sozusagen den embryonalen Zustand von manchen Strukturen zeigen, die dann auch woanders wichtig sind“. Sicher überall in der Mathematik wichtig seien die Begriffe Funktion, Injektivität, Surjektivität, Bijektivität und Umkehrfunktion. Die algebraischen Strukturen, Gruppen, seien auch sehr wichtig. Modulares Rechnen diene als Vorbereitung zum Umgang mit Quotientenstrukturen und die Zahlentheorie komme als eine wichtige Disziplin der Mathematik auch immer wieder in Verbindungen vor.

2.2 Studienrelevanz

In welchen Studien sind die Inhalte der hier vorgestellten Aspekte der Kryptographie wichtig? Dazu wurden die Studienpläne einiger relevanter Studien untersucht und mit den in der Arbeit vorkommenden mathematischen Themen verglichen. Zur Studienrelevanz für das Mathematikstudium betreffend haben sich auch die Professoren der Universität Wien ao. Univ.-Prof. Mag. Dr. Günther Hörmann und Univ.-Prof. Mag. Dr. Andreas Cap geäußert.

Bachelor Mathematik:

Im Bachelor Mathematik besteht die StEOP (Studieneingangs- und Orientierungsphase) aus dem Pflichtmodul „Grundlagen der höheren Mathematik“. In den Modulzielen finden sich gleich mehrere der Themen, die in dieser Arbeit zumindest ansatzweise besprochen werden:

- Mathematische Sprache und Denkweise: Operatoren, wie $\forall, \exists, \ldots$, werden immer wieder verwendet, um die Schülerinnen und Schüler an den Umgang damit zu gewöhnen
- Naive Mengenlehre: Injektive, Surjektive und Bijektive Abbildungen
- Grundlegende algebraische Strukturen: Gruppoide, Halbgruppen, Monoide und Gruppen
- Restklasse (mod n): Restklassen an sich kommen zwar in dieser Ausarbeitung nicht vor, es wird aber viel mit Modulo-Operationen gearbeitet

- Euklidischer Algorithmus

Auch im Pflichtmodul „Zahlentheorie“, das für das 2. Semester vorgesehen ist, kommen Inhalte, die den Schülerinnen und Schülern nach Bearbeitung dieses Themas bekannt sein werden, vor:

- Euklidischer Algorithmus
- Eulersche Phi-Funktion
- Kleiner Satz von Fermat

(Vgl. Curriculum Bachelor Mathematik, 2014)

Lehramt Bachelor Mathematik:

Das Pflichtmodul StEOP Unterrichtsfach Mathematik, das im 1. Semester des Studiums zu absolvieren ist, hat unter anderem folgende Modulziele:

- Mathematische Sprache und Denkweise
- Beweismethoden (Induktion, direkt, indirekt): Direkte und Indirekte Beweise werden in dieser Ausarbeitung verwendet
- Abbildungen (injektiv, surjektiv, bijektiv)
- Gruppe
- Restklassen
- Euklidischer Algorithmus
- Teilbarkeit
- Primfaktorzerlegung

(Vgl. Curriculum Unterrichtsfach Mathematik, 2016)

Bachelor Informatik (Universität):

Im Pflichtmodul Netzwerktechnologien „erarbeiten die Studierenden zentrale Ansätze zum Schutz von IT-Systemen auf konzeptueller wie auch strategischer Basis“ (Curriculum Informatik Bachelor, 2016)

Im Wahlmodul Network Security „werden die Schutzziele „Authentifikation“, „Vertraulichkeit“ und „Verfügbarkeit“ erarbeitet. Die Studierenden machen sich dann […] mit softwaretechnischen Lösungen, wie dem Einsatz von kryptographischen Verfahren […] vertraut und wissen, wie sie diese zum Schutz ihrer Daten einsetzen können.“ (Curriculum Informatik Bachelor, 2016)

Bachelor Informatik (Fachhochschule):

Im Modul Informationstheorie ist das Kapitel Restklassen einer der Lehrinhalte, im Modul Mathematik 1 sind das exakte Wiedergeben von mathematischen Definitionen und Beweisen und modulares Rechnen Teile der gewünschten Lernergebnisse. Beide genannten Module sind im 1. Semester abzulegen (Vgl. Curriculum Informatik Bachelor, 2017).

Bachelor Informations- und Kommunikationssysteme:

Die Lernergebnisse des im 1. Semester angesetzten Moduls Angewandte Mathematik 1 sind unter anderem das exakte Wiedergeben von mathematischen Definitionen und Beweisen, modulares Rechnen in $\mathbb{Z}_m$ und Funktionen in einer Variable auf Umkehrbarkeit zu analysieren.

Im 3. Semester gibt es dann das Pflichtmodul Kryptographie und Codierungstheorie, das sich in vielen Bereichen mit den in dieser Arbeit erarbeiteten Themenpunkten überschneidet, jedoch um einiges umfangreicher ausfällt.

(Vgl. Curriculum Informations- und Kommunikationssysteme, 2017)

Sonstige Studien:

Außer in diesen Studien der Mathematik und Informatik sind die gelernten Inhalte wahrscheinlich in keinen weiteren Studien direkt anzuwenden.

2.3 Anwendungsorientierung

Durch die Verwendung der mathematischen Theorie für die Kryptographie wird den Schülerinnen und Schülern die Anwendbarkeit der an sich doch sehr theoretisch wirkenden Teile der Mathematik direkt vor Augen geführt. Die Mathematik wird genau dann gelernt, wenn es für die Anwendung der Kryptographie wichtig ist. Dass auch die Kryptographie anwendungsorientiert ist, zeigt sich in den vielen Anwendungsfeldern: W-LAN, Online Überweisungen, E-Mails, Bankomatkartenabhebungen und Digitale Unterschriften sind nur ein paar der Anwendungen der Kryptographie im Alltag.

2.4 Fächerübergreifende Vernetzungen

Das Thema Kryptographie ist ein fächerübergreifendes Gebiet der Mathematik und Informatik. Die mathematische Theorie wird mit der informationstechnischen Praxis vernetzt. Allerdings beschränken sich die informationstechnischen Aspekte innerhalb dieser Arbeit auf ein Minimum, sodass sie im Zuge des Wahlpflichtfaches Mathematik den Schülerinnen und Schülern ohne große Exkurse oder vorausgesetztes Wissen nähergebracht werden können. Bei Interesse besteht natürlich die Möglichkeit noch mehr auf diese Aspekte einzugehen und das Thema auch von Seiten der Informatik genauer zu betrachten.

2.5 Fazit

Die mathematischen Bereiche, die Schülerinnen und Schüler bei der Bearbeitung des Themas Kryptographie anhand dieser Arbeit kennenlernen, sind zumindest sehr wichtige Grundlagen für innermathematische Konzepte und Ideen. Für ein Studium der Mathematik kann das Gelernte sehr hilfreich sein. Vor allem der Einstieg ins Studium kann erleichtert werden. Im Studium der Informatik oder ähnlicher Richtungen kann das Thema Kryptographie im Laufe des Studiums wieder vorkommen, es kommt aber auf die gewählte Universität bzw. Fachhochschule und den genauen Studiengang an, in welchem Ausmaß das passiert. Eine unbestreitbare Anwendungsorientierung sowohl der mathematischen als auch der informatischen Aspekte und die Vernetzung der mathematischen Theorie mit der informationstechnischen Anwendung kann die Motivation der Schülerinnen und Schüler steigern.

3. Theorieteil

In diesem Kapitel soll eine Erklärung für Lehrerinnen und Lehrer erfolgen, die sich für das Thema Kryptographie interessieren, aber sich bisher zu wenig Wissen dazu aneignen konnten. Außerdem kann es auch als Skriptum für die Schülerinnen und Schüler verwendet werden.

3.1 Was ist Kryptographie? - Terminologie

Den Wunsch Briefe oder Texte zu verschlüsseln gibt es schon, seit es die Schrift gibt. Sei es für Liebesbriefe oder Schatzkarten, das Ziel war dasselbe: gewisse Nachrichten sollten nur von bestimmten Adressaten gelesen werden können.

Kryptographie ist die Wissenschaft der Verschlüsselung von Daten. Es geht um Verfahren, die Informationen vor unbefugten Zugriff bewahren sollen. Um dies zu erreichen, werden mathematische Methoden und Denkweisen benutzt, die auf Computern angewendet werden. (Vgl. Schmeh, 2016, S. 9f.)

Das Wort Kryptographie wurde aus den griechischen Wörtern κρυπτός (kryptós), was auf Deutsch „versteckt, verborgen, geheim“ bedeutet (Vgl. Schenkl, 1859, S. 450), und γράφειν (gráphein), was übersetzt „schreiben“ heißt (Vgl. Schmidt, 1832, S. 500), gebildet.

Nicht zu verwechseln ist die Kryptographie mit der **Kryptanalyse** (manchmal auch Kryptoanalyse genannt). Die Kryptanalyse beschäftigt sich mit dem Knacken von Geheimnachrichten, also dem unbefugten Entschlüsseln von verschlüsselten Daten. **Kryptologie** ist der Überbegriff für die Kryptographie und die Kryptanalyse. (Vgl. Ertel, 2007, S. 18)

Zur Vereinfachung wird das Problem, dass eine Person namens Alice ihrem Freund Bob eine Nachricht über einen nicht gesicherten Weg (z.B. über das Internet oder per Postkarte) senden möchte, behandelt. Eine dritte Person, Eve, kann diesen Weg uneingeschränkt abhören und soll den Inhalt der Nachricht trotzdem nicht verstehen können.

Das Problem kann dadurch gelöst werden, dass nicht die eigentliche Nachricht übertragen wird, sondern ein „Geheimcode“. Der ursprüngliche Text, genannt **Klartext**, wird von Alice mit einem **Chiffrierschlüssel** (oder kurz: Schlüssel) **verschlüsselt** bzw. chiffriert. So erhält sie einen **Chiffriertext**, den „Geheimcode“. Dieser kann nun ohne einen passenden **Dechiffrierschlüssel** nicht mehr in den originalen Klartext zurückversetzt werden. Wenn Alice den Chiffriertext an Bob sendet, kann Eve, obwohl sie die Nachricht abhören kann, nichts mit der Nachricht anfangen. Nur Bob, der den Dechiffrierschlüssel besitzt, kann die Nachricht lesen. (Vgl. Küsters & Wilke, 2011, S. 7)

Das Anwenden eines Chiffrierschlüssels auf einen Klartext, nennt man **Verschlüsselung** oder **Chiffrierung**. Das Gegenverfahren dazu heißt **Entschlüsselung** oder **Dechiffrierung**.

Das Problem könnte auch auf andere Arten gelöst werden. So könnten sich Alice und Bob alleine an einem sicheren Ort treffen, um sicherzustellen, dass sie von niemandem belauscht werden, was eine Organisatorische Maßnahme wäre. Als Physikalische Maßnahme könnte Alice ihre Nachricht an Bob als Brief versenden, den sie mit Geheimtinte verfasst. Für diese Arbeit ist jedoch nur die oben genannte kryptographische Maßnahme interessant. (Vgl. Beutelspacher, Schwenk, & Wolfenstetter, Moderne Verfahren der Kryptographie, 2006, S. 1)

Eine Nachricht wird mit einer Schrift verfasst, die eine nichtleere, endliche Menge an Zeichen verwendet. So eine Menge wird **Alphabet** genannt. (Vgl. Freiermuth, Hromkovic, Keller, & Steffen, 2010, S. 10) In dieser Arbeit wird meist das lateinische Alphabet

$$lat = \{a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z\}$$

verwendet. Die Satzzeichen werden einfach weggelassen und Umlaute durch ae, oe und ue ersetzt. Ein „ß“ wird als „ss“ geschrieben. Wie im definierten Alphabet zu erkennen ist, werden auch nur Kleinbuchstaben benutzt. Ein anderes Beispiel für ein Alphabet können auch die Schriftzeichen anderer Sprachen sein, wie z.B. das griechische oder kyrillische Alphabet. In dieser Arbeit ist auch noch das binäre Alphabet

$$bin = \{0, 1\}$$

wichtig. Aber auch beliebige Zeichenfolgen oder Zahlen können ein Alphabet bilden. Hier sind einige Beispiele:

$$cards = \{♥, ♦, ♣, ♠\}$$

$$digits = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

$$alphabet_1 = \{♪, 2, *, j, \%, ☼, a\}$$

Eine Folge mehrerer Buchstaben eines Alphabets wird **Text** genannt. Auch die Buchstabenfolge „aefigh“ wird als Text aus dem Alphabet *lat* bezeichnet, auch wenn sie keine eindeutige Bedeutung hat. Es kann sich hierbei auch um einen Chiffriertext handeln, der erst entschlüsselt werden muss, um die Bedeutung erkennen zu können. Im gerade definierten $alphabet_1$ kann auch der Text „2♪*☼“ gebildet werden. (Vgl. Freiermuth, Hromkovic, Keller, & Steffen, 2010, S. 10)

Als **Länge eines Textes** wird die Anzahl der Buchstaben in der Buchstabenfolge bezeichnet. In vielen Alphabeten ist es auch sinnvoll eine **Ordnung** der einzelnen Buchstaben festzulegen. Im lateinischen Alphabet können die Buchstaben wie gewohnt geordnet werden, sodass Ord(a) = 0, Ord(b) = 1, …, Ord(z) = 25. (Vgl. Freiermuth, Hromkovic, Keller, & Steffen, 2010, S. 12f.)

3.2 Ziele der Kryptographie

Manchmal werden die durch Kryptographie zu erreichenden Ziele, nämlich Vertraulichkeit, Authentizität, Integrität und Verbindlichkeit, auch **Sicherheitsdienste** genannt (Vgl. Spitz, Pramateftakis, & Swoboda, 2011, S. 2). Diese Begriffe werden in den folgenden Absätzen näher erläutert.

Verschlüsselungen verlangen nicht immer nach allen möglichen Sicherheitsdiensten, es kommt auf den Anwendungskontext an. So kann es sein, dass ein Empfänger eines unterschriebenen Vertrages versichert sein möchte, dass der Vertrag verbindlich ist und nicht verändert wurde, es aber kein Problem darstellt, falls dieser öffentlich lesbar ist. Für die unterschiedlichen Sicherheitsdienste werden manchmal unterschiedliche Namen verwendet, die Bedeutung ist jedoch immer dieselbe. Hier wurden die Namen nach (Dorfmayr, 2007) verwendet.

Das ursprüngliche Ziel der Kryptographie war **Vertraulichkeit**. Lange Zeit war es die einzige Aufgabe, die mit Verschlüsselungen erreicht werden sollte, und auch jetzt wird es noch oftmals als Hauptziel angesehen. Vertraulichkeit bzw. Zugriffsschutz bedeutet Geheimhaltung, also dass keine unautorisierten Personen die Informationen einer Nachricht lesen können sollen. Vertraulichkeit kann in den unterschiedlichsten Situationen, wie beim Versenden von Liebesnachrichten, medizinischen Informationen oder Bankdaten wichtig sein.

In der modernen Kryptographie wurden aber auch neue Sicherheitsdienste wichtig, so auch die **Authentizität**. Unter Authentizität versteht man die Sicherstellung der Identität des Absenders vom Empfänger. Der Empfänger soll also nachprüfen können, ob der Absender wirklich der ist, für den er sich ausgibt. Außerhalb der elektronischen Medien ist dieser Sicherheitsdienst durch Aussehen, Stimme oder Handschrift meist gegeben. Wenn beispielsweise Alice eine E-Mail an Bob sendet, in der sie um eine Geldüberweisung von ihm bittet, ist kryptographische Sicherheit, dass es sich wirklich um Alice handelt, wichtig.

Weiters kann auch **Integrität** notwendig oder gewünscht sein. Integrität bedeutet Änderungsschutz, also die Möglichkeit nachzuprüfen, ob die Nachricht verändert wurde. Verändert heißt nicht nur, dass wirklich ein Teil oder die ganze Nachricht ausgetauscht wurde, sondern auch wenn ein Teil der Nachricht fehlt oder etwas zur Nachricht hinzugefügt wurde. Wenn beim vorherigen Beispiel, Alice auch ihre Kontodaten in dieser E-Mail mitsendet, reicht es für Bob nicht, sicher zu sein, dass die E-Mail von Alice stammt. Die Kontodaten könnten verändert worden sein, sodass er das Geld an jemand anderen sendet. Er muss sich also auch sicher sein können, dass die E-Mail nicht verändert wurde.

Zuletzt gibt es als Ziel noch die **Verbindlichkeit** bzw. Nichtabstreitbarkeit. Die Identität des Absenders soll auch gegenüber Dritten nachweisbar sein, sodass dies nicht bestreitbar ist. Dies ist zu vergleichen mit einer Unterschrift, die jemanden an das, was geschrieben oder unterschrieben wurde, bindet. Wenn z.B. ein Vertrag über elektronische Medien abgeschlossen wird, soll dieser trotzdem nachweisbar und verbindlich sein. (Vgl. Dorfmayr, 2007, S. 27)

3.3 Verschlüsselungsarten anhand historischer Verfahren

Seit den Anfängen der Kryptographie wurden verschiedene Arten der Nachrichtenverschlüsselung verwendet. Ein Teil davon soll hier angeführt und kurz besprochen werden.

3.3.1 Polybios

Bereits 200 Jahre vor unserer Zeitrechnung wurde eine der ersten Verschlüsselungsarten verwendet. Der griechische Geschichtsschreiber Polybios hatte sich ein System ausgedacht, mit dem die griechischen Buchstaben durch Zahlen verschlüsselt wurden. Der Geheimtext wurde mit dem Alphabet {1, 2, 3, 4, 5} verfasst, und je zwei dieser Ziffern standen für einen der 24 griechischen Buchstaben. Wenn das Alphabet wie in Tabelle 1 aufgeschrieben wurde, konnten die Verschlüsselungszahlen wie die Indizes einer Matrix abgelesen werden. So wäre z.B. ein σ (sigma) als 43 kodiert. (Vgl. Freiermuth, Hromkovic, Keller, & Steffen, 2010, S. 6)

Die Entschlüsselung funktioniert dann genau umgekehrt: Man erhält zwei Zahlen n und m. Dann sucht man sich in der Polybios-Tabelle die n. Zeile und m. Spalte und liest den entsprechenden Klartext-Buchstaben ab.

Tabelle 1: Polybios-Tabelle

	1	**2**	**3**	**4**	**5**
1	α	β	γ	δ	ϵ
2	ζ	η	θ	ι	κ
3	λ	μ	ν	ξ	ο
4	π	ρ	σ	τ	υ
5	φ	χ	ψ	ω	

Ein Beispiel:

Wir erhalten den Geheimtext 4135314512243543 und wissen, dass er mit Polybios verschlüsselt wurde. Da jeweils zwei Ziffern einen Buchstaben kodieren, können wir den Text leichter lesen, wenn wir Leerzeichen einfügen:

41 35 31 45 12 24 35 43

Als erstes Zahlenpaar erhalten wir also 41. D.h. wir suchen den Buchstaben in der 4. Zeile und 1. Spalte: π. Danach schauen wir in die 3. Zeile und 5. Spalte: ο. Insgesamt ergibt sich dann

π ο λ υ β ι ο σ

Wer das griechische Alphabet beherrscht, kann nun den Klartext schon lesen, ansonsten kann Tabelle 2 zu Hilfe genommen werden.

Tabelle 2: Griechische Kleinbuchstaben

α	Alpha	ι	Iota	ρ	Rho
β	Beta	κ	Kappa	σ	Sigma
γ	Gamma	λ	Lambda	τ	Tau
δ	Delta	μ	My	υ	Ypsilon
ϵ	Epsilon	ν	Ny	φ	Phi
ζ	Zeta	ξ	Xi	χ	Chi
η	Eta	ο	Omikron	ψ	Psi
θ	Theta	π	Pi	ω	Omega

In lateinischer Schrift erhalten wir also den Klartext „Polybios“.

Anhand des Beispiels ist schon zu sehen, dass das Klartext-Alphabet nicht immer mit dem Geheimtext-Alphabet übereinstimmen muss. Um eine Verschlüsselung zu definieren, muss darum auch angegeben werden, in welchem Alphabet man sich im Klartext und im Geheimtext befindet. Auch die in Kapitel 3.1: *„Was ist Kryptographie? – Terminologie“* bereits definierten Alphabete *bin* = {0, 1} oder *cards* = {♥, ♦, ♣, ♠} können als Klartext- und/oder Geheimtext-Alphabet verwendet werden.

Polybios verwendet als Klartext-Alphabet das Alphabet

greek = {α, β, γ, δ, ϵ, ζ, η, θ, ι, κ, λ, μ, ν, ξ, ο, π, ρ, σ, τ, υ, φ, χ, ψ, ω}

und als Geheimtext-Alphabet

{1, 2, 3, 4, 5}.

Der Schlüssel dieser Chiffrierung besteht nur aus der Polybios-Tabelle. Das heißt, wer einmal erfahren hat, wie die Geheimschrift funktioniert, kann jeden auf diese Art verschlüsselten Geheimtext entschlüsseln, da man keine weiteren Schlüssel-Informationen benötigt. Das führt natürlich zu einer sehr niedrigen Sicherheit dieses Verfahrens.

Eine naheliegende Idee, die Chiffrierung so zu verändern, dass der Schlüssel anders als die angegebene Tabelle aussieht, ist, die Tabelle immer wieder zu verändern. So könnte das Geheimtext-Alphabet von {1, 2, 3, 4, 5} auf {6, 7, 8, 9, 0} abgeändert werden. Auch die griechischen Buchstaben können in einer anderen Reihenfolge in die Tabelle eingetragen werden, sodass sie mit anderen Zahlenkombinationen ver- und entschlüsselt werden. In allen diesen Fällen bildet die neue, veränderte Tabelle, den neuen Chiffrierschlüssel.

Eine weitere Idee wäre es, den griechischen Buchstaben, wie in Kapitel 3.1, Ordnungsnummern zu verpassen, und den Text damit zu verschlüsseln. So wäre z.B. Ord(δ) = 4, also würde δ als 4 im Geheimtext codiert werden und anders herum die Zahl 4 im Geheimtext als δ entschlüsselt werden. Ord(λ) = 11, d.h. λ wird als 11 verschlüsselt und 11 als λ entschlüsselt. Das sieht auf dem ersten Blick nach einer ähnlichen Verschlüsselung wie die der Polybios-Verschlüsselung, und somit einer möglichen, wenn auch nicht besonders sicheren, Chiffrierung, aus. Bei genauerer Betrachtung, fällt jedoch ein Problem bei dieser Art der Verschleierung des Textes auf. Wenn man z.B. den Geheimtext 411 erhält, könnte dieser als „4 11“ = „δ λ“, oder auch als „4 1 1“ = „δ α α“ verstanden werden, was natürlich nicht gewollt ist. Genauer gesagt, widerspricht das sogar der Definition einer Codierung, diese Veränderung des Textes gilt also nicht als Verschlüsselung oder Chiffrierung. (Vgl. Freiermuth, Hromkovic, Keller, & Steffen, 2010, S. 13)

Für eine gültige Chiffrierung muss nämlich die Ver- und Entschlüsselung auf jeden Fall eindeutig sein. Mathematisch basiert diese Eigenschaft auf der Injektivität von Funktionen. Näheres dazu findet sich in Kapitel 3.5.2: „Funktionen: Injektivität, Surjektivität und Bijektivität“

3.3.2 Skytale

Ab ca. 500 v. Chr. wurde die Skytale verwendet. Ein Leder- oder Pergamentband wurde spiralförmig um einen Holzstab gewickelt und die Nachricht entlang des Stabes darauf geschrieben. Danach wurde das Pergament wieder vom Stab genommen und versendet. Die Buchstaben waren nun durcheinander und so auch die Nachricht nicht mehr lesbar. Nur ein Empfänger, der das Band wieder um einen Stab desselben Durchmessers wickelte, konnte die Nachricht wieder entziffern.

Diese Art der Verschlüsselung, bei der die verwendeten Zeichen nur in eine andere Reihenfolge gebracht werden, wird Transpositions-Chiffre genannt.

Da im Chiffretext dieselben Zeichen in derselben Häufigkeit verwendet werden wie im Klartext, kann hier die Häufigkeitsverteilung der Buchstaben nicht zum Knacken der Chiffre

verwendet werden. Dass dies z.B. bei der Caesar-Verschlüsselung möglich ist, wird im nächsten Abschnitt aufgezeigt. (Vgl. Spitz, Pramateftakis, & Swoboda, 2011, S. 3f.)

Abbildung 1: Skytale mit Lederstreifen[4]

3.3.3 Caesar-Chiffre

Dieser einfache Algorithmus wurde nach Gaius Julius Caesar (100 v. Chr. - 44 v. Chr.) benannt. Er soll dieses Verfahren für die Korrespondenz mit seinen Generälen verwendet haben (Vgl. Küsters & Wilke, 2011, S. 7).

Die Funktionsweise ist einfach: Jeder Buchstabe des Klartextes wird im Chiffriertext durch den um k Buchstaben später im Alphabet folgenden Buchstaben ersetzt. Als Alphabet wird das in *Kapitel 3.1: „Was ist Kryptographie? – Terminologie“* definierte lateinische Alphabet verwendet. Wenn das Ende, also der Buchstabe „z“ erreicht wird, wird einfach wieder von vorne, bei „a“, begonnen. Der geheime Schlüssel für dieses symmetrische Verfahren ist der Wert k. Julius Caesar hat für die Verschlüsselung den Wert k = 3 verwendet.

Verwendet Alice k = 2, wird z.B. aus der Nachricht „bob der schluessel liegt unter der matte alice“ der Chiffriertext „dqd fgt uejnwguugn nkgiv wpvgt fgt ocvvg cnkeg“. Auf den ersten Blick, sieht es aus, als wäre es nicht leicht zu erraten, was der Originaltext der Nachricht war. Da k sinnvollerweise aber nur Werte aus [1;25] annehmen kann, wäre die Nachricht mit dem Wissen, dass es sich um eine Caesar-Chiffre handelt, leicht geknackt.

Ein Beispiel:

> Angenommen wir fangen die Nachricht „glh yruohvxqj lvw vr odqjzhlolj jhkhq zlu olhehu dxi hlq elhu“ ab und wollen sie entschlüsseln. Weil wir (noch) nicht viele Verschlüsselungsarten kennen, versuchen wir zuerst die 25 Möglichkeiten der Caesar-Verschlüsselung. Mit k = 1, also wenn wir alle Buchstaben um 1 im Alphabet zurücksetzen, erhalten wir: „fkg xqtnguwpi kuv uq ncpiygknki igjgp ykt nkgdgt cwh gkp dkgt“ – das hört sich nach keiner sinnvollen Nachricht in uns bekannten Sprachen an. Auch k = 2 ergibt keine lesbare Nachricht. Beim Versuch mit k = 3 ergibt sich „die vorlesung ist so langweilig gehen wir lieber auf ein bier“, was sofort als deutscher Satz identifiziert werden kann.

Die Caesar-Chiffre kann verbessert werden, indem die Buchstaben nicht durch einen fixen Wert k im Alphabet verschoben werden, sondern jeder Buchstabe durch einen beliebigen anderen ersetzt wird. Jedoch muss ein Buchstabe immer durch denselben ersetzt werden und umgekehrt. Diese Verschlüsselung wird monoalphabetische Chiffre genannt. Ein möglicher Schlüssel für diese Chiffre ist in Tabelle 3 dargestellt.

[4] Abgerufen am 15. März 2017 von https://commons.wikimedia.org/wiki/File:Skytale.png

Tabelle 3: Monoalphabetische Chiffre

Klartext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Chiffretext	o	k	a	m	t	w	z	x	u	r	q	b	y	s	i	d	f	e	v	g	j	h	l	c	n	p

Für eine monoalphabetische Chiffre über das lateinische Alphabet gibt es schon 26! ($\approx 4 \cdot 10^{26}$) mögliche Schlüssel. Obwohl es zu viel Aufwand wäre, alle 26! möglichen Kombinationen auszuprobieren, ist es trotzdem noch relativ leicht diese Chiffre zu knacken. Wie schon bei der Skytale erwähnt, kann man sich hier z.B. der Häufigkeitsverteilung der Buchstaben einer Sprache bedienen. So sind in einem typischen deutschen Text die Buchstaben „e“ (17,4%) und „n“ (9,8%) am häufigsten vertreten (Vgl. Gartner, 2010). Die häufigsten Doppelbuchstaben sind „ss“ und „nn“ und die häufigsten Bigramme[5] „er“ und „en“ (Vgl. Hebisch, 2010). Wenn Eve diese Statistiken kennt und die Nachricht abfängt, kann sie so einige Buchstabenkombinationen schneller herausfinden. Wenn sie außerdem vermutet, dass die Namen Bob und Alice im Text vorkommen, wird es natürlich noch leichter. (Vgl. Kurose & Ross, 2013, S. 676f.)

3.3.4 Vigenère-Chiffre

Im 16. Jahrhundert wurden polyalphabetische Chiffrierungen erfunden.

Einschub: ***Monoalphabetische und Polyalphabetische Chiffrierungen***

> Monoalphabetische Chiffrierungen arbeiten mit nur einer Alphabet-Zuordnungsliste. Das heißt, wenn ein bestimmter Buchstabe, z.B. e, einmal mit einem anderen Buchstaben, z.B. x, kodiert wurde, dann wird er in diesem Text immer so codiert, also jedes e durch ein x ersetzt.
> Polyalphabetische Chiffrierungen verwenden hingegen mehrere Alphabet-Zuordnungslisten. Es wird dann z.B. nach jedem Buchstaben die Zuordnungsliste gewechselt, sodass auch direkt aufeinanderfolgende gleiche Buchstaben, z.B. ss, durch verschiedene Buchstaben, z.B. am, chiffriert werden können. Wie eine polyalphabetische Chiffrierung genau funktionieren könnte, wird hier am Beispiel der Vigenère-Chiffre gezeigt. (Vgl. Spitz, Pramateftakis, & Swoboda, 2011, S. 5ff)

Der Name Vigenère-Chiffre bezieht sich auf Blaise de Vigenère (1523 - 1596). Die Vigenère-Verschlüsselung verwendet mehrere Caesar-Chiffren mit unterschiedlichen Schlüsseln k. Ein Schüssel k einer Vigenère-Chiffre kann sich z.B. aus 4 Schlüsseln k_1, k_2, k_3, k_4 von Caesar-Chiffren zusammensetzen. Dann wird der erste Buchstabe des Klartextes wie bei einer Caesar-Chiffre mit k_1 verschlüsselt. Da am Ende der Schlüsselfolge wieder mit dem ersten Schlüssel begonnen und das Schema periodisch fortgesetzt wird, wird auch der fünfte, neunte, dreizehnte, usw. Buchstabe des Klartextes auf dieselbe Art verschlüsselt. Für die Verschlüsselung des zweiten, sechsten, zehnten, usw. Buchstabens, wird der Schlüssel k_2 verwendet. Analog wird auch mit k_3 und k_4 fortgesetzt. Ein Beispiel für eine Vigenère-Chiffre-Tabelle ist Tabelle 4. Hier ist auch zu sehen, dass z.B. zwei der Schlüssel gleich sein können. (Vgl. Spitz, Pramateftakis, & Swoboda, 2011, S. 7)

[5] Zwei aufeinanderfolgende Buchstaben

Tabelle 4: Vigenère-Chiffre

Klartext	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
k_1=1	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
k_2=11	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
k_3=20	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
k_4=1	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a

Die Beispielnachricht von vorher „bob der schluessel liegt unter der matte alice“, würde nun zu „czv efc mdiwoftdym mtyhu fhufc xfs xuuup umjny“ werden. Der erste Buchstabe „b“ wurde mit k1 verschlüsselt, also zu „c“. Der zweite Buchstabe „o“ mit k_2 zu „z“, usw. Gleich beim Namen Bob ist zu erkennen, dass nun derselbe Buchstabe („b“) zu verschiedenen Buchstaben („c“ und „v“) verschlüsselt werden kann, je nachdem an welcher Stelle des Klartextes er verwendet wird. (Vgl. Kurose & Ross, 2013, S. 678)

Anstatt sich den Schlüssel als k = {k_1 = 1, k_2 = 11, k_3 = 20, k_4 = 1} zu merken, können die Buchstaben, durch die „a“ ersetzt werden soll, den Schlüssel bilden, was in diesem Fall k = „blub“ ergeben würde[6]. Dafür gibt es auch ein sogenanntes Vigenère-Quadrat, das in Tabelle 5 zu sehen ist.

In diesem Beispiel würde man zuerst in Spalte „b“ (Klartext-Buchstabe „b“ von „bob“), Zeile „b“ (Schlüssel-Buchstabe „b“ von „blub“) gehen und den Chiffrier-Buchstaben „c“ finden. Dann in Spalte „o“, Zeile „l“, um den Buchstaben „z“ zu finden, usw.

Natürlich sollte dafür kein zu einfaches Wort gewählt werden, denn wenn es erraten wird und die Verschlüsselungsart bekannt ist, kann bereits die gesamte Nachricht entschlüsselt werden.

Die Vigenère-Chiffre ist sehr viel schwieriger als die Caesar-Chiffre zu knacken. So wurde sie erst drei Jahrhunderte nach ihrer Erfindung systematisch geknackt. (Vgl. Spitz, Pramateftakis, & Swoboda, 2011, S. 7)

[6] Siehe dazu die Markierung in Tabelle 5

Tabelle 5: Vigenere-Quadrat

	Klartext-Buchstabe																								
Schlüssel - Buchstabe	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

3.3.5 Vernam-Chiffre

1917 wurde von Gilbert S. Vernam (1890 – 1960) eine Chiffre erfunden, die die Vigenère-Chiffre sozusagen erweitert. Verändert wurde das Alphabet und die Schlüsselfolge: Statt 26 Buchstaben werden nur noch die beiden Zeichen 0 und 1 verwendet und der Schlüssel, der immer nur einmal verwendet wird, ist in der Vernam-Chiffre genauso lang wie der Klartext selbst. (Vgl. Spitz, Pramateftakis, & Swoboda, 2011, S. 10)

Hat man nun einen Klartext und einen Schlüssel, wird die Addition modulo 2 durchgeführt, um den Chiffretext zu erhalten. Zur Entschlüsselung kann wieder die Addition modulo 2 verwendet werden, da sie identisch mit der Subtraktion modulo 2 ist. Wie die Addition bzw. Subtraktion modulo 2 funktioniert, ist im Kapitel 3.5.4 „Modulares Rechnen“ erklärt, als kleine Übersicht ist aber auch die Verknüpfungstabelle[7] der Addition modulo 2 in Tabelle 6 gegeben.

[7] Wie eine Verknüpfungstabelle zu lesen ist, ist in *Kapitel 3.5.3: „Grundlegende Mathematische Strukturen“* erklärt

Tabelle 6: Addition modulo 2

+	**0**	**1**
0	0	1
1	1	0

Der Schlüssel wird immer nur einmal, für eine Ver- und eine Entschlüsselung, verwendet (One-Time-Pad). Bei der Erzeugung eines Schlüssels wird wie bei mehrmaligem Münzwurf Stelle für Stelle zufällig eine Ziffer entschieden, wobei „0“ und „1“ jeweils mit einer Wahrscheinlichkeit von 0,5 gewählt werden. (Vgl. Spitz, Pramateftakis, & Swoboda, 2011, S. 11)

Ein Beispiel:

> Der Klartext ist „010101110001“ mit dem Schlüssel „110010010011“.
> Addition modulo 2:
>
> | | |
> |---|---|
> | 010101110001 | Klartext |
> | 110010010011 | Schlüssel |
> | **100111100010** | **Chiffriertext** |
>
> Damit erhalten wir den Chiffriertext. Wird wieder eine Addition modulo 2 mit dem Schlüssel durchgeführt, kommen wir zurück zum Klartext.
>
> | | |
> |---|---|
> | 100111100010 | Chiffriertext |
> | 110010010011 | Schlüssel |
> | **010101110001** | **Klartext** |

Dass der Schlüssel bei Anwendung dieser Chiffre immer nur einmal verwendet wird, wirkt sich natürlich positiv auf deren Sicherheit aus. Allerdings wird damit das Problem der Schlüssel-Übermittlung zusätzlich erschwert. Müsste man sich für die Verwendung der Vigenère-Chiffre nur einmal treffen bzw. nur einmal eine sichere Möglichkeit finden, um einen geheimen Schlüssel auszutauschen, muss man für die Verwendung der Vernam-Chiffre vor jeder gewünschten Nachrichtenübermittlung erneut einen geheimen Schlüssel auf eine sichere Art übermitteln – dann könnte man doch auch gleich die geheime Nachricht überbringen, anstatt den Schlüssel? Man merkt schon, dass dieses Problem nicht unbedeutend ist. Wie es gelöst wurde, ist in Kapitel 3.4: *„Asymmetrische Verschlüsselung“* zu lesen.

3.3.6 Enigma

Enigma kommt vom griechischen Wort αίνιγμα (aínigma), was auf Deutsch „Rätsel, Anspielung“ bedeutet (Vgl. Schenkl, 1859, S. 19).

Das Kapitel über die Enigma wird in dieser Arbeit anhand der Werke (Spitz, Pramateftakis, & Swoboda, 2011, S. 12ff.) und (Freiermuth, Hromkovic, Keller, & Steffen, 2010, S. 172 - 180) bearbeitet.

Die Enigma[8] ist eine kryptographische Maschine, die vom deutschen Ingenieur Arthur Scherbius (1878 – 1929) 1918[9] patentiert und von der deutschen Wehrmacht im 2. Weltkrieg (1939 – 1945) verwendet wurde.

Das Herzstück des Verschlüsselungsmechanismus der Maschine arbeitet mit drei Rotorscheiben und einer Umkehrscheibe. Ansonsten besteht die Enigma aus einer Tastatur, einem Lampenfeld, das alle Buchstaben enthält und einem Steckbrett. Verwendet wird der Apparat, indem der Klartext auf der Tastatur, wie bei einer Schreibmaschine, eingegeben wird. Die Klartextbuchstaben werden von der Maschine übersetzt und die jeweiligen Lampen leuchten auf. Dann kann der so erhaltene Chiffriertext versendet werden. In Abbildung 2 ist ein Foto einer Enigma mit Beschriftungen der Teile zu sehen.

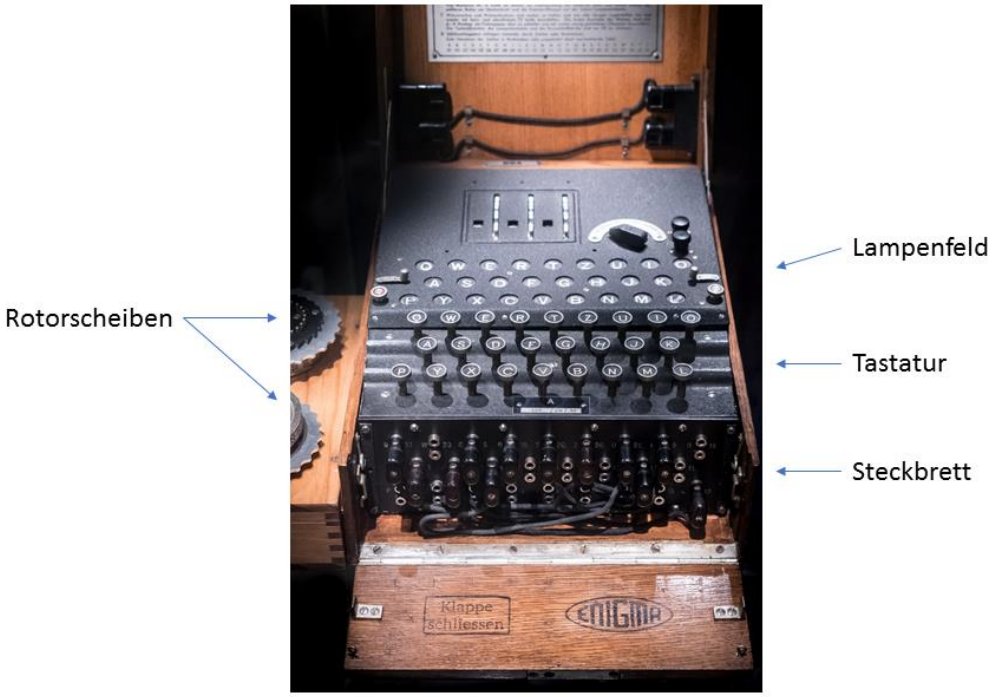


Abbildung 2: Enigma[10]

[8] Fast zeitgleich wurden ähnliche Maschinen und Varianten von mehreren Personen erfunden. In dieser Arbeit ist, wenn nicht anders geschrieben, die Enigma I von Arthur Scherbius gemeint.
[9] Chiffrierapparat DRP Nr. 416 219 (Deutsches Reichspatentamt, 1925)
[10] Abgerufen am 29. März 2017 von https://upload.wikimedia.org/wikipedia/commons/f/f8/Enigma_%2820967055154%29.jpg
Urheber: William Warby

Die Rotorscheiben können jeweils auf 26 verschiedene Positionen gedreht werden. Bei der Enigma gibt es fünf verschiedene Rotorscheiben, von denen für eine Verschlüsselung immer drei in die Maschine eingesetzt werden. Auch die Anordnung der drei ausgewählten Scheiben kann verändert werden. Eine Rotorscheibe hat rechts und links jeweils 26 Kontakte (für die 26 Buchstaben des lateinischen Alphabets), wobei jeder rechte Kontakt mit einem linken Kontakt durch einen Draht verbunden ist. Die Verbindungen sind willkürlich ausgewählt.

Die Umkehrwalze befindet sich hinter den drei Rotorscheiben und hat nur auf der rechten Seite 26 Kontakte. Diese sind wiederum willkürlich paarweise miteinander verdrahtet. Die Umkehrwalze ist fest verankert und kann nicht gedreht werden. (Siehe Abbildung 3)

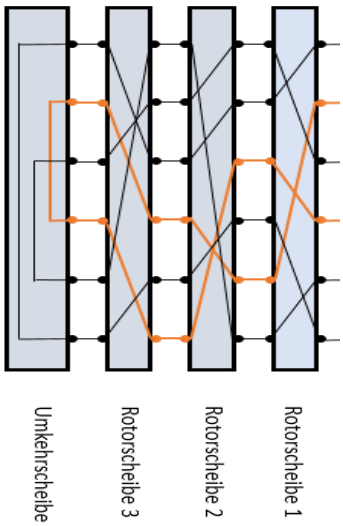


Abbildung 3: Rotorscheiben und Umkehrscheibe

Zusätzlich zum Verschlüsselungsmechanismus der Rotorscheiben, gibt es auch noch das Steckbrett. Es ist zwischen der Tastatur und der ersten Rotorscheibe geschaltet. Auf dem Steckbrett können mit sechs Kabeln die elektrischen Wege von je zwei Buchstaben miteinander vertauscht werden. In Abbildung 4 wurden z.B. die Buchstaben C und D vertauscht. Jene Buchstaben, die nicht vertauscht wurden, folgen ihrem Weg einfach weiter zur ersten Rotorscheibe.

Das Steckbrett und die Rotorscheiben an sich ergeben bereits eine Verschlüsselung mit einer hohen Anzahl an möglichen Schlüsseln, jedoch ist dadurch nur eine monoalphabetische Verschlüsselung möglich. Das Herzstück der hohen Sicherheit der Enigma bringen die Drehungen der Rotorscheiben. Durch jede Eingabe eines Buchstabens auf der Tastatur wird die erste Rotorscheibe um eine Position im Uhrzeigersinn weitergedreht. Nach einer vollen Umdrehung der Rotorscheibe 1 (= 26 Eingaben) dreht sich die zweite Rotorscheibe um eine Position weiter. Erst wenn auch die zweite Rotorscheibe eine vollständige Umdrehung gemacht hat (= 26 · 26 = 676 Eingaben), dreht sich die dritte Rotorscheibe das erste Mal um eine Position weiter. Bis alle möglichen Zustände der drei Rotorscheiben durchlaufen sind, braucht man also 26 · 26 · 26 = 17576 Eingaben. Diese Drehungen der Rotorscheiben kann man sich wie einen Kilometerzähler vorstellen. Anstatt zehn Positionen pro Scheibe, gibt es 26. Durch diese Funktionsweise wird der Text polyalphabetisch verschlüsselt: Nach jedem Buchstaben ändert sich das Zuordnungsschema durch die Drehung der Scheiben. Die Periode des Schemas übersteigt mit 26^3 normalerweise auch die Länge des Klartextes, sodass die Buchstaben innerhalb eines Textes nie mit dem gleichen Zuordnungsschema verschlüsselt werden.

In Abbildung 4 ist die Funktionsweise der Enigma schematisch dargestellt. Zur Vereinfachung der Grafik sind nur die ersten sechs Buchstaben des Alphabets zu sehen, die restlichen 20 würden analog funktionieren. Als Beispiel ist zu sehen, wie der Buchstabe B auf der Tastatur betätigt wird. Der Strom fließt durch den Anschluss des gedrückten Buchstabens. Auf dem Steckbrett fließt er in die festgelegte Leitung weiter und durch alle Rotorscheiben, um zur

Umkehrscheibe zu gelangen. Danach fließt der Strom auf einem anderen Weg wieder zurück durch die Rotorscheiben und bringt die Glühlampe C zum Leuchten, was signalisiert, dass der Klartextbuchstabe B mit dem Chiffrierbuchstaben C zu verschlüsseln ist.

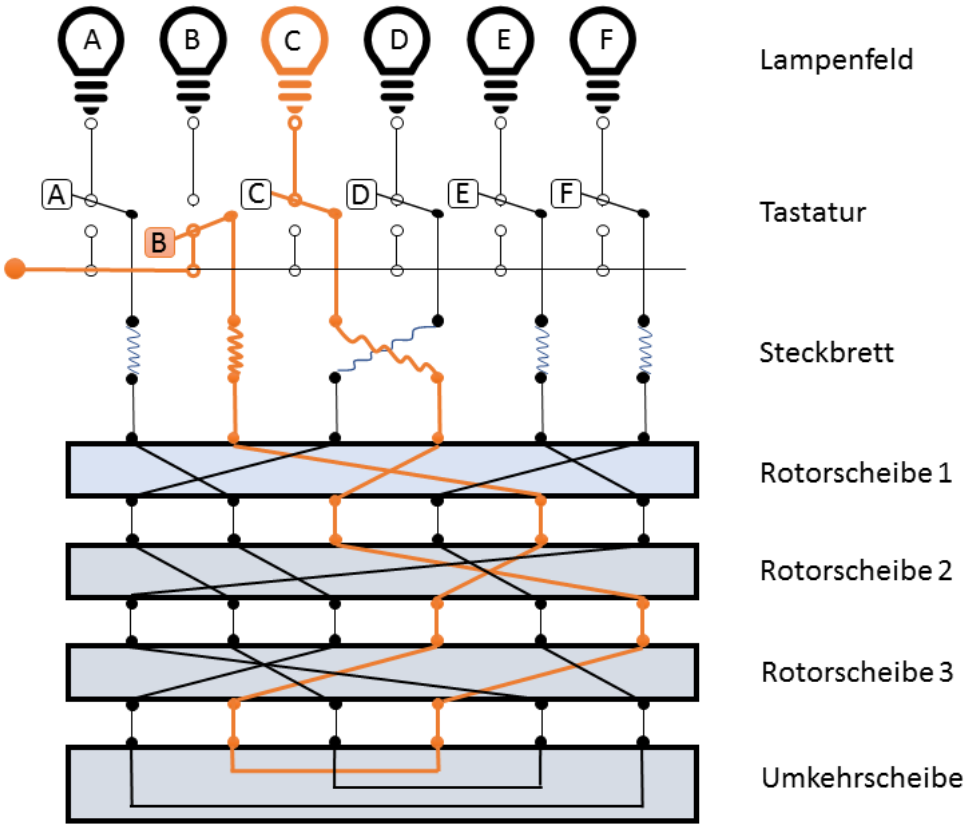


Abbildung 4: Funktionsweise der Enigma

Alan Turing baute 1940 gemeinsam mit seinem Team eine Maschine, die die Verschlüsselung der Enigma in kurzer Zeit entschlüsseln konnte (Vgl. Rempe & Waldecker, 2009, S. 105).

3.3.6.1 Schlüsselmenge der Enigma

Wie bei den schon kennengelernten Verschlüsselungsverfahren braucht man auch für die Enigma einen Schlüssel. Dieser betrifft die Vorkehrungen, die der Anwender der Enigma vor der Ver- bzw. Entschlüsselung an der Maschine durchführen muss.

Der Schlüssel der Enigma besteht aus folgenden Angaben:

- Auswahl und Anordnung der drei Rotationsscheiben (aus den vorhandenen fünf)
- Grundstellung der Scheiben: Auf welchen Positionen befinden sich die Scheiben zu Beginn der Nachricht
- Steckverbindungen: Welche Buchstaben sollen mit den Steckkabeln „vertauscht“ werden

Man kann sich schon vorstellen, dass so sehr viele mögliche Schlüssel zustande kommen. Eine genaue Auflistung folgt in Tabelle 7:

Tabelle 7: Schlüsselmenge der Enigma

	Erklärung	Rechnung	Anzahl der Möglichkeiten
Auswahl der Rotationsscheiben	3 der 5 Rotationsscheiben werden ausgewählt	$\binom{5}{3}$	10
Anordnung der Rotationsscheiben	3 Rotationsscheiben werden in 3 Stellen eingeordnet: Die erste Scheibe hat 3 mögliche Plätze, die zweite noch 2 und für die letzte Scheibe bleibt nur mehr 1 Platz	$3 \cdot 2 \cdot 1$	6
Grundstellung der Scheiben	Jede Scheibe hat 26 mögliche Positionen	$26 \cdot 26 \cdot 26$	17 576
Steckverbindungen	6 Buchstabenpaare werden aus 26 ausgewählt und miteinander „vertauscht“	(*)	100 391 791 500
Gesamt	**Multiplikation aller Einstellungsmöglichkeiten**	**10 · 6 · 17 576 · 100 391 791 500**	**105 869 167 644 240 000**

(*) <u>Wie funktioniert nun die Berechnung der Möglichkeiten der Steckverbindungen?</u>
Wir möchten 6 Buchstabenpaare aus 26 Buchstaben auswählen, die miteinander durch die Kabelverbindungen vertauscht werden. Wir wollen also 12 Buchstaben aus 26 auswählen. Das kann mit $\binom{26}{12}$ = 9 657 700 berechnet werden. Die 12 ausgewählten Buchstaben dürfen in eine beliebige Reihenfolge gebracht werden, d.h. für den ersten Buchstaben gibt es 12 mögliche Positionen, für den zweiten 11, usw., bis für den letzten Buchstaben nur noch ein Platz übrigbleibt. Als Rechnung ergibt das 12 · 11 · … · 1 = 12!
Mit $\binom{26}{12} \cdot 12!$ haben wir nun die Anzahl der Möglichkeiten 12 Buchstaben aus 26 auszuwählen und sie beliebig anzuordnen. Statt $\binom{26}{12} \cdot 12!$ kann auch einfacher $\underbrace{26 \cdot 25 \cdot \ldots \cdot 15}_{12\ Faktoren}$ geschrieben werden. Wenn wir so z.B. die Buchstabenfolge

A – B – C – D – E – F – G – H – I – J – K – L

erhalten, können wir uns vorstellen, dass jeweils 2 Buchstaben der Reihe nach ein Paar bilden, welches durch die Kabel vertauscht wird:

(A – B), (C – D), (E – F), (G – H), (I – J), (K – L). ①

Dann ist aber die Reihe

(B – A), (C – D), (E – F), (G – H), (I – J), (K – L)

für uns gleichbedeutend zu ① - da die Kabel kein erstes und zweites Ende besitzen, sondern diese gleichwertig sind - werden aber in unserer Rechnung als zwei Möglichkeiten gezählt. Da wir jedes der Buchstabenpaare in beliebiger Reihenfolge anführen können, sind insgesamt also $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 26$ der Möglichkeiten redundant.
Da es nicht relevant ist, in welcher Reihenfolge die Kabel angesteckt werden, können wir die Buchstabenpaare in beliebiger Reihenfolge anführen, sodass auch

(C – D), (A – B), (E – F), (G – H), (I – J), (K – L)

mit ① gleichzusetzen ist. D.h. wir haben 6 Paare, die in beliebiger Ordnung aufgezählt werden dürfen: 6 · 5 · 4 · 3 · 2 · 1 = 6!

Von den zu Beginn $\binom{26}{12} \cdot 12!$ Möglichkeiten, werden je $2^6 \cdot 6!$ Möglichkeiten zu einer einzigen zusammengefasst, also erhalten wir:

$$\frac{\binom{26}{12} \cdot 12!}{2^6 \cdot 6!} = 100\,391\,791\,500$$

Wollen wir eine allgemeine Formel für eine beliebige Anzahl von Buchstaben b und eine beliebige Anzahl von Kabelverbindungen k angeben, ergibt sich die Formel:

$$\frac{\binom{b}{2k} \cdot (2k)!}{2^k \cdot k!}$$

3.4 Asymmetrische Verschlüsselung

Bei den im Kapitel 3.3 vorgestellten historischen Verfahren benutzten Sender und Empfänger den gleichen Schlüssel für die Verschlüsselung und Entschlüsselung der Geheimnachrichten. Solche Verfahren nennt man symmetrisch. Seit den 1970er Jahren gibt es auch asymmetrische Verfahren, die Schlüsselpaare aus privaten und öffentlichen Schlüsseln verwenden. Jeder Teilnehmer hat einen geheimen privaten Schlüssel. Dazu gibt es immer einen passenden öffentlichen Schlüssel. Daher wird die Asymmetrische Verschlüsselung auch oft als **Public-Key-Verschlüsselung** (bzw. Public-Key-Chiffrierung) bezeichnet. (Vgl. Spitz, Pramateftakis, & Swoboda, 2011, S. 2)

Alle symmetrischen Verfahren haben ein gemeinsames, großes Problem: Zur geheimen Kommunikation musste vor der sicheren Nachrichtenübertragung ein geheimer Schlüssel ausgetauscht werden. Bei der Skytale ist das zum Beispiel der Durchmesser des Stabes, bei der Caesar-Chiffre der Wert k, um den das Alphabet verschoben wird und bei der Vigenère-Verschlüsselung das Schlüsselwort. Um diesen geheimen Schlüssel miteinander auszutauschen müssen die Kommunikationspartner zuvor schon eine Möglichkeit zur sicheren Übertragung haben. Wenn man sich sowieso öfter trifft, ist das keine so große Schwierigkeit, wenn sich aber zwei Feldherrn über eine große Distanz über ihren nächsten Feldzug unterhalten wollen, sieht das schon anders aus.

Durch die Erfindung der asymmetrischen Verschlüsselung wurde dieses Problem gelöst. Das veränderte die Kryptographie grundlegend, sodass man die klassische Kryptographie, die symmetrische Verfahren verwendet, und die moderne Kryptographie der asymmetrischen Verschlüsselung als zwei verschiedene Welten sehen kann (Vgl. Beutelspacher, Schwenk, & Wolfenstetter, Moderne Verfahren der Kryptographie, 2006, S. V).

3.4.1 Einwegfunktionen und Einwegfunktionen mit einer Hintertür

Für die Asymmetrische Verschlüsselung werden Funktionen mit ihren Umkehrfunktionen genützt.[11] Dabei wird für die Verschlüsselung die Funktion selbst und für die Entschlüsselung

[11] Siehe dazu *Kapitel 3.5.2: „Funktionen: Injektivität, Surjektivität und Bijektivität“* und das *Unterkapitel 3.5.2.1: „Umkehrfunktionen“*

die jeweilige Umkehrfunktion verwendet. Weil die Entschlüsselung aber möglichst schwierig gestaltet werden soll, eignet sich dafür nicht jede Funktion.

> Definition (**Einwegfunktion**): „Als eine Einwegfunktion bezeichnen wir eine Funktion f mit folgenden Eigenschaften:
> (1) Die Funktion f ist effizient […] berechenbar.
> (2) Die Umkehrfunktion f^{-1}, die aus dem Wert $f(x)$ das Argument x berechnet, $f^{-1}\big(f(x)\big) = x$, ist nicht effizient berechenbar.“ (Freiermuth, Hromkovic, Keller, & Steffen, 2010, S. 238)

Für die Zwecke dieser Arbeit reicht es, unter effizient zu verstehen, dass es mit einem Computer leicht ist, etwas zu berechnen. Nicht effizient heißt, dass man auch mit Rechnerunterstützung bei größer werdenden Zahlen, zu lange brauchen würde, um eine Berechnung durchzuführen.[12]

Wenn f die Verschlüsselungsfunktion und f^{-1} die Entschlüsselungsfunktion ist, ist es mit so einer Einwegfunktion also leicht den Klartext x in den Chiffriertext y zu übersetzen. Allerdings ist es praktisch nicht durchführbar den Chiffriertext y wieder in den Klartext zurückzuführen.

Würden man eine Einwegfunktion als Verschlüsselungsfunktion verwenden, wäre es für den Empfänger im Allgemeinen nicht möglich, den Chiffriertext wieder auf den Klartext zu entschlüsseln und die Verschlüsselung somit unbrauchbar. Also benötigt man eine weitere Eigenschaft für die Einwegfunktion:

> Definition (**Einwegfunktion mit einer Hintertür**): „Als eine Einwegfunktion mit einer Hintertür bezeichnen wir eine Funktion f mit folgenden Eigenschaften:
> (1) Die Funktion f ist effizient […] berechenbar.
> (2) Die Umkehrfunktion f^{-1}, die aus dem Wert $f(x)$ das Argument x berechnet, $f^{-1}\big(f(x)\big) = x$, ist nicht effizient berechenbar.
> (3) Es existiert ein Geheimnis (genannt Hintertür) von f, so dass mit Hilfe dieses Geheimnisses das x aus dem $f(x)$ schnell bestimmt werden kann.“ (Freiermuth, Hromkovic, Keller, & Steffen, 2010, S. 239)

3.4.2 Das Konzept der Public-Key-Kryptographie

Mit den besprochenen Einwegfunktionen mit einer Hintertür, kann nun das Konzept von Public-Key-Verschlüsselungen beschrieben werden.

Der Empfänger, Bob, besitzt das Geheimnis der Einwegfunktion f mit einer Hintertür. Dieses Geheimnis nennt man den privaten Schlüssel von Bob. Er kann die Funktion f an Alice und alle anderen weitergeben, die ihm eine Nachricht senden wollen. Er kann sie sogar z.B. im Internet veröffentlichen. So kann Alice dann ihre Nachricht mit der Funktion f verschlüsseln und nur Bob kann sie mithilfe des Geheimnisses entschlüsseln. Die Verschlüsselungsfunktion f wird dann öffentlicher Schlüssel von Bob genannt.

[12] Genauer ist die Zeitkomplexität von Algorithmen z.B. in (Freiermuth, Hromkovic, Keller, & Steffen, 2010) beschrieben

Jede Person, die in einem Netzwerk, das mit Public-Key-Verschlüsselungen arbeitet, kommunizieren möchte, benötigt also einen eigenen öffentlichen Schlüssel und den dazugehörigen privaten Schlüssel, der geheim bleiben muss.

Befinden sich n Personen in so einem Netzwerk, werden n Schlüsselpaare benötigt. Vergleicht man das mit einem Netzwerk von n Personen mit symmetrischer Verschlüsselung, bemerkt man eine deutliche Verbesserung. Bei symmetrischer Verschlüsselung benötigen je 2 Personen einen gemeinsamen, geheimen Schlüssel. Anders gesagt benötigt jede Person $n - 1$ Schlüssel (einen, für jede andere Person). Mit dem Term $n \cdot (n-1)$ würde man jeden Schlüssel im Netzwerk doppelt zählen, also ergibt sich $\frac{n \cdot (n-1)}{2}$ für die Anzahl der benötigten Schlüssel. (Vgl. Freiermuth, Hromkovic, Keller, & Steffen, 2010, S. 240f)

Für ein Netzwerk mit 100 Personen, benötigt man mit asymmetrischer Verschlüsselung 100 Schlüsselpaare, mit einer symmetrischen hingegen 4950 Schlüssel.

3.4.3 RSA

Zahlentheoretische Problemstellungen, im Speziellen das Problem der Faktorisierung, liefern die einzigen heute in der Realität verwendeten Public-Key-Verschlüsselungen. Das Problem besteht darin, dass zu einer gegebenen natürlichen Zahl die Primfaktoren nicht effizient berechnet werden können. Genauer gesagt, nimmt man an, dass für Dezimalzahlen mit mehr als 500 Stellen in realistischer Zeit keine Primfaktorzerlegung durchgeführt werden kann.

Dieses Problem haben sich die Kryptographen zunutze gemacht. Wenn zwei Primzahlen q und p gegeben sind, kann die Funktion $f(p,q) = p \cdot q$ effizient berechnet werden. Die Umkehrfunktion $f^{-1}(n)$, die für $n = p \cdot q$ die beiden Faktoren p und q berechnen soll, stößt aber nun auf das Problem der Faktorisierung.

Da es kein Geheimnis gibt, mit dem die Primfaktorzerlegung leichter lösbar wäre, kann sie nicht direkt für die Verschlüsselung verwendet werden, sie ist aber trotzdem die zentrale Idee für sichere asymmetrische Verschlüsselungen. (Vgl. Freiermuth, Hromkovic, Keller, & Steffen, 2010, S. 289f)

Die Sicherheit dieses Verfahrens hängt also eng mit der Schwierigkeit, große Zahlen in Primfaktoren zu zerlegen, zusammen. Der Name RSA leitet sich von den Anfangsbuchstaben seiner drei Erfinder Ron **R**ivest, Adi **S**hamir und Len **A**dleman ab. (Vgl. Buchmann, 2008, S. 137)

3.4.3.1 Schlüsselerzeugung

Bob wählt zwei große Primzahlen p und q zufällig aus. Er bildet das Produkt

$$n = p \cdot q.$$

Dann berechnet er auch die Euler'sche Phi-Funktion[13]

$$\phi(n) = \phi(pq) = (p-1)(q-1).$$

Er sucht dann zwei Zahlen e und d, für die gilt

$$e \cdot d \; mod \; \phi(n) = 1.$$

[13] Dazu brauchen wir die mathematischen Grundlagen des *Kapitels 3.5.5: „Ein Satz von Euler".*

Dazu wählt er e als eine teilerfremde Zahl zu $\phi(n)$ und berechnet dann d, wozu er den erweiterten Euklidischen Algorithmus[14] verwendet. Er wendet ihn auf $\phi(n)$ und e an, und erhält d und k, für die gilt:

$$e \cdot d + k \cdot \phi(n) \underbrace{= 1}_{ggT(e,\phi(n))} \Leftrightarrow e \cdot d \; mod \; \phi(n) = 1$$

Bobs öffentlicher Schlüssel besteht nun aus dem Zahlenpaar n und e. Sein privater Schlüssel ist die Zahl d.

Die Zahlen p, q und $\phi(n)$, die er für die Schlüsselerzeugung verwendet hat, müssen auch geheim bleiben. Er wird sie aber zur Entschlüsselung nicht mehr brauchen, also kann Bob sie vergessen. (Vgl. Beutelspacher, Kryptologie: Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen, 2007, S. 108f)

3.4.3.2 Anwendung des RSA-Algorithmus

Wenn Alice eine Nachricht an Bob senden möchte, braucht sie zuerst wieder seinen öffentlichen Schlüssel, der aus den Zahlen n und e besteht.

Technische Gegebenheiten verlangen, dass der Text zur Verschlüsselung in binärer Codierung gegeben ist. Die Übersetzung der Schriftzeichen in binäre Codes wird mit internationalen Standards, wie der ASCII-Tabelle, festgelegt. Die binäre Darstellung wird dann in Blöcke zerlegt, auf die einzeln und unabhängig voneinander der Algorithmus angewendet wird. Dabei werden die binären Darstellungen der Blöcke als Zahlen im Dualsystem interpretiert und in das Dezimalsystem umgewandelt. Insgesamt wird also aus einem Text, der aus beliebigen Schriftzeichen bestehen kann, eine Zahl. In dieser Arbeit werden diese technischen Übersetzungen nicht genauer behandelt und als gegeben betrachtet. Wichtig ist, dass der Klartext danach aus einer natürlichen Zahl $m < n$ besteht.

Alice berechnet den Chiffriertext dann mit der Formel

$$c = m^e \; mod \; n.$$

Diesen Geheimtext c versendet Alice dann an Bob.

Bob berechnet den Klartext m_1 aus c und mithilfe seines geheimen Schlüssels:

$$m_1 = c^d \; mod \; n.$$

Damit die RSA-Verschlüsselung funktioniert, sollte dann $m_1 = m$ gelten, was nun überprüft werden soll. (Vgl. Beutelspacher, Kryptologie: Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen, 2007, S. 109ff)

3.4.3.3 Korrektheit des RSA-Algorithmus

Zur Kontrolle der Korrektheit des RSA-Algorithmus möchte man überprüfen, ob nach der Anwendung des RSA-Algorithmus für die natürlichen Zahlen m und m_1 wirklich die Gleichheit folgt.

[14] Siehe *Kapitel 3.5.1.3: „Euklidischer Algorithmus und Erweiterter Euklidischer Algorithmus“.*

Beweis:

Aus den Formeln für die Berechnung von m_1 und m und den Rechenregeln des Potenzierens und modularen Rechnens[15] folgt direkt

$$m_1 = c^d \; mod \; n$$
$$= (m^e)^d \; mod \; n$$
$$= m^{e \cdot d} \; mod \; n$$

Um zu zeigen, dass der Algorithmus korrekt arbeitet, muss also $m = m^{e \cdot d} \; mod \; n$ gelten.

Bob hat e und d so gewählt, dass $e \cdot d = 1 + k \cdot \phi(n)$ gilt. Das können wir in den Term einsetzen und erhalten

$$m^{e \cdot d} \; mod \; n = m^{1 + k \cdot \phi(n)} \; mod \; n.$$

Wegen der Eigenschaft der Euler'schen ϕ-Funktion (P1)[16] gilt $\phi(n) = \phi(pq) = (p-1)(q-1)$, daraus folgt

$$m^{1 + k \cdot \phi(n)} \; mod \; n = m^{1 + k \cdot (p-1) \cdot (q-1)} \; mod \; pq$$
$$=^{Hilfssatz[17]} \; m.$$

Somit ist die Nachricht m_1 nach der Dechiffrierung wieder dieselbe, wie die ursprüngliche Klartextnachricht m, vor der Verschlüsselung. (Vgl. Beutelspacher, Kryptologie: Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen, 2007, S. 111)

□

[15] Siehe *Kapitel 3.5.4: „Modulares Rechnen".*
[16] (P1) ist formuliert und bewiesen in *Kapitel 3.5.5: "Ein Satz von Euler".*
[17] Die Formulierung und der Beweis des Hilfssatzes finden sich in *Kapitel 3.5.5: „Ein Satz von Euler".*

3.5 Mathematische Grundlagen

An diesem Punkt sollen mathematische Grundlagen besprochen werden, die in Kapitel 4 benötigt werden. In Kapitel 4 selbst wird dann auf das jeweilige Kapitel der benötigten mathematischen Grundlagen verwiesen.

3.5.1 Ganze Zahlen

In diesem Kapitel werden Teilbarkeiten, der größte gemeinsame Teiler, der Euklidische Algorithmus und der erweiterte Euklidische Algorithmus behandelt.

3.5.1.1 Teilbarkeit, Division mit Rest

Definition (**Teilbarkeit**): „Eine ganze Zahl $a \neq 0$ ist ein Teiler von $b \in \mathbb{Z}$ (und b ein Vielfaches von a), falls es ein $q \in \mathbb{Z}$ mit $b = qa$ gibt. Dann sagt man auch, dass b durch a teilbar ist und bezeichnet dies mit $a|b$." (Jukna, 2008, S. 68)

Es gilt also z.B. $16|368$ („16 teilt 368"), weil es eine ganze Zahl (23) gibt, für die gilt: $368 = 23 \cdot 16$.

16 teilt aber nicht 369 (man schreibt $16 \nmid 369$), weil $369 : 16 = 23{,}0625$ (oder $369 : 16 = 23$ mit Rest 1) und es daher keine Zahl $q \in \mathbb{Z}$ gibt, sodass $369 = q \cdot 16$.

Teilbarkeitsregeln: $\forall a, b, c \in \mathbb{Z}$ gilt:
T1: $a \mid b$ und $b \mid c \Rightarrow a \mid c$
T2: $a \mid b \Rightarrow ax \mid bx \;\; \forall x \in \mathbb{Z}$
T3: $c \mid a$ und $c \mid b \Rightarrow c \mid (xa + yb) \;\; \forall x, y \in \mathbb{Z}$
T4: $a \mid b$ und $b \neq 0 \Rightarrow |a| \leq |b|$
T5: $a \mid b$ und $b \mid a \Rightarrow |a| = |b|$

Beweis:

(T1) Wegen $a \mid b$ und $b \mid c$ gibt es $d, e \in \mathbb{Z}$, sodass $b = da$ und $c = eb$.
Dann gilt $c = eb = e(da) = (ed)a$. Da $ed \in \mathbb{Z} \Rightarrow a \mid c$.

(T2) Wegen $a \mid b$ gibt es ein $d \in \mathbb{Z}$, sodass $b = da$.
Dann gilt $bx = (da)x = d(ax)$. Da $d \in \mathbb{Z} \Rightarrow ax \mid bx$.

(T3) Wegen $c \mid a$ und $c \mid b$ gibt es $d, e \in \mathbb{Z}$, sodass $a = dc$ und $b = ec$.
Dann gilt $xa + yb = x(dc) + y(ec) = (xd)c + (ye)c = (xd + ye)c$. Da $(xd + ye) \in \mathbb{Z} \Rightarrow c \mid (xa + yb)$

(T4) Wegen $a \mid b$ und $b \neq 0$ gibt es ein $d \in \mathbb{Z}$ mit $d \neq 0$, sodass $b = da$.
Dann gilt $|b| = |da| \geq |a|$.

(T5) Wenn $a = 0$, dann folgt $b = 0$ und umgekehrt.
Wenn $a \neq 0$, dann folgt aus (T4), dass $|a| \leq |b|$ und $|b| \leq |a|$ ist. Dann gilt $|a| = |b|$.

□

Satz (Division mit Rest): „Seien a, b ganze Zahlen mit $b \neq 0$. Dann gibt es ganze Zahlen q und r, so dass $a = qb + r$ und $0 \leq r < |b|$ gilt. Hierbei sind q und r eindeutig bestimmt. Die (eindeutig bestimmte) Zahl r nennt man Rest von a modulo b und bezeichnet sie mit $r = a \; mod \; b$." (Jukna, 2008, S. 68f)

Beweis (aus (Jukna, 2008, S. 69))**:**

Sei S die Menge aller natürlichen Zahlen der Form $a - xb$ mit $x \in \mathbb{Z}$. Da $b \neq 0$ gilt, ist diese Menge nicht leer und muss daher das kleinste Element $r = a - qb \geq 0$ enthalten. Dann gilt aber auch $a = qb + r$. Um $r < |b|$ zu zeigen, sei $r \geq |b|$. Wegen $0 \leq r - |b| < r$ gehört dann aber die Zahl $r - |b| = (a - qb) - |b| = a - (q \pm 1)b$, die kleiner als r ist, auch zu der Menge S, ein Widerspruch.

Um die Eindeutigkeit zu zeigen, sei $a = qb + r$ und $a = q'b + r'$ mit $0 \leq r, r' < |b|$. Dann ist die Zahl $r - r' = b(q' - q)$ ein Vielfaches von b. Wegen $|r - r'| < |b|$ kann dies nur dann der Fall sein, wenn $r = r'$ und damit auch $q = q'$ gilt.

□

Wir können z.B. die Rechnung

$$369 : 16 = 23 \text{ mit Rest } 1$$

wie im Lemma aufschreiben als

$$369 = 23 \cdot 16 + 1.$$

Somit wissen wir, dass

$$369 \; mod \; 16 = 1.$$

In diesem Beispiel würden wir die Zahl 23 als $369 \; div \; 16$ bezeichnen. D.h. wir können aufschreiben:

$$369 = \underbrace{(369 \; div \; 16)}_{23} \cdot 16 + \underbrace{269 \; mod \; 16}_{1}$$

Der Rest der ganzzahligen Division muss immer nicht-negativ sein. Z.B. ergibt $9 \; mod \; 4 = 1$ (weil $9 = 2 \cdot 4 + 1$), aber $-9 \; mod \; 4 = 3$ (weil $-9 = (-3) \cdot 4 + 3$). (Vgl. Jukna, 2008, S. 69)

3.5.1.2 Größter gemeinsamer Teiler

Zuerst wird die Definition eines gemeinsamen Teilers zweier ganzer Zahlen a und b benötigt.

Definition (**Gemeinsamer Teiler**): „Ein gemeinsamer Teiler von a und b ist eine ganze Zahl c, die sowohl a als auch b teilt." (Buchmann, 2008, S. 9)

Satz: „Unter allen gemeinsamen Teilern zweier ganzer Zahlen a und b, die nicht beide gleich 0 sind, gibt es genau einen (bezüglich $\leq$) größten. Dieser heißt größter gemeinsamer Teiler (ggT) von a und b“. (Buchmann, 2008, S. 9)

Beweis:

Sei $a \neq 0$. Nach der Teilbarkeitsregel (T4) gilt für alle Teiler von a, dass sie $\leq |a|$ und somit beschränkt sind. D.h. es muss einen größten Teiler von a geben. Daraus folgt, dass es auch einen größten gemeinsamen Teiler von a und b geben muss.

□

Der größte gemeinsame Teiler von a und b wird als $ggT(a,b)$ aufgeschrieben. Wenn $ggT(a,b) = 1$, dann heißen a und b teilerfremd. (Vgl. Beutelspacher, Schwenk, & Wolfenstetter, Moderne Verfahren der Kryptographie, 2006, S. 110)

Beispiele:

$ggT(27{,}15) = 3$
$ggT(a,0) = a, \quad \forall a \in \mathbb{Z}\backslash\{0\}$
$ggT(9{,}20) = 1$, d.h. 9 und 20 sind teilerfremd.

3.5.1.3 Euklidischer Algorithmus und Erweiterter Euklidischer Algorithmus

Da es bei größeren Zahlen schnell zeitaufwendig wird, den ggT durch Ausprobieren bzw. Primfaktorzerlegung zu finden, verwendet man zum Berechnen des ggT meist den euklidischen Algorithmus.

Der euklidische Algorithmus verwendet den bereits beschriebenen und bewiesenen Satz von der Division mit Rest[18]. Und zwar wird die Division mit Rest immer wieder hintereinander ausgeführt.

$$a = q \cdot b + r, \text{mit } 0 \leq r < b$$

Dann gilt $ggT(a,b) = ggT(b,r)$. Die Berechnung wird so oft wiederholt, bis sich $r = 0$ ergibt.

Beweis (Euklidischer Algorithmus):

Wir nehmen an, dass $b > 0$ und setzen $a \coloneqq x_0$ und $b \coloneqq x_1$, dann können wir die Rechenschritte des Euklidischen Algorithmus folgendermaßen beschreiben:

$$\begin{aligned}
&x_0 = q_1 \cdot x_1 + x_2, \text{ mit } 0 < x_2 < x_1 \\
&x_1 = q_2 \cdot x_2 + x_3, \text{ mit } 0 < x_3 < x_2 \\
&x_2 = q_3 \cdot x_3 + x_4, \text{ mit } 0 < x_4 < x_3 \\
(1) \quad &\vdots \\
&x_{n-3} = q_{n-2} \cdot x_{n-2} + x_{n-1}, \text{ mit } 0 < x_{n-1} < x_{n-2} \\
&x_{n-2} = q_{n-1} \cdot x_{n-1} + x_n, \text{ mit } 0 < x_n < x_{n-1} \\
&x_{n-1} = q_n \cdot x_n + 0
\end{aligned}$$

[18] Der Beweis ist in *Kapitel 3.5.1.1: „Teilbarkeit, Division mit Rest“* angeführt.

Da $x_1 > x_2 > x_3 > x_4$ … streng monoton abnimmt, erreicht man nach endlichen vielen Schritten den Rest 0.

Jetzt wollen wir beweisen, dass der letzte Rest > 0, also x_n, der größte gemeinsame Teiler von x_1 und x_2 ist.

Schritt 1: x_n teilt x_0 und x_1. Aus der letzten Gleichung von ① folgt x_n teilt x_{n-1}. Aus der vorletzten Gleichung folgt, dass x_{n-1} ein Teiler von x_{n-2} ist, also teilt x_n nach der Teilbarkeitsregel (T1) auch x_{n-2}. Dieses Prinzip lässt sich fortführen bis $x_n \mid x_1$ und $x_n \mid x_0$.

Schritt 2: Für jede Zahl x'_n, die x_0 und x_1 teilt, gilt $x'_n \leq x_n$. Aus $x'_n \mid x_0$ und $x'_n \mid x_1$, der ersten Gleichung aus ① und (T3) folgt $x'_n \mid x_2$. Dann folgt aus der zweiten Gleichung $x'_n \mid x_3$. Das kann fortgeführt werden, bis $x'_n \mid x_n$. Aus (T5) folgt, dass $|x'_n| \leq |x_n|$ und weil $x_n > 0$ gilt $x'_n \leq x_n$.

□

Ein Beispiel:

$ggT(1156, 953) =$

$1156 = 1 \cdot 953 + 203$ $\quad ggT(1156{,}953) = ggT(953{,}203)$
$953 = 4 \cdot 203 + 141$ $\quad ggT(953{,}203) = ggT(203{,}141)$
$203 = 1 \cdot 141 + 62$ $\quad ggT(203{,}141) = ggT(141{,}62)$
$141 = 2 \cdot 62 + 17$ …
$62 = 3 \cdot 17 + 11$
$17 = 1 \cdot 11 + 6$
$11 = 1 \cdot 6 + 5$
$6 = 1 \cdot 5 + [1]$
$5 = 5 \cdot 1 + 0$

$ggT(1156{,}953) = ggT(1{,}0) = [1]$

Lemma von Bézout: „Zu $a_0, a_1 \in \mathbb{N}$ existieren ganze Zahlen u und v mit $ggT(a_0, a_1) = u \cdot a_0 + v \cdot a_1$." (Beutelspacher, Neumann, & Schwarzpaul, Kryptografie in Theorie und Praxis: Mathematische Grundlagen für Internetsicherheit, Mobilfunk und elektronisches Geld, 2010, S. 121)

Das Lemma folgt direkt aus dem Euklidischen Algorithmus, da der Algorithmus im Prinzip nur umgekehrt wird. Die Darstellung wird oft auch **Vielfachsummendarstellung** genannt. (Vgl. Beutelspacher, Neumann, & Schwarzpaul, Kryptografie in Theorie und Praxis: Mathematische Grundlagen für Internetsicherheit, Mobilfunk und elektronisches Geld, 2010, S. 121)

Ein Beispiel:

$ggT(24{,}14) =$

$24 = 1 \cdot 14 + 10$ $\quad \mathbf{2} = 10 - 2 \cdot 4$
$14 = 1 \cdot 10 + 4$ $\quad = 10 - 2 \cdot (14 - 10)$
$10 = 2 \cdot 4 + 2$ $\quad = 3 \cdot 10 - 2 \cdot 14$
$4 = 2 \cdot 2 + 0$ $\quad = 3 \cdot (24 - 14) - 2 \cdot 14$
$\Rightarrow \boldsymbol{ggT(24, 14) = 2}$ $\quad = \mathbf{3 \cdot 24 - 5 \cdot 14}$

Wir haben also jetzt zuerst den Euklidischen Algorithmus zur Berechnung des größten gemeinsamen Teilers verwendet und die Gleichungen dann von unten nach oben wieder aufgelöst.

Der Algorithmus, der im Beispiel zur Erstellung der Vielfachsummendarstellung verwendet wurde, wird **erweiterter Euklidischer Algorithmus** genannt. (Vgl. Beutelspacher, Kryptologie: Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen, 2007, S. 106f)

3.5.2 Funktionen: Injektivität, Surjektivität und Bijektivität

In diesem Kapitel bestimmte Eigenschaften von Funktionen, nämlich Injektivität, Surjektivität und Bijektivität, besprochen werden. Dazu zuerst eine kurze Wiederholung der Definition und einer Darstellungsmöglichkeit von Funktionen.

3.5.2.1 Funktionen

Definition (**Funktion**): „Seien A und B Mengen.

(i) Unter einer Funktion oder Abbildung f von A nach B verstehen wir eine Vorschrift, die jedem $a \in A$ genau ein $b \in B$ zuordnet.

(ii) Das dem Element a zugeordnete Element b bezeichnen wir $f(a)$ und nennen es den Wert der Funktion f an der Stelle a oder das Bild von a unter f; a wird das Urbild von b unter f bezeichnet.

(iii) Weiters wird A als Definitionsmenge oder -bereich von f bezeichnet und B als Zielmenge oder -bereich von f." (Schichl & Steinbauer, 2012, S. 158)

Ein Beispiel für eine Funktion:

$$f: \mathbb{R} \to \mathbb{R}, f(x) = x^2$$

$\mathbb{R}$ ist Definitions- und Zielmenge der Funktion f und jede Zahl x $\in \mathbb{R}$ wird auf den Funktionswert $x^2 \in \mathbb{R}$ abgebildet.

Eine Möglichkeit die Funktion darzustellen ist in Abbildung 5 gezeigt. Das ist nur ein kleiner Ausschnitt der Elemente der Menge A (= $\mathbb{R}$), die den Elementen der Menge B (= $\mathbb{R}$) durch die Funktion f, die hier durch die Pfeile dargestellt wird, zugewiesen werden.

Es fällt auf, dass von jedem $x \in A$ genau ein Pfeil weggeht, weil jedem $a \in A$ nach Definition genau ein $b \in B$ zugeordnet werden muss.

Die Elemente der Menge B dürfen jedoch sehr wohl von mehreren Pfeilen (z.B.: $2^2 = 4$ und $(-2)^2 = 4$), oder von gar keinem Pfeil ($\nexists x \in \mathbb{R}: x^2 = -3$) getroffen werden. (Vgl. Schichl & Steinbauer, 2012, S. 159)

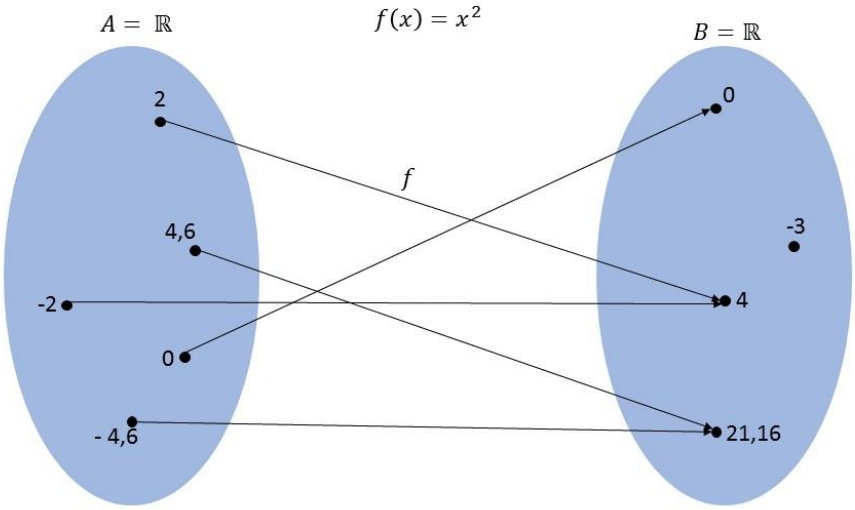


Abbildung 5: Pfeildiagramm einer Funktion

3.5.2.2 Injektivität

Es gibt aber Funktionen, bei denen auch ein Element der Menge B nie öfter als einmal von einem Pfeil getroffen wird. So eine Funktion heißt dann injektiv.

> Definition (**Injektivität**): „Sei $f: A \rightarrow B$ eine Abbildung.
>
> (i) Wir sagen f ist injektiv, wenn jedes Element $b \in B$ von f höchstens einmal getroffen wird, d.h. höchstens ein Urbild hat. Anders ausgedrückt verlangen wir, dass verschiedene Urbilder auch verschiedene Bilder haben. In Symbolen können wir schreiben
>
> $x \neq y \in A \Rightarrow f(x) \neq f(y)$ oder $f(x) = f(y) \Rightarrow x = y$“
>
> (Schichl & Steinbauer, 2012, S. 165)

Damit eine Funktion injektiv ist, dürfen also nicht zwei Elemente existieren, die beide auf denselben Funktionswert abgebildet werden. Wir sehen sofort, dass unsere Funktion von vorhin: $f: \mathbb{R} \rightarrow \mathbb{R}, f(x) = x^2$ nicht injektiv ist, da $f(2) = 4$ und $f(-2) = 4$.

Eine praktische Eigenschaft injektiver Funktionen ist, dass man, wenn man den Funktionswert $f(x)$ kennt, immer eindeutig auf das Argument x schließen kann. Wenn für die Funktion $i: \mathbb{Z} \rightarrow \mathbb{Z}, i(x) = 4x - 2$ bekannt ist, dass $i(x) = 10$ der Funktionswert ist, dann kann auch das Argument x eindeutig ausgerechnet werden:

$$4x - 2 = 10 \quad | + 2$$

$$4x = 12 \quad | : 4$$

$$x = 3$$

(Vgl. Freiermuth, Hromkovic, Keller, & Steffen, 2010, S. 9)

Das „Zurückrechnen“ vom Funktionswert auf das Argument x kann man sich vorstellen, wie wenn man die Pfeile des Pfeildiagramms vom gewünschten Element der Menge B rückwärts zum Ausgangspunkt in Menge A verfolgt. Manche Elemente kann man jedoch nicht

zurückverfolgen (weil sie von keinem Pfeil getroffen werden), wie man in Abbildung 6 sieht. (Achtung: Menge $\mathbb{Z}$!)

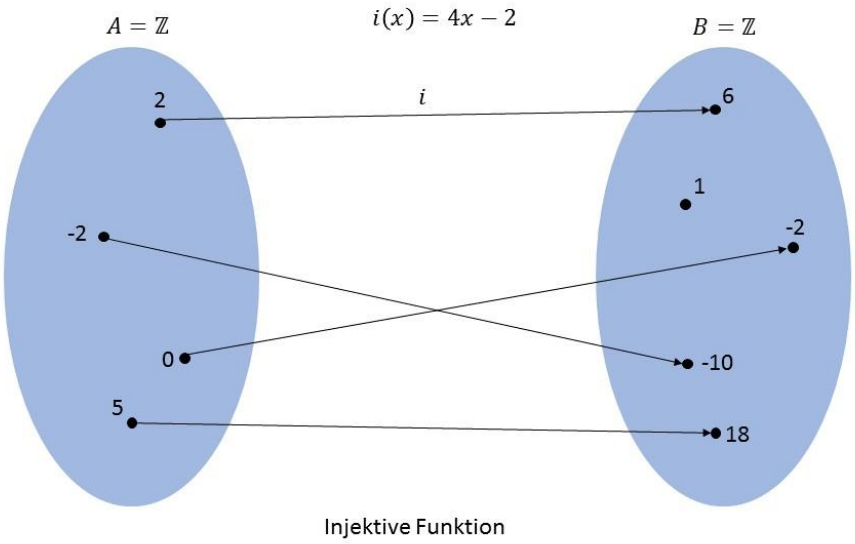


Abbildung 6: Pfeildiagramm einer injektiven Funktion

3.5.2.3 Surjektivität

Wenn Funktionen benötigt werden, bei denen alle Elemente der Zielmenge getroffen werden, braucht man eine surjektive Funktion.

> Definition (**Surjektivität**): „Sei $f: A \rightarrow B$ eine Abbildung. […]
> (ii) f heißt surjektiv, wenn jedes Element $b \in B$ von f getroffen wird, also mindestens ein Urbild besitzt. In Symbolen:
> $$\forall b \in B: \exists a \in A: f(a) = b."$$
> (Schichl & Steinbauer, 2012, S. 165)

Nimmt man aber $h: \mathbb{R} \rightarrow \mathbb{R}, h(x) = x^3 - 3x$ an, sieht man, dass alle Elemente der Zielmenge auch wirklich von mindestens einem Element der Definitionsmenge getroffen werden. Da aber z.B. $h(-1) = h(2) = 2$ ist die Funktion h nicht injektiv. Das Pfeildiagramm der surjektiven Funktion h ist in Abbildung 7 gezeigt.

> Wir haben bereits gemerkt, dass $f: \mathbb{R} \rightarrow \mathbb{R}, f(x) = x^2$ nicht surjektiv ist, da z.B. $f(x) = -3$ keine Lösung in $\mathbb{R}$ hat.[19] Auch $i: \mathbb{Z} \rightarrow \mathbb{Z}, i(x) = 4x - 2$ ist nicht surjektiv, weil $i(x) = 1$ keine Lösung in $\mathbb{Z}$ besitzt. (es wäre $x = \frac{3}{4}$) .

[19] $x^2 = -3 \mid \sqrt{\ }$
$x = \sqrt{-3} \Rightarrow$ Wurzel aus negativer Zahl

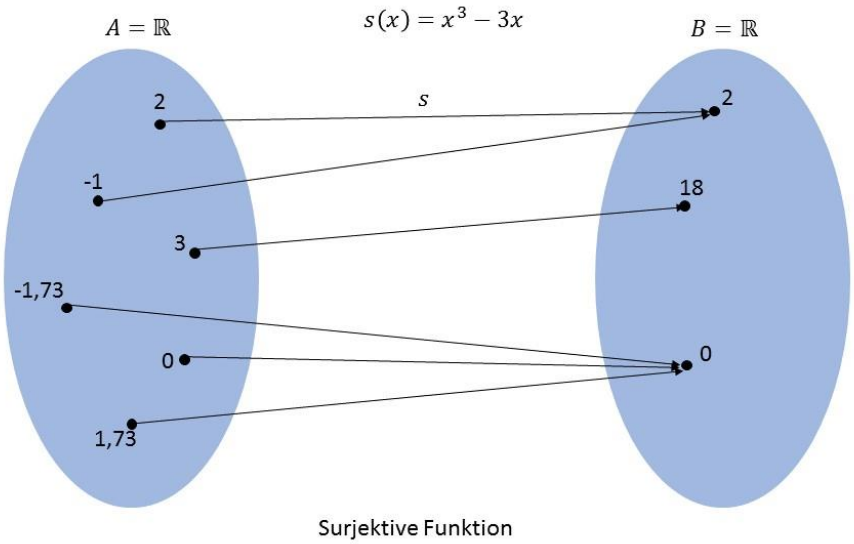


Abbildung 7: Pfeildiagramm einer surjektiven Funktion

3.5.2.4 Bijektivität

Für eine Funktion, die sowohl injektiv, als auch surjektiv ist, gibt es auch eine Bezeichnung:

> Definition (**Bijektivität**): „Sei f: A → B eine Abbildung. […]
> (iii) Wir nennen f bijektiv, wenn f injektiv und surjektiv ist. Das ist der Fall, wenn jedes Element in der Zielmenge B genau ein Urbild besitzt."
> (Schichl & Steinbauer, 2012, S. 165)

In den schon bekannten Pfeildiagrammen heißt das also, das jedes Element in der Zielmenge B von genau einem Pfeil getroffen wird.

Ein Beispiel für eine bijektive Funktion ist $b: \mathbb{R} \to \mathbb{R}, b(x) = x$, die jedes Element $x \in \mathbb{R}$ auf sich selbst abbildet. Das passende Pfeildiagramm ist in Abbildung 8 zu sehen.

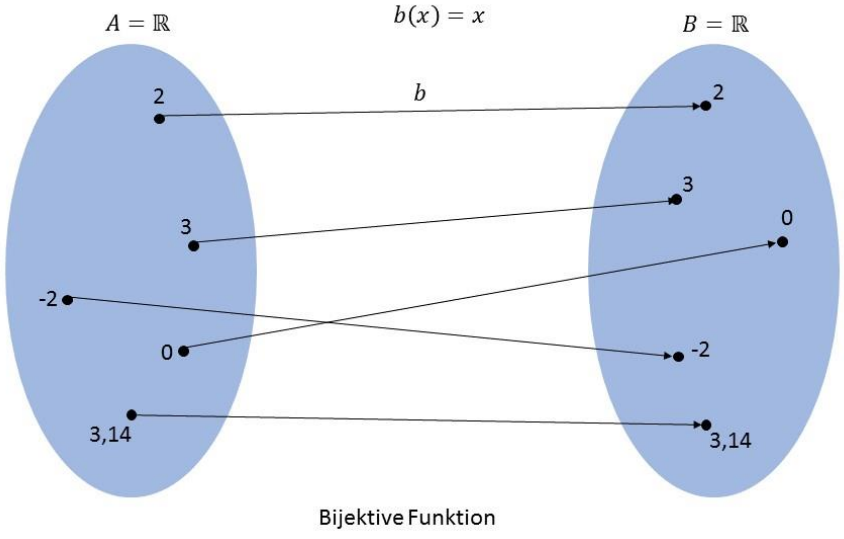
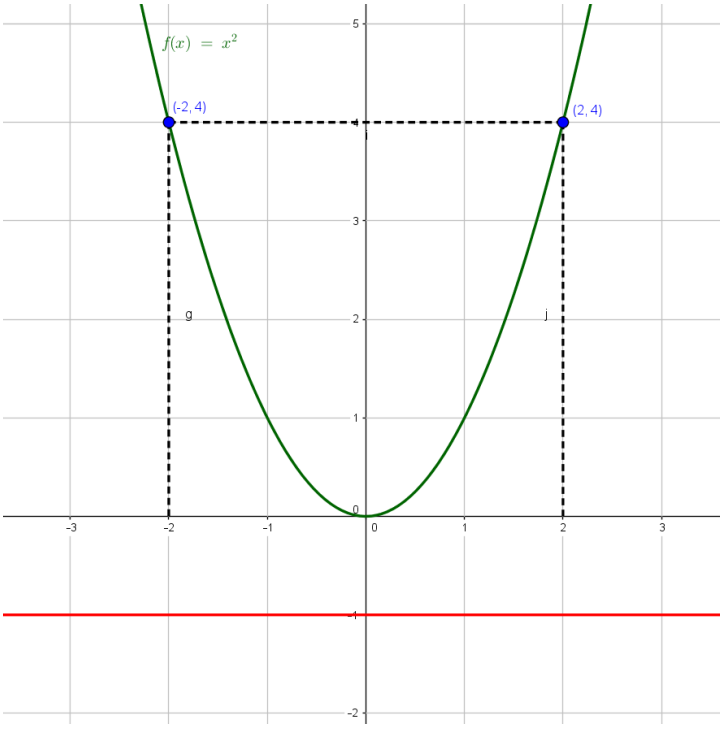


Abbildung 8: Pfeildiagramm einer bijektiven Funktion

Die Pfeildiagramme der Funktionen eignen sich einerseits gut, um sich vorstellen zu können, was die Eigenschaften Injektivität, Surjektivität und Bijektivität bedeuten („Gibt es einen Pfeil der auf dieses Element zeigt?“, „Wohin zeigt der Pfeil jenes Elements?“, usw.), allerdings wird so immer nur ein kleiner Teil der Definitions- und Zielmengen dargestellt.

Eine andere Darstellungsart für Funktionen, bei der auch der Verlauf der Funktion sichtbar gemacht wird, ist der bereits aus dem Mathematikunterricht bekannte Funktionsgraph. Auch anhand des Graphen kann gut abgelesen werden, ob die Funktionen injektiv, surjektiv oder bijektiv sind. Dazu nochmals die Beispiele:

- $f: \mathbb{R} \to \mathbb{R}, f(x) = x^2$

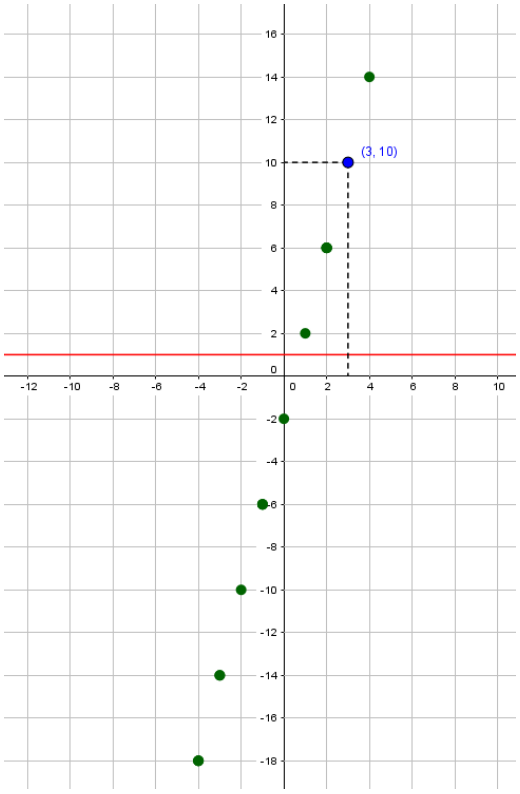


Wenn durch $y = 4$ eine zur x-Achse parallele Gerade gezeichnet wird, schneidet diese öfter als 1x den Graphen (nämlich in diesem Fall bei $x = -2$ und $x = 2$), d.h. die Funktion ist nicht injektiv, da mehrere Argumente, denselben Funktionswert besitzen.

Da bei $y = -1$ eine zu x parallele Gerade gezeichnet wurde, die den Graphen nie schneidet, ist die Funktion auch nicht surjektiv, da es kein Argument gibt, das diesen Funktionswert ergibt.

So können alle Graphen auf diese Eigenschaften geprüft werden.

- $i: \mathbb{Z} \to \mathbb{Z}, i(x) = 4x - 2$

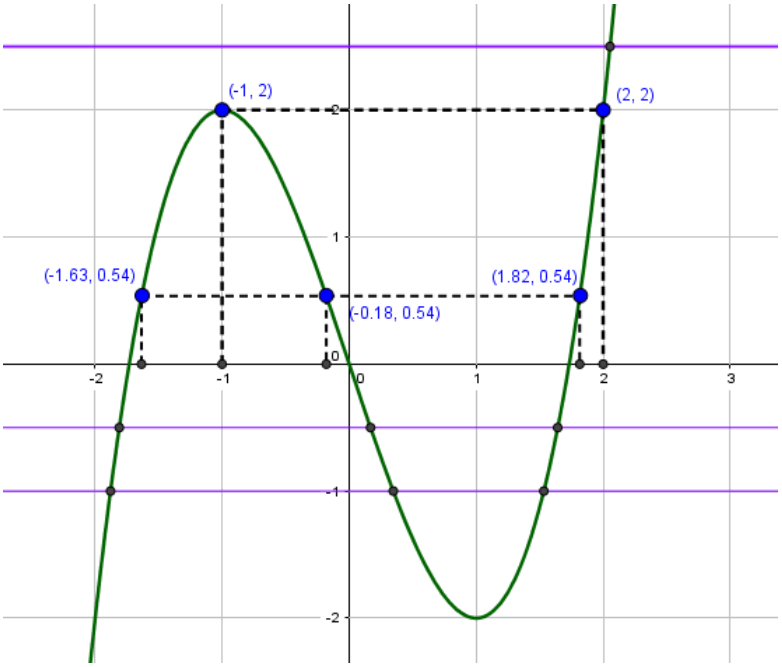


Der Graph besteht in diesem Fall aus einer Mengen von Punkten, da es sich um eine Abbildung von $\mathbb{Z}$ nach $\mathbb{Z}$ handelt.

Die Funktion ist injektiv, weil jeder x-Wert mit einem unterschiedlichem y-Wert gepaart ist. Wenn also durch jeden y-Wert $\in \mathbb{Z}$ eine zur x-Achse parallele Gerade gelegt wird, schneidet man den Funktionsgraphen nie zweimal oder öfter.

Da aber sehr wohl $y \in \mathbb{Z}$ existieren, die den Graphen der Funktion gar nicht schneiden, ist die Funktion i nicht surjektiv, und somit auch nicht bijektiv.

- $h: \mathbb{R} \to \mathbb{R}, h(x) = x^3 - 3x$



Die Funktion h ist surjektiv, weil jede zur x-Achse parallele Gerade mindestens einen Schnittpunkt mit dem Funktionsgraphen hat.

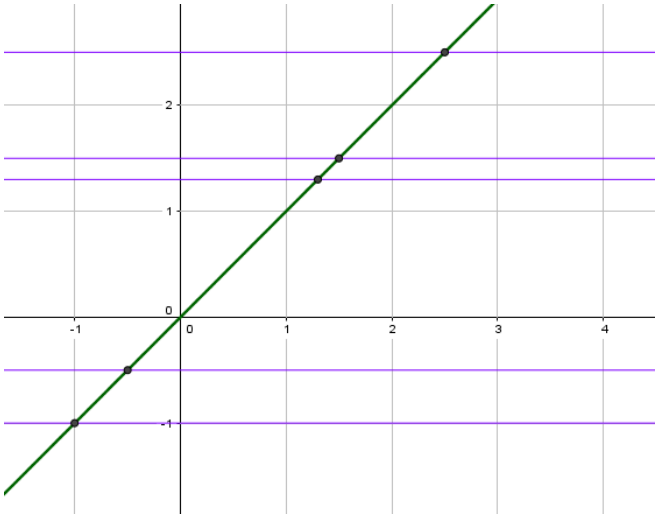
Die Funktion ist nicht injektiv, weil mehrere dieser Geraden den Funktionsgraphen zwei Mal oder sogar drei Mal schneiden. In der Abbildung ist z.B. eingezeichnet, dass $h(-1) = h(2) = 2$ und $h(-1{,}63) = h(-0{,}18) = h(1{,}82) = 0{,}54$.

Daher kann auch keine Bijektivität vorhanden sein.

- $b: \mathbb{R} \to \mathbb{R}, b(x) = x$

Da jede zur x-Achse parallele Gerade den Funktionsgraphen genau 1 Mal schneidet, ist die Funktion injektiv (weil es nie öfter als 1 Mal ist) und auch surjektiv (weil es nie weniger als 1 Mal ist).

Das heißt die Funktion b ist bijektiv.



Bei der Überprüfung von Funktionen auf Injektivität und Surjektivität ist es immer sehr wichtig, auf die Definitions- und Zielmenge zu achten.

Ein Beispiel:

Wir wissen schon, dass $f: \mathbb{R} \to \mathbb{R}, f(x) = x^2$ in dieser Form weder bijektiv, noch surjektiv ist.

Wenn wir nun die Funktion auf $f_1: \mathbb{R}_0^+ \to \mathbb{R}, f_1(x) = x^2$ abändern[20], ist sie injektiv, aber nicht surjektiv. („Da von den negativen Zahlen keine Pfeile mehr weggehen, fallen genau die Pfeile weg, die vorher doppelt waren.“)

$f_2: \mathbb{R} \to \mathbb{R}_0^+, f_2(x) = x^2$ ist surjektiv, aber nicht injektiv. („Die Funktion trifft die Zahlen in B wieder doppelt, weil von den negativen Zahlen aus A auch Pfeile weggehen, es trifft dafür alle Zahlen, die sich in der Menge B befinden, weil ja hier nur die negativen ohne Argument waren.“)

Mit $f_3: \mathbb{R}_0^+ \to \mathbb{R}_0^+, f_3(x) = x^2$ definiert man eine bijektive Funktion. („Die negativen Zahlen in A, die die doppelten Pfeile verursachten, sind weg, und auch die negativen Zahlen in B, die gar nicht getroffen wurden, fehlen, also wird jede Zahl in B genau 1x getroffen.“)

3.5.2.5 Umkehrfunktionen

Jede bijektive Funktion $f: A \to B$ besitzt eine Umkehrfunktion $f^{-1}: B \to A$, die dem Funktionswert $f(x)$ den Wert des Arguments x zuordnet. Die Funktion f muss dafür bijektiv sein, da sonst nicht jeder Funktionswert eindeutig auf ein Argument zurückgeführt werden kann. In den Pfeildiagrammen würden für die jeweiligen Umkehrfunktionen die Pfeile einfach in die andere Richtung gezeichnet werden.

[20] $\mathbb{R}_0^+$ = positive reelle Zahlen inkl. 0

Definition (**Umkehrfunktion**): „Sei f: A → B bijektiv. Die inverse Abbildung von f, die Inverse oder die Umkehrfunktion von f ist definiert durch

$$f^{-1}: B \to A$$
$$f(a) \mapsto a.\text{"}$$

(Schichl & Steinbauer, 2012, S. 165)

Aus der Definition einer Umkehrfunktion ist nun erkennbar, dass für eine Funktion $\mathrm{f}: \mathrm{A} \to \mathrm{B}$ mit der Umkehrfunktion $\mathrm{f}^{-1}: \mathrm{B} \to \mathrm{A}$ gilt:

$$\mathrm{f}\left(\mathrm{f}^{-1}(\mathrm{b})\right) = \mathrm{b}, \quad \mathrm{f}^{-1}\left(\mathrm{f}(\mathrm{a})\right) = \mathrm{a}.$$

(Vgl. Schichl & Steinbauer, 2012, S. 172)

Wenn man die Funktion und die Umkehrfunktion nacheinander auf einen Wert anwendet (egal in welcher Reihenfolge), gelangt man wieder zum ursprünglichen Wert.

Ein Beispiel:

Wir haben die injektive Funktion $f: \mathbb{R} \to \mathbb{R}$, $f(x) = 4x - 2$ gegeben und wollen die Umkehrfunktion bestimmen. Da $f(x) = y$ setzen wir das ein und lösen die Gleichung nach x auf, um von dem Funktionswert y wieder auf das Argument x schließen zu können:

$$y = 4x - 2$$
$$y + 2 = 4x$$
$$\frac{y+2}{4} = x$$

Also ergibt sich für die Umkehrfunktion $f^{-1}: \mathbb{R} \to \mathbb{R}, f^{-1}(y) = \frac{y+2}{4}$.

Wenn wir nun beim Wert

$$x = 12$$

starten und die Funktion f darauf anwenden, erhalten wir:

$$f(x) = 4x - 2$$
$$f(12) = 4 \cdot 12 - 2$$
$$f(12) = 46$$

Danach wenden wir die Umkehrfunktion auf 46 an:

$$f^{-1}(x) = \frac{x+2}{4}$$
$$f^{-1}(f(12)) = f^{-1}(46) = \frac{46+2}{4}$$
$$f^{-1}(f(12)) = f^{-1}(46) = 12$$

Wenn man also zuerst f und dann die Umkehrfunktion f^{-1} auf einen Ausgangswert anwendet, so ergibt sich wieder der Ausgangswert.

Wir starten wieder beim Wert

$$x = 12.$$

Wenn wir nun zuerst die Umkehrfunktion f^{-1} darauf anwenden, ergibt sich:

$$f^{-1}(x) = \frac{x+2}{4}$$
$$f^{-1}(12) = \frac{12+2}{4}$$
$$f^{-1}(12) = 3{,}5$$

Dann wenden wir die Funktion f auf das Ergebnis $3{,}5$ an:

$$f(x) = 4x - 2$$
$$f\left(f^{-1}(12)\right) = f(3{,}5) = 4 \cdot 3{,}5 - 2$$
$$f\left(f^{-1}(12)\right) = f(3{,}5) = 12$$

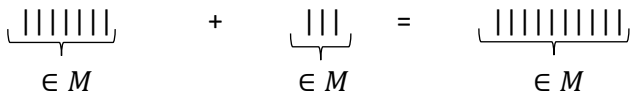
Wenn man also zuerst die Umkehrfunktion f^{-1} und dann die Funktion f auf einen Ausgangswert anwendet, so ergibt sich wieder der Ausgangswert.

3.5.3 Grundlegende mathematische Strukturen

Die Strukturen, die in diesem Teil vorgestellt werden, sind Mengen und Abbildungen bzw. Funktionen mit bestimmten Eigenschaften.

„Eine mathematische Struktur ist, grob gesagt, eine Klasse von Objekten, die alle dieselben Eigenschaften aufweisen, und eine dazu passende Klasse von Abbildungen zwischen den Objekten, die eben diese Eigenschaften erhalten." (Schichl & Steinbauer, 2012, S. 193)

Als Beispiel für eine mathematische Struktur könnte z.B. die Menge M aller Strichblöcke mit der Abbildung + der Aneinanderreihung zweier Strichblöcke dienen. Wenn ein Strichblock aus gleich langen aneinander gefügten Strichen besteht, befindet sich auch das Ergebnis der Abbildung wieder in M.



Auch die Menge der natürlichen Zahlen $\mathbb{N}$ mit der Abbildung der Addition oder der Multiplikation, bildet eine mathematische Struktur, da das Ergebnis wieder in $\mathbb{N}$ liegt. (Vgl. Schichl & Steinbauer, 2012, S. 194f)

3.5.3.1 Gruppoid, algebraische Struktur

Definition (**Gruppoid, algebraische Struktur**): „Sei G eine nichtleere Menge.

(i) Eine Verknüpfung auf G ist eine Abbildung

$$\circ: G \times G \to G$$

Anstelle von $\circ\,(g,h)$ für zwei Elemente $g, h \in G$ schreiben wir $g \circ h$ und wir nennen das Bild von (g,h) unter $\circ$ das Ergebnis oder den Wert der Verknüpfung

(ii) Wenn wir die Menge G zusammen mit der Verknüpfung $\circ$ untersuchen, so schreiben wir meist $(G,\circ)$ und nennen sie Gruppoid oder algebraische Struktur oder Magma. In diesem Zusammenhang nennen wir G auch Grundmenge." (Schichl & Steinbauer, 2012, S. 197)

Die Menge der Strichblöcke mit der Abbildung der Aneinanderreihung, $(\mathbb{N},+)$ und $(\mathbb{N},\cdot)$ sind also Gruppoide bzw. algebraische Strukturen. Auch $(\mathbb{Z},+)$, $(\mathbb{Z},\cdot)$, $(\mathbb{R},+)$ und $(\mathbb{R},\cdot)$ sind Gruppoide, da das Ergebnis einer Addition oder Multiplikation zweier Zahlen dieser Mengen immer in der jeweiligen Menge liegt.

Bei endlichen Mengen, ist es oft nützlich, die Ergebnisse der möglichen Abbildungen zwischen den Elementen in einer Verknüpfungstabelle anzugeben. Die Abbildung ⋄ auf der Menge M = {a,b}, für die gilt: $a \diamond a = a, a \diamond b = a, b \diamond a = b$ und $b \diamond b = b$ könnte wie in Tabelle 8 dargestellt werden:

Tabelle 8: Beispiel für eine Verknüpfungstabelle

⋄	a	b
a	a	a
b	b	b

In Verknüpfungstabellen wird üblicherweise der erste Operand der Zeile und der zweite Operand der Spalte entnommen (Vergleiche die Eintragungen für $a \diamond b$ und $b \diamond a$). Es funktioniert also wie die Benennung von Matrixelementen. (Vgl. Schichl & Steinbauer, 2012, S. 198)

3.5.3.2 Halbgruppen

Weil oft Mengen mit Abbildungen untersucht werden, die noch mehr als nur die Eigenschaften eines Gruppoids aufweisen sollen, kommt bei der Struktur der Halbgruppe eine neue Eigenschaft hinzu:

> Definition (**Assoziativgesetz, Halbgruppe**): „Ein Gruppoid $(G,\circ)$ heißt Halbgruppe, falls die Verknüpfung assoziativ ist, also das Assoziativgesetz
> $$(AG) \quad \forall g,h,k \in G: (g \circ h) \circ k = g \circ (h \circ k)$$
> gilt. In diesem Fall ist das Setzen von Klammern nicht notwendig, und wir dürfen an Stelle von $(g \circ h) \circ k$ einfach $g \circ h \circ k$ schreiben.“ (Schichl & Steinbauer, 2012, S. 207)

Die Menge der Strichblöcke mit der Abbildung der Aneinanderreihung, $(\mathbb{N},+)$, $(\mathbb{N},\cdot)$, $(\mathbb{Z},+)$, $(\mathbb{Z},\cdot)$, $(\mathbb{R},+)$ und $(\mathbb{R},\cdot)$ sind Halbgruppen, da jeweils das Assoziativgesetz gilt.

3.5.3.3 Monoide

Um besprechen zu können, welche zusätzliche Eigenschaft die mathematische Struktur der Monoide ausmacht, muss zuerst eine neue Definition eingeführt werden.

> Definition (**Einselement**): „Ein Element e eines Gruppoids G heißt Einselement oder neutrales Element, falls
> $$\forall g \in G: g \circ e = e \circ g = g$$
> gilt. Wird die Verknüpfung mit + bezeichnet (additiv geschrieben), so bezeichnet man e oft mit 0 oder $\mathbb{0}$ und nennt es Nullelement. Einselemente bezüglich multiplikativ geschriebener Verknüpfungen erhalten auch oft die Bezeichnung 1 oder $\mathbb{1}$.“ (Schichl & Steinbauer, 2012, S. 209)

Für $(\mathbb{N},+),(\mathbb{Z},+)$ und $(\mathbb{R},+)$ ist 0 ein Nullelement. Für $(\mathbb{N},\cdot),(\mathbb{Z},\cdot)$ und $(\mathbb{R},\cdot)$ ist 1 ein Einselement.

Eindeutigkeit des neutralen Elements: „Besitzt ein Gruppoid $(G,\circ)$ ein Einselement e, so ist e eindeutig bestimmt (und wir können von dem Einselement in G sprechen)." (Schichl & Steinbauer, 2012, S. 211)

Beweis: Der Satz gilt nur, wenn G ein Einselement $e \in G$ hat, also gilt nach der Definition des Einselements

$$\forall g \in G: g \circ e = e \circ g = g$$

Wenn es ein zweites Einselement $e_1 \in G$ gibt, gilt auch für dieses

$$\forall g \in G: g \circ e_1 = e_1 \circ g = g$$

Wir können nun zeigen, dass $e = e_1$, da $e \in G$ und $e_1 \in G$. Aus $e_1 \circ e = e$ und $e_1 \circ e = e_1$ folgt

$$e = e_1$$

□

Definition (**Monoid**): „Ist $(G,\circ)$ eine Halbgruppe und existiert ein Einselement $e \in G$, so nennt man G auch Monoid und schreibt oft $(G,\circ,e)$." (Schichl & Steinbauer, 2012, S. 212)

$(\mathbb{N},+,0)$, $(\mathbb{Z},+,0)$, $(\mathbb{R},+,0)$, $(\mathbb{N},\cdot,1)$, $(\mathbb{Z},\cdot,1)$ und $(\mathbb{R},\cdot,1)$ sind Monoide.

3.5.3.4 Gruppen

Definition (**Kommutativgesetz**): „Eine Verknüpfung $\circ$ in einem Gruppoid $(G,\circ)$ heißt kommutativ, falls das Kommutativgesetz erfüllt ist, d.h. falls

$$(KG) \quad \forall g,h \in G: g \circ h = h \circ g$$

gilt." (Schichl & Steinbauer, 2012, S. 215)

Auf $(\mathbb{N},+)$, …, $(\mathbb{R},\cdot)$ gilt das Kommutativgesetz.

Definition (**Inverses Element**): „Sei $(G,\circ,e)$ ein Gruppoid mit Einselement, und sei $a \in G$. Wir nennen $a' \in G$ inverses Element von a, falls

$$a' \circ a = a \circ a' = e$$

gilt. Wir nennen a' auch Inverses zu a und schreiben meist a^{-1}. Ist das Verknüpfungszeichen ein +, schreiben wir die Operation also additiv, dann bezeichnen wir das Inverse von a üblicherweise mit $-a$." (Schichl & Steinbauer, 2012, S. 217)

Wir betrachten wieder unsere Beispiele:

- $(\mathbb{N},+,0)$: Nur für 0 gibt es ein inverses Element.
- $(\mathbb{Z},+,0)$: Jedes Element $a \in Z$ hat als inverses Element $-a$.
- $(\mathbb{R},+,0)$: Jedes Element $a \in \mathbb{R}$ hat als inverses Element $-a$.
- $(\mathbb{N},\cdot,1)$: Nur für 1 gibt es das inverse Element 1.
- $(\mathbb{Z},\cdot,1)$: 1 hat als inverses Element 1 und -1 das Element -1, ansonsten gibt es für kein Element aus $\mathbb{Z}$ ein Inverses.

- $(\mathbb{R},\cdot,1)$: Jedes Element $a \in \mathbb{R}\backslash\{0\}$ hat als inverses Element a^{-1}. Nur 0 hat kein Inverses Element. (Vgl. Schichl & Steinbauer, 2012, S. 217)

Eindeutigkeit des Inversen: „Sei $(G,\circ,e)$ ein Monoid und $g \in G$. Existiert zu g ein Inverses g^{-1}, so ist g^{-1} eindeutig bestimmt." (Schichl & Steinbauer, 2012, S. 218)

Beweis: Weil g^{-1} invers zu g ist, gilt nach Definition des Inversen:

$$g \circ g^{-1} = g^{-1} \circ g = e$$

Sei g_1 ein weiteres Inverses zu g, dann gilt außerdem:

$$g \circ g_1 = g_1 \circ g = e$$

Dann erhalten wir

$$g_1 = g_1 \circ e = g_1 \circ (g \circ g^{-1}) \overset{(AG)}{=} (g_1 \circ g) \circ g^{-1} = e \circ g^{-1} = g^{-1}.$$

Also gilt $g_1 = g^{-1}$.

□

Definition (**Gruppe**): „Sei $(G,\circ)$ ein Gruppoid. Gelten die folgenden Eigenschaften

(G1) Assoziativgesetz:
$$\forall g,h,k \in G: (g \circ h) \circ k = g \circ (h \circ k),$$

(G2) Einselement:
$$\exists e \in G: \forall g \in G: e \circ g = g \circ e = g,$$

(G3) Inverse:
$$\forall g \in G: \exists g^{-1} \in G: g^{-1} \circ g = g \circ g^{-1} = e,$$

dann heißt (G,o) Gruppe. Gilt außerdem noch

(G4) Kommutativgesetz:
$$\forall g,h \in G: g \circ h = h \circ g,$$

dann heißt G kommutative oder abelsche Gruppe (nach Nils Henrik Abel (1802-1829))." (Schichl & Steinbauer, 2012, S. 219)

Wenn ein Monoid zusätzlich für jedes Element ein Inverses besitzt, ist es eine Gruppe. (Schichl & Steinbauer, 2012, S. 220)

Mit dem Wissen, welche der betrachteten Zahlenmengen Inverse Elemente für all ihre Elemente besitzen, können sofort ein paar Beispiele für Gruppen genannt werden: $(\mathbb{Z},+)$ und $(\mathbb{R},+)$. Da auch das Kommutativgesetz gilt, sind sie sogar abelsche Gruppen. Mit einer kleinen Änderung bildet auch $(\mathbb{R}\backslash\{0\},\cdot)$ eine kommutative Gruppe.

Wie man sieht, werden die gezeigten mathematischen Strukturen immer spezieller. So werden für ein Gruppoid die wenigsten Eigenschaften vorausgesetzt, für eine Gruppe die meisten. Jede Gruppe ist auch ein Gruppoid, aber ein Gruppoid im Allgemeinen keine Gruppe. Oft macht es Sinn die spezifischste Bezeichnung zu wählen. In Abbildung 9 sind die kennengelernten Strukturen zusammengefasst. Diese Abbildung erinnert an bekannte Darstellungen der Zahlenmengen ($\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$, …). Auch hier gilt, dass jede natürliche Zahl auch

eine reelle Zahl ist, aber nicht jede reelle Zahl ist auch in $\mathbb{N}$ enthalten. (Vgl. Schichl & Steinbauer, 2012, S. 201f)

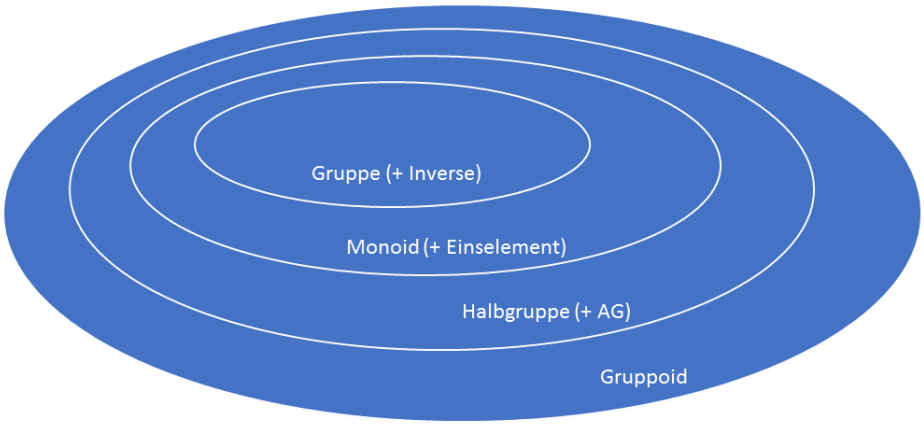


Abbildung 9: Mathematische Strukturen

3.5.4 Modulares Rechnen

Beim Modularen Rechnen beschäftigt man sich mit dem Rechnen auf endlichen Mengen. Die Zahlenmengen wie $\mathbb{N}$, $\mathbb{Q}$ und $\mathbb{R}$ sind unendlich. Eine endliche Menge wäre

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n\text{-}1\}.$$

Als Beispiel kann man sich $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ ansehen. Wie kann man nun auf dieser Menge rechnen? Auf der Menge $\mathbb{Z}_{12}$ addiert und subtrahiert man im täglichen Leben ständig. Wenn es 8 Uhr ist, wie spät ist es in 6 Stunden? Wie spät war es vor 10 Stunden? Auf diese und ähnliche Fragen sollen in diesem Kapitel Antworten gefunden werden. (Vgl. Jukna, 2008, S. 68)

3.5.4.1 Modulare Addition

Definition (**Modulare Addition**): Die Operation $\oplus_a$ wird für $a \in \mathbb{N}\backslash\{0\}$ und $x, y \in \mathbb{N}$ durch

$$x \oplus_a y = (x + y)\ mod\ a,$$

definiert. Die Operation $\oplus_a$ wird Addition modulo a genannt. (Vgl. Freiermuth, Hromkovic, Keller, & Steffen, 2010, S. 33f)

Ein Beispiel:

$$32 \oplus_7 16 = (32 + 16)\ mod\ 7 = 48\ mod\ 7 = 6.$$

Man beachte, dass das Ergebnis der Addition modulo a nach dem Satz Division mit Rest aus *Kapitel 3.5.1: „Ganze Zahlen"* immer kleiner als a ist. Es werden hier eine Reihe von

Rechengesetzen für modulares Rechnen vorgestellt werden, die mit M1, M2, usw. nummeriert werden.

M1: Für $z, m, a \in \mathbb{N}$ und $a > 0$ gilt:

$$z \; mod \; a = (z + m \cdot a) \; mod \; a.$$

Beweis: Seien $z, m, a \in \mathbb{N}$ und $a > 0$. Wir setzen $r := z \; mod \; a$, dann kann z als ein Vielfaches von a mit dem Rest r ausgedrückt werden. Der Rest r ist nicht durch a teilbar.

$$\exists n \in \mathbb{Z}: z = n \cdot a + r$$

Das können wir in $(z + m \cdot a) \; mod \; a$ einsetzen:

$$(z + m \cdot a) \; mod \; a =$$

$$\big((n \cdot a + r) + m \cdot a\big) \; mod \; a =$$

$$\big((a \cdot n + a \cdot m) + r\big) \; mod \; a =$$

$$(a \cdot (n + m) + r) \; mod \; a$$

Da $a \cdot (n + m)$ durch a teilbar ist, ist der Rest bei Division von $(z + m \cdot a)$ durch a genau r. Weil wir zu Beginn außerdem $r := z \; mod \; a$ gesetzt haben, gilt:

$$(z + m \cdot a) \; mod \; a = r = z \; mod \; a$$

□

M2: Für $x, y, a \in \mathbb{N}$ und $a > 0$ gilt:

$$(x + y) \; mod \; a = (x \; mod \; a + y \; mod \; a) \; mod \; a$$

Beweis:

Wir erinnern uns, dass

$$x = a \cdot x \; div \; a + x \; mod \; a \; (\text{und } y = a \cdot y \; div \; a + y \; mod \; a)$$

Deswegen gilt:

$$(x + y) \; mod \; a =$$

$$= (a \cdot x \; div \; a + x \; mod \; a + a \cdot y \; div \; a + y \; mod \; a) \; mod \; a$$

$$=^{(KG \text{ und } DG)} \left(\underbrace{a \cdot (x \; div \; a + y \; div \; a)}_{Vielfaches \; von \; a} + x \; mod \; a + y \; mod \; a \right) mod \; a$$

$$=^{(M1)} (x \; mod \; a + y \; mod \; a) \; mod \; a$$

□

(M2) bedeutet, dass man bei der modularen Addition mehrerer Zahlen zwei Möglichkeiten hat. Entweder können die Summanden zusammengezählt werden und danach der Rest modulo a berechnet werden, oder man berechnet für alle Summanden modulo a den Rest, zählt diese Reste zusammen und bildet danach (falls die erhaltene Zahl größer als a ist) wieder den Rest modulo a. (Vgl. Freiermuth, Hromkovic, Keller, & Steffen, 2010, S. 36f)

Ein Beispiel, bei dem wir beide Möglichkeiten ausprobieren:

1. Möglichkeit:
$1170 \oplus_7 3390 = (1170 + 3390)\ mod\ 7 = 4560\ mod\ 7 = 3.$

2. Möglichkeit:
$1170 \oplus_7 3390 = \big((1170\ mod\ 7) + (3390\ mod\ 7)\big)\ mod\ 7 = (1 + 2)\ mod\ 7 = 3\ mod\ 7 = 0.$

3.5.4.2 Modulare Multiplikation

Definition (**Modulare Multiplikation**): Die Operation $\odot_a$ wird für $a \in \mathbb{N}\backslash\{0\}$ und $x, y \in \mathbb{N}$ durch

$$x \odot_a y = (x \cdot y)\ mod\ a$$

definiert. Die Operation $\odot_a$ wird Multiplikation modulo a genannt. (Vgl. Freiermuth, Hromkovic, Keller, & Steffen, 2010, S. 45)

Ein Beispiel:

$25 \odot_6 19 = (25 \cdot 19)\ mod\ 6 = 475\ mod\ 6 = 1$

Definiere für jedes $n \in \mathbb{N}\backslash\{0\}$ die Bezeichnung:

$$\mathbb{Z}_n = \{0, 1, \dots, n-1\} = \{x \in \mathbb{Z} \mid 0 \leq x < n\}.$$

Modulares Rechnen baut auf dieser Menge gemeinsam mit den Operationen $\oplus_n$ und $\odot_n$ statt der üblichen Rechenoperationen auf.

3.5.4.3 Modulares Rechnen und mathematische Strukturen[21]

Man sieht, dass $(\mathbb{Z}_n, \oplus_n)$ und $(\mathbb{Z}_n, \cdot)$ Gruppoide bilden, da durch die Verknüpfung zweier Elemente aus $\mathbb{Z}_n$ mit $\oplus_n$ oder $\odot_n$ keine Elemente entstehen, die nicht in $\mathbb{Z}_n$ liegen. (Vgl. Freiermuth, Hromkovic, Keller, & Steffen, 2010, S. 45)

Nun wird überprüft, ob $\oplus_n$ auch assoziativ auf $\mathbb{N}$ ist.

$$(x \oplus_n y) \oplus_n z =^{Def(\oplus_n)} \big((x + y)\ mod\ n\big) \oplus_n z$$

$$=^{Def(\oplus_n)} \Big(\big((x + y)\ mod\ n\big) + z\Big)\ mod\ n$$

$$=^{(M2)} (x + y + z)\ mod\ n$$

[21] Siehe dazu *Kapitel 3.5.3: „Grundlegende mathematische Strukturen“*

Und analog folgt auch:

$$x \oplus_n (y \oplus_n z) =^{Def(\oplus_n)} x \oplus_n \big((y+z) \bmod n\big)$$

$$=^{Def(\oplus_n)} \Big(x + \big((y+z) \bmod n\big)\Big) \bmod n$$

$$=^{M2} (x+y+z) \bmod n$$

Daraus folgt

$$(x \oplus_n y) \oplus_n z = (x+y+z) \bmod n = x \oplus_n (y \oplus_n z).$$

D.h. $\oplus_n$ ist auf $\mathbb{N}$ assoziativ.

□

$(\mathbb{N}, \oplus_n)$ ist also eine Halbgruppe $\forall n \in \mathbb{N}\backslash\{0\}$. Da es auch ein neutrales Element, nämlich 0, gibt, ist die Struktur auch ein Monoid. (Vgl. Freiermuth, Hromkovic, Keller, & Steffen, 2010, S. 48)

Nun soll auch $(\mathbb{N}, \odot_n)$ genauer betrachtet werden. Dazu kommt ein neues Gesetz zum modularen Rechnen:

M3: Für $x, y, n \in \mathbb{N}$ und $n \neq 0$ *gilt*

$$(x \cdot y) \bmod n = (x \bmod n \cdot y \bmod n) \bmod n$$[22]

Beweis: x und y können für $k = x \; div \; n$ und $l = y \; div \; n$ ausgedrückt werden durch

$$x = k \cdot n + x \bmod n \text{ und } y = l \cdot n + y \bmod n$$

Dadurch erhalten wir

$$x \odot_n y$$

$$=^{Def(\odot_n)} (x \cdot y) \bmod n$$

$$=^{\substack{x=k\cdot n+x \bmod n \\ y=l\cdot n+y \bmod n}} \big((k \cdot n + x \bmod n) \cdot (l \cdot n + y \bmod n)\big) \bmod n$$

$$=^{Ausmultiplizieren} \big(n^2 kl + nk \cdot (y \bmod n) + nl \cdot (x \bmod n) + (x \bmod n) \cdot (y \bmod n)\big) \bmod n$$

$$=^{DG} \left(n \cdot \underbrace{[nkl + k \cdot (y \bmod n) + l \cdot (x \bmod n)]}_{\in \mathbb{Z}} + (x \bmod n) \cdot (y \bmod n)\right) \bmod n$$

$$=^{(M1)} \big((x \bmod n) \cdot (y \bmod n)\big) \bmod n$$

□

[22] $x \bmod n \cdot y \bmod n$ ist in dieser Arbeit immer zu lesen als $(x \bmod n) \cdot (y \bmod n)$. Analog dazu ist auch $x \; div \; n \cdot y \; div \; n$ als $(x \; div \; n) \cdot (y \; div \; n)$ zu deuten.

Das Gesetz (M3) kann auch als

$$x \odot_n y = x \bmod n \odot_n y \bmod n$$

formuliert werden. (Vgl. Freiermuth, Hromkovic, Keller, & Steffen, 2010, S. 49)

Auch die Operation $\odot_n$ ist auf $\mathbb{N}$ assoziativ. Der Beweis funktioniert analog wie der Beweis zur Assoziativität von $\oplus_n$ auf $\mathbb{N}$ und wird hier darum nicht durchgeführt.

Weil $(\mathbb{N},\odot_n)$ als neutrales Element die Zahl 1 hat, ist auch $(\mathbb{N},\odot_n), \forall n \in \mathbb{N}\backslash\{0\}$ ein Monoid.

Als nächstes soll untersucht werden, ob es in $(\mathbb{Z}_n,\oplus_n)$ auch inverse Elemente gibt. Als Beispiel kann man die Struktur $(\mathbb{Z}_5,\oplus_5)$ annehmen. Das neutrale Element ist 0.

Wenn jetzt für ein $a \in \mathbb{Z}_5$ das inverse Element $(-a)$ gesucht wird, muss gelten:

$$\big(a + (-a)\big) \bmod 5 = 0$$

Setzt man $a = 0$, erhält man für $(-0) = 0$, weil:

$$(0 + 0) \bmod 5 = 0$$

Wenn man das inverse Element von 1 finden will, sieht man, dass $(-1) = 4$, denn nur dann gilt:

$$(1 + 4) \bmod 5 = 0$$

Analog dazu ergibt sich, dass

$$(-2) = 3, \text{ denn } (2 + 3) \bmod 5 = 0$$

$$(-3) = 2, \text{ denn } (3 + 2) \bmod 5 = 0$$

$$(-4) = 1, \text{ denn } (4 + 1) \bmod 5 = 0$$

Man kann für $(\mathbb{Z}_5,\oplus_5)$ also die Regel $(-a) = (5 - a) \bmod a$ für die Berechnung der inversen Elemente aufstellen.

M4: „In jeder kommutativen Gruppe $(\mathbb{Z}_d,\oplus_d)$ gilt für jedes $a \in \mathbb{Z}_d$

$$(-a) = (d - a) \bmod d,$$

wobei $(d - a) \bmod d \in \mathbb{Z}_d$, weil $d - a$ eine positive Zahl ist.“ (Freiermuth, Hromkovic, Keller, & Steffen, 2010, S. 53)

Beweis:

$$a \oplus_d (d - a)$$

$$=^{Def(\oplus_d)} \big(a + (d - a)\big) \bmod d$$

$$= (a + d - a) \bmod d$$

$$= d \bmod d$$

$$= 0$$

□

Das heißt, dass die Subtraktion in $\mathbb{Z}_d$ anhand der Addition berechnet werden kann. Wenn man sich wieder an das Anfangsbeispiel mit der Uhr erinnert, macht das auch Sinn, denn eine Subtraktion würde einfach bedeuten, dass man auf der Uhr gegen den Uhrzeigersinn weiterzählt. Anstatt das zu tun, kann jede Zahl aus einer anderen auch einfach durch Weiterzählen im Uhrzeigersinn erreicht werden, weshalb man die Subtraktion gar nicht unbedingt braucht. Allgemein kann man also sagen:

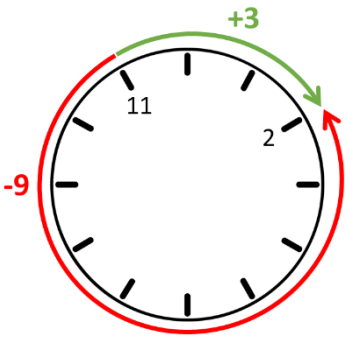


Abbildung 10: Uhr-Beispiel

$$a \ominus_d b = a \oplus_d (-b) = \big(a + (d - b)\big) \bmod d.$$

(Vgl. Freiermuth, Hromkovic, Keller, & Steffen, 2010, S. 53)

Siehe dazu auch Abbildung 10 als Veranschaulichung.

3.5.4.4 Modulares Quadrieren und modulare Wurzeln

Das modulare Quadrieren funktioniert wie das modulare Multiplizieren. Zu einer Zahl x berechnet man das Quadrat $x^2 \bmod n$ in $(\mathbb{Z}_n\backslash\{0\},\odot_n)$, wobei das Quadrat wieder in $\mathbb{Z}_n$ liegt.

Ein Beispiel:

Wir sollen für $(\mathbb{Z}_9\backslash\{0\},\odot_9)$ die modularen Quadrate berechnen:

$$1^2 mod\ 9 = 1$$
$$2^2 mod\ 9 = 4$$
$$3^2 mod\ 9 = 9\ mod\ 9 = 0$$
$$4^2 mod\ 9 = 16\ mod\ 9 = 7$$
$$5^2 mod\ 9 = 25\ mod\ 9 = 7$$
$$6^2 mod\ 9 = 36\ mod\ 9 = 0$$
$$7^2 mod\ 9 = 49\ mod\ 9 = 4$$
$$8^2 mod\ 9 = 64\ mod\ 9 = 1.$$

Wir sehen, dass 1 das Quadrat modulo 9 von 1 und 8 ist. Das Quadrat modulo 9 der Zahlen 2 und 7 ist 4. 0 ist das Quadrat modulo 9 der Zahlen 3 und 6 und die Zahlen 4 und 5 haben das modulare Quadrat 7.
$0, 1, 4$ und 7 sind modulare Quadrate in $(\mathbb{Z}_9\backslash\{0\},\odot_9)$.

Definition (**Modulares Quadrat**): „Sei n eine positive ganze Zahl. Wir nennen eine Zahl $z \in \mathbb{Z}_n\backslash\{0\}$[23] modulares Quadrat in $(\mathbb{Z}_n\backslash\{0\},\odot_n)$ oder quadratischer Rest, wenn eine Zahl $x \in \mathbb{Z}_n\backslash\{0\}$ existiert, so dass $z = x^2 \bmod n$.“ (Freiermuth, Hromkovic, Keller, & Steffen, 2010, S. 291)

Alle Zahlen aus $(\mathbb{Z}_n\backslash\{0\},\odot_n\}$ haben ein modulares Quadrat, aber es sind nicht alle ein modulares Quadrat einer Zahl. (Vgl. Freiermuth, Hromkovic, Keller, & Steffen, 2010, S. 292)

[23] Hier und in weiterer Folge wird statt der Schreibweise der zitierten Quelle $\mathbb{Z}_n - 0$, die weiter verbreitete Schreibweise $\mathbb{Z}_n\backslash 0$ verwendet.

Definition (**Modulare Wurzel**): „Wir sagen, dass x eine modulare Wurzel von $z \in (\mathbb{Z}_n \backslash \{0\}, \odot_n)$ ist, falls $x^2 \; mod \; n = z$." (Freiermuth, Hromkovic, Keller, & Steffen, 2010, S. 292)

D.h. manche Zahlen haben keine modularen Wurzeln.

Satz W1: „Sei p eine Primzahl. Sei $x \in \mathbb{Z}_p$ eine modulare Wurzel der Zahl $z \in \mathbb{Z}_p \backslash \{0\}$. Dann ist auch $(-x) = p - x \in \mathbb{Z}_p \backslash \{0\}$ eine modulare Wurzel von z." (Freiermuth, Hromkovic, Keller, & Steffen, 2010, S. 292)

Beweis:
x ist eine modulare Wurzel von z modulo $p \Rightarrow x^2 \; mod \; p = z$.

$$(p - x)^2 \; mod \; p$$

$$=^{Ausmultiplizieren} (p^2 - 2px + x^2) \; mod \; p$$

$$=^{DG} (p \cdot (p - 2x) + x^2) \; mod \; p$$

$$=^{(M1)} x^2 \; mod \; p$$

$$= z$$

D.h. $(p - x)^2 \; mod \; p = z$, was laut der Definition der modularen Wurzel bedeutet, dass auch $(p - x) = (-x)$ eine modulare Wurzel von z modulo p ist.

□

Satz W2: „Sei p eine [ungerade] Primzahl und sei z ein modulares Quadrat (ein quadratischer Rest) in $(\mathbb{Z}_p \backslash \{0\}, \odot_p)$. Dann hat z genau zwei modulare Wurzeln." (Freiermuth, Hromkovic, Keller, & Steffen, 2010, S. 293)

Beweis (nach (Freiermuth, Hromkovic, Keller, & Steffen, 2010, S. 293))**:**

z ist ein modulares Quadrat $\Rightarrow \exists x: x^2 mod \; p = z$

$\xRightarrow{Satz \; W1}$ $(-x) = p - x$ ist eine modulare Wurzel von z

p ist ungerade $\Rightarrow x \neq -x$, weil eine Zahl gerade und eine ungerade sein muss

$\Rightarrow z$ hat mindestens zwei modulare Wurzeln, nämlich x und $-x$

Nun muss noch gezeigt werden, dass z nicht mehr als zwei modulare Wurzeln hat. Jede modulare Wurzel y von $z = x^2 mod \; p$ muss also x oder $(-x)$ sein. Das additive Inverse ist in $(\mathbb{Z}_p, \odot_p)$ eindeutig, also kann es außer x und $-x$ keine modularen Wurzeln geben.

Wir setzen y eine modulare Wurzel von z in $(\mathbb{Z}_p - \{0\}, \odot_p)$, dann gilt $y^2 \; mod \; p = z$.

$$z - z = x^2 \; mod \; p - y^2 \; mod \; p = 0$$

$$\Rightarrow (x^2 - y^2) \; mod \; p = 0$$

$$\Rightarrow p | (x^2 - y^2)$$

$$\Rightarrow p|\big((x+y)\cdot(x-y)\big)$$

Wegen $0 \leq |x-y| < p \Rightarrow x-y$ kann nur durch p teilbar sein, wenn $x-y=0$, also $x=y$ gilt. Weil $0 < x+y < 2p$, kann $x+y$ nur dann durch p teilbar sein, wenn $x+y=p$ bzw. $y=(-x)=p-x$ gilt. Somit kann y nur x oder das additive Inverse $(-x)$ sein.

□

Satz W3: „Sei p eine Primzahl. Für jede Zahl $a \in \{1,2,3,\dots,(p-1)\}$ gilt:
$$\{a \odot_p 1, a \odot_p 2, a \odot_p 3, \dots, a \odot_p (p-1)\} = \{1,2,3,\dots,(p-1)\}.$$
(Freiermuth, Hromkovic, Keller, & Steffen, 2010, S. 299)

Beweis (nach (Freiermuth, Hromkovic, Keller, & Steffen, 2010, S. 299f))**:**

Die Mengen haben beide gleich viele, nämlich $p-1$ Elemente. Das heißt wir müssen beweisen, dass

$$\forall i \neq j: a \odot_p i \neq a \odot_p j \text{ und } \forall k \in \mathbb{Z} - \{0\}: a \odot_p k \neq 0.$$

Wäre $a \odot_p k = 0$, würde gelten $p \mid a \cdot k$, d.h. a oder k wären durch p teilbar. Das führt zu einem Widerspruch, da $0 < a < p$ und $0 < k < p$.

Angenommen es gibt i und j mit $i > j$ und $a \odot_p i = a \odot_p j$. D.h. es gilt

$$(a \cdot i)\ mod\ p = (a \cdot j)\ mod\ p$$
$$\Leftrightarrow p \mid (a \cdot i - a \cdot j)$$
$$\Leftrightarrow p \mid a \cdot (i-j)$$
$$\Leftrightarrow p \mid a \text{ oder } p \mid (i-j)$$

Das kann nicht sein, weil gilt $0 < a < p$ und $0 < (i-j) < p$. Das heißt, es gilt

$$a \odot_p i \neq a \odot_p j, \forall i \neq j.$$

□

3.5.5 Ein Satz von Euler

Um die Aussage des Satzes von Euler verstehen zu können, muss zuvor noch der Begriff der **Euler'schen ϕ-Funktion** kennengelernt werden. Und zwar definiert man die Funktion $\phi(n)$ für ein $n \in \mathbb{N}$ als die Anzahl der Zahlen, die teilerfremd zu n und kleiner oder gleich n sind. (Vgl. Beutelspacher, Kryptologie: Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen, 2007, S. 102)

Einige Beispiele:

n	$\phi(n)$	Zahlen, die $\leq n$ und teilerfremd zu n sind
1	1	1
2	1	1
3	2	1,2
4	2	1,3
6	2	1,5
10	4	1,3,7,9
15	8	1,2,4,7,8,11,13,14

Eigenschaften der ϕ-Funktion:
(P1) „Wenn p eine Primzahl ist, so gilt
$$\phi(p) = p - 1.$$" (Beutelspacher, 2007, S. 102)
(P2) „Wenn p und q zwei verschiedene Primzahlen sind, so gilt
$$\phi(pq) = (p-1)(q-1).$$" (Beutelspacher, 2007, S. 102)

Beweis:

(P1) Weil p eine Primzahl ist, ist sie nur durch 1 und sich selbst teilbar, d.h. alle Zahlen $1, 2, \dots, p-1$ sind teilerfremd zu p und $\leq p$.

(P2) Anstatt die zu pq teilerfremden Zahlen anzusehen, kann man alle Zahlen, die nicht teilerfremd zu pq und $\leq pq$ sind, suchen. Insgesamt gibt es pq Zahlen $\in \mathbb{N}$, die $\leq pq$ sind. Von dieser Anzahl zieht man dann die nicht teilerfremden ab.

Das sind die q Vielfachen von p

$$\underbrace{p, 2p, 3p, \dots, (q-1)p, qp}_{=q \text{ verschiedene Zahlen}}$$

zusammen mit den p Vielfachen von q

$$\underbrace{q, 2q, 3q, \dots, (p-1)q, pq}_{=p \text{ verschiedene Zahlen}}.$$

Weil $pq = qp$, wurde dieses Element doppelt gezählt, d.h. eines davon muss weggerechnet werden. Insgesamt ergeben sich jetzt $(p + q - 1)$ Elemente $\leq pq$, die nicht teilerfremd zu pq sind. Dann erhält man folgende Rechnung:

$$\phi(pq) = pq - (p + q - 1) = pq - p - q + 1 = (p-1)(q-1).$$

□

Kleiner Satz von Fermat: „Für jede Primzahl p und jedes $a \in \mathbb{Z}\backslash\{0\}$ gilt
$$a^{p-1} \; mod \; p = 1.$$" (Freiermuth, Hromkovic, Keller, & Steffen, 2010, S. 301)

Beweis (aus (Freiermuth, Hromkovic, Keller, & Steffen, 2010, S. 301f))**:**

Aus Satz W3 ist bekannt, dass für $a \in \{1,2, \dots, (p-1)\}$ gilt

$$\{a \odot_p 1, a \odot_p 2, \dots, a \odot_p (p-1)\} = \{1, 2, \dots, (p-1)\}.$$

Durch die Produkte von a mit allen Zahlen aus $\mathbb{Z}_p \backslash \{0\}$ erzeugen wir also alle Zahlen aus $\mathbb{Z}_p \backslash \{0\}$, und zwar jede Zahl genau einmal. Damit muss das Produkt aller Zahlen aus der linken Menge gleich dem Produkt aller Zahlen aus der rechten Menge $\{1,2, \dots, (p-1)\}$ sein. Also gilt:

$$\big(a \cdot 1 \cdot 2 \cdot \dots \cdot a \cdot (p-1)\big) \; mod \; p = \big(1 \cdot 2 \cdot \dots \cdot (p-1)\big) \; mod \; p.$$

Weil die Multiplikation kommutativ ist, erhalten wir:

$$(1 \cdot 2 \cdot \dots \cdot (p-1) \cdot a^{p-1}) \; mod \; p = \big(1 \cdot 2 \cdot \dots \cdot (p-1)\big) \; mod \; p.$$

Wenn wir beide Seiten dieser Gleichung von links mit den inversen Elementen $2^{-1}, 3^{-1}, \dots, (p-1)^{-1}$ multiplizieren, erhalten wir

$$(2 \cdot 2^{-1} \cdot \dots \cdot (p-1) \cdot (p-1)^{-1} \cdot a^{p-1}) \; mod \; p = (2 \cdot 2^{-1} \cdot \dots \cdot (p-1) \cdot (p-1)^{-1}) \; mod \; p,$$

und somit

$$a^{p-1} \; mod \; p = 1.$$

Damit ist der kleine Satz von Fermat bewiesen.

□

Hilfssatz: „Seien p und q zwei verschiedene Primzahlen, und sei m eine natürliche Zahl $\leq pq$. Dann gilt für jede natürliche Zahl k:

$$m^{k(p-1)(q-1)+1} \; mod \; pq = m."$$

(Beutelspacher, 2007, S. 103)

Beweis (aus (Beutelspacher, Kryptologie: Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen, 2007, S. 104f))**:**

Für den Beweis brauchen wir als Voraussetzung den Kleinen Satz von Fermat, den wir bereits formuliert und bewiesen haben.

Zur Abkürzung setzen wir $h := k(p-1)(q-1)+1$. Dann ist zu zeigen: $m^h \; mod \; n = m$, mit anderen Worten: $(m^h - m) \; mod \; n = 0$. Dies geschieht in drei Schritten.

Schritt 1 (*p*)*.* Es gilt

$$(m^h - m) \; mod \; p = 0.$$

Wir erinnern uns daran, dass $h := k(p-1)(q-1)+1$ ist.

Nun wenden wir den kleinen Satz von Fermat an. Dazu brauchen wir die Voraussetzung, dass m und p teilerfremd sind. Das ist im Allgemeinen natürlich nicht richtig, da die Behauptung ja für alle Zahlen m gelten soll.

Was passiert, wenn m und p nicht teilerfremd sind? Da p eine Primzahl ist, muss dann notwendigerweise p ein Teiler von m sein. Wenn p die Zahl m teilt, so teilt p jede Potenz von

m, insbesondere also die Zahl m^h. Also teilt p nicht nur m, sondern auch m^h, und somit $m^h - m$. Mit anderen Worten:

$$(m^h - m)\ mod\ p = 0.$$

Also gilt unsere Behauptung in diesem Spezialfall, und wir können nun wirklich voraussetzen, dass m und p teilerfremd sind. Dann sagt der kleine Satz von Fermat

$$m^{p-1}\ mod\ p = 1.$$

Daraus ergibt sich:

$$m^h mod\ p = m^{1+k\cdot\phi(n)}\ mod\ p = m \cdot m^{k\cdot\phi(n)}\ mod\ p = m \cdot m^{k\cdot(p-1)(q-1)} mod\ p$$

$$= m \cdot (m^{p-1})^{k\cdot(q-1)} mod\ p = m \cdot 1^{k\cdot(q-1)} mod\ p = m\ mod\ p.$$

Also gilt die Behauptung von Schritt 1 (p).

Wie der nächste Schritt lautet, ist wohl jedem klar; wir verzichten auf einen Beweis:

Schritt 2 (q). Für jede natürliche Zahl m gilt

$$(m^h - m) mod\ q = 0.$$

Nun müssen wir nur noch die beiden Schritte zusammenführen:

Schritt 3 (n). Es gilt

$$m^h mod\ n = m.$$

Das folgt wie folgt: Nach den Schritten p und q gilt:

$$p \text{ teilt } (m^h - m) \text{ und } q \text{ teilt } (m^h - m)$$

Die beiden Primzahlen p und q teilen also dieselbe Zahl $z := m^h - m$. Da p und q verschiedene Primzahlen sind, muss dann auch ihr Produkt $p \cdot q$ die Zahl z teilen. Wenn wir das wieder zurückübersetzen, erhalten wir die Aussage

$$m^h - m\ mod\ p \cdot q = 0, \text{ oder } m^h\ mod\ n = m.$$

Das ist die Aussage von Schritt 3 (n), und damit ist die Aussage des Satzes bewiesen.

□

Der folgende Satz von Euler wird für die Kryptographie dieser Arbeit nicht benötigt, aus Gründen der Vollständigkeit, wird er trotzdem formuliert. Den Beweis dazu findet man z.B. in (Beutelspacher, Neumann, & Schwarzpaul, Kryptografie in Theorie und Praxis: Mathematische Grundlagen für Internetsicherheit, Mobilfunk und elektronisches Geld, 2010, S. 122).

Satz von Euler: „Seien m und n zwei teilerfremde natürliche Zahlen. Dann gilt:

$$m^{\phi(n)} mod\ n = 1."$$

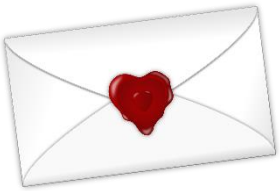
(Beutelspacher, 2007, S. 103)

4. Kryptographie in der Schule

Dieser Teil der Arbeit kann für ein Wahlpflichtfach oder eine ähnliche Situation wie ein Schulbuch verwendet werden. Es wird die Theorie des vorangegangenen Kapitels bearbeitet, wobei immer wieder auch auf dieses verwiesen wird. Man kann den Schülerinnen und Schülern Schritt für Schritt die benötigten Kapitel bereitstellen. Der Schulbuch-Teil ist mit Aufgaben versehen, deren Lösungen am Ende des Kapitels zu finden sind. Besonders beim geschichtlichen Teil können natürlich einzelne Ausschnitte weggelassen oder ersetzt werden.

Einige Teile des Theorieteils werden in diesem Teil weniger genau behandelt, was ein Versuch sein soll, den Unterrichtsstoff leichter verständlich für die Schülerinnen und Schüler zu halten.

4.1 Kryptographie - Was ist das denn?



Erinnern wir uns an die Geschichte von Romeo und Julia. Romeo und Julia waren ein Liebespaar, durften ihre Liebe aber wegen ihren Familien nicht öffentlich zeigen. Wenn sie einander Liebesnachrichten schicken wollten, riskierten sie immer, dass jemand sie fand und ihr Geheimnis offenbarte. Den Wunsch nach geheimer Kommunikation gab es schon immer und wird es immer geben. Bestimmt kennst auch du Situationen, bei denen du lieber nicht möchtest, das deine Gespräche oder Nachrichten für jeden öffentlich bekannt sind. Die Kryptographie beschäftigt sich damit, solche geheimen Kommunikationen zu ermöglichen. Sie entwickelt Geheimschriften, die auch über das Internet – wo theoretisch jede Nachrichten-übertragung abgefangen und sogar verändert werden kann – sicher übertragen werden können. Die versendeten Nachrichten sollen dann nur von den gewünschten Personen gelesen werden können.

Übung 1: Überlegt alleine oder zu zweit eine Geheimschrift. Denkt euch einen kurzen Text aus, übersetzt ihn dann in eure Geheimschrift und entschlüsselt die Geheimnachricht danach wieder. Zum Schluss stellt jede Gruppe ihre Geheimsprache kurz vor der Klasse vor.
Übung 2: Versucht an andere Lebenssituationen zu denken, in welchen Geheimnachrichten und geheime Kommunikationen nötig oder wünschenswert sind. Sammelt eure Ideen danach an der Tafel.

Lies dir *Kapitel 3.1 „Was ist Kryptographie? – Terminologie“* aus dem Theorieskript durch. Beschreibe mithilfe des Textes folgende Begriffe mit eigenen Worten:

Kryptographie:

Verschlüsselung:

Klartext:

Entschlüsselung:

Chiffriertext:

Alphabet:

Übung 1 (Fortsetzung): Nehmt euren verschlüsselten Text aus Übung 1 und findet die Antworten zu folgenden Fragen:

- Was war euer Klartext und was der Chiffriertext?
- Was war der Chiffrier- und der Dechiffrierschlüssel?
- Welche Alphabete habt ihr verwendet?
- Was war die Länge eures Klartextes und eures Chiffriertextes? Waren sie gleich

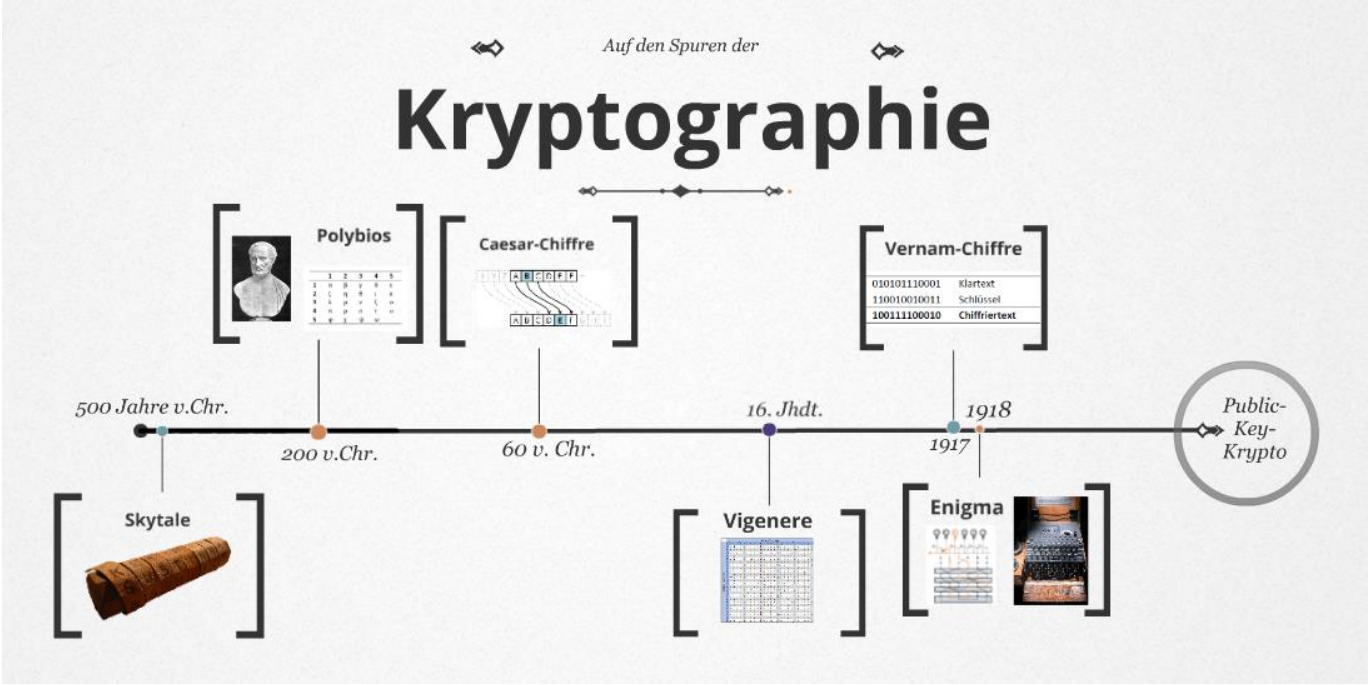
Lies *Kapitel 3.2 „Ziele der Kryptographie“*. Überlege dir zu jedem der 4 Sicherheitsziele zwei weitere Beispiele aus dem täglichen Leben, wo die jeweiligen Sicherheitsziele wichtig sind.
Vertraulichkeit:

Authentizität:

Integrität:

Verbindlichkeit:

4.2 Eine Reise durch die Zeit



4.2.1 Skytale

Mit unserer Zeitreise starten wir bereits 500 Jahre vor Christus. Die Spartaner verwendeten ab dieser Zeit die sogenannte Skytale, um in ihren zahlreichen Schlachten miteinander geheime Nachrichten austauschen zu können. (Vgl. Freiermuth, Hromkovic, Keller, & Steffen, 2010, S. 27) Somit war die Skytale wohl die erste militärische Verschlüsselungsmethode.

Geheimschrift Skytale

Verschlüsselung: Zur Verschlüsselung einer Nachricht wurde ein Streifen Pergament spiralförmig um einen Stab gewickelt. Die Nachricht wurde dann entlang des Stabes darauf geschrieben.

Entschlüsselung: Die Entschlüsselung erfolgte, indem der Pergamentstreifen wieder um einen Stab desselben Durchmessers gewickelt wurde. Nur so konnte man die ursprüngliche Nachricht wieder lesen.

Schlüssel: Der geheime Schlüssel besteht aus dem Durchmesser des Stabes. Ohne dieses Wissen, ist es schwierig den Klartext herauszufinden.

Um noch höhere Sicherheit zu erreichen, wurde das Pergamentband von Boten manchmal noch mit der beschriebenen Seite nach innen als Gürtel verwendet, sodass die Nachricht erst gar nicht gefunden wurde. (Singh, 2016, S. 23f)

Da bei dieser Art der Verschlüsselung die Buchstaben nur in eine andere Reihenfolge gebracht werden – es werden keine Buchstaben durch andere ersetzt, sondern nur vertauscht – werden solche Verschlüsselungen als **Transpositions-Chiffre** bezeichnet.

Übung 3: Probiert die Skytale-Verschlüsselung aus. Sucht dazu in der Klasse bzw. im Schulgebäude Gegenstände, die ihr als Skytale verwenden könnt, zerschneidet Papierstreifen und schreibt Nachrichten darauf. Tauscht dann die Geheimnachrichten aus und versucht sie zu entschlüsseln.

4.2.2 Polybios

Unser nächstes Verschlüsselungsverfahren bringt uns in das Jahr 200 vor Christus im Antiken Griechenland. Dort erfand der griechische Geschrichtsschreiber Polybios eine Geheimschrift, die heute nach ihm benannt ist.

Geheimschrift Polybios

Verschlüsselung: Jeder Buchstabe wird durch 2 Ziffern ersetzt. Dabei wird jeweils zuerst die Zeile und dann die Spalte angegeben. So schrieb Polybios z.B. statt π das Ziffernpaar 41.

Entschlüsselung: Je ein Zahlenpaar wird zuerst als Zeielennummer und dann als Spaltennummer gelesen. Es ergibt sich der Klartext-Buchstabe. Liest man im Chiffriertext die Zahlenkombination 53, bedeutet das ein ψ.

	1	2	3	4	5
1	α	β	γ	δ	ϵ
2	ζ	η	θ	ι	κ
3	λ	μ	ν	ξ	ο
4	π	ρ	σ	τ	υ
5	φ	χ	ψ	ω	

α	Alpha	ι	Iota	ρ	Rho
β	Beta	κ	Kappa	σ	Sigma
γ	Gamma	λ	Lambda	τ	Tau
δ	Delta	μ	My	υ	Ypsilon
ϵ	Epsilon	ν	Ny	φ	Phi
ζ	Zeta	ξ	Xi	χ	Chi
η	Eta	ο	Omikron	ψ	Psi
θ	Theta	π	Pi	ω	Omega

Die Geheimschrift Polybios ist in der heutigen Zeit kein sicheres Verschlüsselungsverfahren mehr, aber in der damaligen Zeit war es noch nicht so einfach zu entschlüsseln.

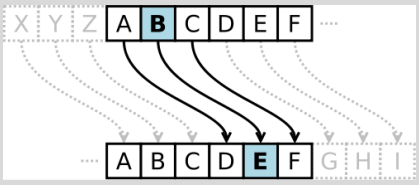
Aufgabe 1: Versuche den Klartext „π υ θ α γ ό ρ α σ“ mithilfe der Geheimschrift Polybios zu verschlüsseln. Wenn du Hilfe dabei brauchst, sieh dir das Beispiel in *Kapitel 3.3.1 „Polybios“* dazu an. Was bedeutet der Text in lateinischen Buchstaben? Was weißt du über diese Person?
Aufgabe 2: Dechiffriere den Text „1542114435432315332243“. Weißt du wofür man das Verfahren, das diesen Namen trägt, verwendet?

Ein Nachteil des Verschlüsselungsverfahrens Polybios ist, dass jede Person, die weiß wie es funktioniert, alle Geheimtexte, die damit verfasst wurden, sofort entschlüsseln kann. Das heißt du kannst jetzt, wo es alle deine Klassenkolleginnen und -kollegen kennen, nicht mehr verwenden um mit jemanden in der Klasse Geheimnachrichten auszutauschen. Beim nächsten Verfahren gibt es deshalb einen geheimen Schlüssel, ohne den man das Verfahren (nicht so leicht) knacken kann.

4.2.3 Caesar

Wir befinden uns in der Zeit von Gaius Julius Caesar (100 v. Chr. – 44 v. Chr.). Der Kaiser verwendete häufig Geheimschriften für militärische Zwecke. Überliefert wurde, dass Caesar für die nach ihm benannte Methode immer den Schlüsselwert k = 3 verwendete, insgesamt sind aber 25 verschiedene Schlüssel möglich. (Vgl. Singh, 2016, S. 25f)

Caesar-Verschlüsselung



Verschlüsselung: Die Buchstaben des Klartextes werden der Reihe nach jeweils um den Schlüsselwert k im Alphabet verschoben. Statt des Klartext-Buchstabens wird dann der Chiffrebuchstabe an dessen Stelle im Text gesetzt. Bei k = 3 würde wie im Bild statt „B“ ein „E“ geschrieben werden.

Enschlüsselung: Die Entschlüsselung funktioniert genau umgekehrt. Ein Buchstabe wird immer mit dem Buchstaben, der sich um k Stellen vor ihm im Alphabet befindet, ersetzt.

Schlüssel: Den geheimen Schlüssel bildet der Wert k ∈ [1;25]

Wenn bei der Verschiebung das Ende des Alphabets erreicht wird, wird wieder von vorne zu zählen begonnen. Man sieht das auch auf dem Bild im oberen grauen Kästchen – das „Y“ wird hier durch ein „B“ ersetzt, das „Z“ durch ein „C“.

Aufgabe 3: Chiffriere den Klartext „`caesar chiffre`“ mit dem Schlüssel k = 5.

Aufgabe 4: Du hast gemerkt, dass deine Freundin/dein Freund in letzter Zeit oft geheime Nachrichten verschickt und schaffst es, eine der Nachrichten unbemerkt mitzunehmen. Natürlich weißt du den Geheimschlüssel nicht. Schaffst du es trotzdem die Nachricht zu entschlüsseln?

Klartext:

_____

_____

Lies *Kapitel 3.3.3 „Caesar-Chiffre“*. Auf die dort vorgestellte Verbesserung der Caesar-Verschlüsselung kamen auch die Menschen der damaligen Zeit und Substitutionsverfahren erfreuten sich großer Beliebtheit. Aufgrund der riesigen Anzahl an möglichen Schlüsseln, hielten es viele Gehlerte für unmöglich diese Art von Codes zu knacken. Erst im 9. Jahrhundert schafften es die arabischen Kryptoanalytiker mithilfe der Sprachwissenschaft und Statistik Substitionsverfahren systematisch zu entschlüsseln. (Vgl. Singh, 2016, S. 29f)

Aufgabe 5: Versuche folgenden Geheimtext, der mit der Verbesserung der Caesar Verschlüsselung chiffriert wurde, zu knacken. Drei Buchstaben des Schlüssels sind als Hilfe schon vorgegeben. Die Tabelle kann so verwendet werden, dass zu den Klartext-Buchstaben in der oberen Zeile die passenden Chiffriertext-Buchstaben in der unteren Zeile dazugeschrieben werden, sobald man sie herausgefunden hat. Verwende die im Theorieteil angegebenen Häufigkeitsverteilungen der deutschen Sprache und versuche die kurzen Wörter zuerst herauszufinden.

`jex qxwyxooxwtva jxw dmxomw qxwoduktxooxktva eop vedup cxuw on xevlmdu gt zvmdzxv`

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
		d											*v*								*q*				

Klartext:

_____

_____

4.2.4 Vigenère

„Um das Jahr 1460 wandelte Alberti durch die Gärten des Vatikans und traf dabei auf seinen Freund Leonardo Dato, den Geheimsekretär des Papstes. Sie plauderten ein wenig über Fragen der Kryptographie, und Alberti sah sich schließlich veranlaßt, eine Abhandlung über das Thema zu schreiben, in der er nach eigenem Bekunden eine neue Form der Verschlüsselung entwickelte. Bis dahin hatte man im Substitutionsverfahren ein einziges Geheimtextalphabet zur Verschlüsselung der Botschaft verwendet. Alberti schlug nun vor, zwei oder mehr Geheimtextalphabete zu verwenden und während der Verschlüsselung zwischen ihnen hin und her zu springen, was die etwaigen Entschlüßler erheblich verwirren dürfte.“ (Singh, 2016, S. 65f)

Was der italienische Mathematiker Leon Battista Alberti schon im 15. Jahrhundert vorschlug, brauchte noch viele Jahre und die Arbeit mehrerer Gelehrten, bis der Franzose Blaise de Vigenère im 16. Jahrhundert all diese Schriften zu einem mächtigen Verschlüsselungssystem vereinte. (Vgl. Singh, 2016, S. 66ff)

Vigenère-Chiffre

Verschlüsselung: Die Vigenère-Chiffre funktioniert wie mehrere, hintereinander geschaltete Caesar-Chiffren. Zur Vereinfachung kann man sich das Schlüsselwort immer wieder über den Klartext schreiben. Verschlüsselt wird dann jeder Buchstabe anhand der jeweiligen Zeile im Vigenère-Quadrat.

Klartext „mathematik“ mit dem Schlüssel „leon“:

Schlüssel	l	e	o	n	l	e	o	n	l	e
Klartext	m	a	t	h	e	m	a	t	i	k
Geheimtext	x	e	h	u	p	q	o	g	t	o

Entschlüsselung: Man sucht den Chiffrebuchstaben in der entsprechenden Zeile des Quadrats, und sieht in der ersten Zeile an derselben Stelle den richtigen Klartext-Buchstaben.

Schlüssel: Der Schlüssel besteht aus einem Wort.

Schlüssel - Buchstabe \ Klartext-Buchstabe	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
b	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
c	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
d	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
e	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
f	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
g	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
h	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
i	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
j	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
k	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
l	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
m	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
n	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
o	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
p	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
r	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
s	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
t	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
u	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
v	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
w	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
x	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
z	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

Im Vigenère-Quadrat befinden sich in der ersten Zeile die Klartext-Buchstaben. In der ersten Spalte sind die Schlüssel-Buchstaben. Beim Verschlüsseln sucht man sich in der ersten Zeile den zu verschlüsselnden Buchstaben, und ersetzt ihn durch den Buchstaben direkt darunter, in der Zeile des Schlüssel-Buchstabens. Bei der Entschlüsselung geht man entlang der Zeile des Schlüssel-Buchstabens, sucht den Chiffrebuchstaben, den man vor sich hat, und ersetzt ihn mit dem Buchstaben direkt darüber in der ersten Zeile.

Aufgabe 6: Du hast 3 Tabellen zur Vigenére-Verschlüsselung gegeben. Ergänze jeweils die fehlende Zeile (Schlüssel, Klartext oder Geheimtext):

Schlüssel	f	i	l	m												
Klartext	a	l	i	c	e	i	m	w	u	n	d	e	r	l	a	n	d
Geheimtext																

Schlüssel											
Klartext	u	m	a	c	h	t	i	m	k	i	n	o
Geheimtext	h	m	c	j	y	b	k	t	d	v	n	q

Schlüssel	l	i	e	b	e	a	l	i	c	e								
Klartext																		
Geheimtext	o	z	i	j	e	c	s	b	u	m	p	j	i	o	w	e	n	p	u

Das Vigenère-Verfahren wurde von Charles Babbage, dessen Name vor allem für den Entwurf des ersten Computers bekannt ist, bereits um das Jahr 1854 systematisch geknackt. Dieser wichtige Fortschritt wurde allerdings nie von ihm veröffentlicht, seine Aufzeichnungen dazu fand man erst im 20. Jahrhundert. Stattdessen wird heute der Name Kasiski-Test für das Analyse-Verfahren verwendet, weil Friedrich Wilhelm Kasiski dieses unabhängig von Babbage im Jahr 1863 veröffentlichte. Es gibt mehrere Theorien darüber, warum Babbage seine Entdeckung verschwieg. Eine davon ist, dass er dies tat, um den Briten einen Vorteil im gerade stattfindendem Krimkrieg zu sichern. Dies wäre dann nicht der einzige Fall, bei dem Entdeckungen zur Entschlüsselung von Geheimtexten zur Gewährleistung der nationalen Sicherheit geheim gehalten wurden. (Vgl. Singh, 2016, S. 86-104)

4.2.5 Enigma

„Der deutsche Erfinder Arthur Scherbius und sein enger Freund Richard Ritter gründeten 1918 die Firma Scherbius & Ritter, ein innovatives Unternehmen, das vom Heizkissen bis zur Turbine alles Erdenkliche herstellte. Scherbius, ein findiger und umtriebiger Geist, war für die Forschung und Entschicklung zuständig. Es war eines seiner Lieblingsvorhaben, die unzulänglichen Chiffriersysteme aus dem Ersten Weltkrieg durch neue zu ersetzen. Bleistift und Papier sollten der Vergangenheit angehören, das neue System sollte die technischen Möglichkeiten des 20. Jahrhunderts nutzen. Scherbius, der in Hannover und München Elektrotechnik studiert hatte, entwickelte eine kryptographische Maschine […]. Er nannte sie Enigma, und sie sollte die gefürchtetste Chiffriermaschine der Geschichte werden.“ (Singh, 2016, S. 160)

Die Chiffriermaschine arbeitet mit mehreren Verschlüsselungsmechanismen, einerseits drei Rotorscheiben und einer Umkehrscheibe und andererseits einem Steckbrett. Insgesamt wird so eine immens Große Anzahl an möglichen Schlüsseln erreicht.
Es gibt 5 verschiedene Rotorscheiben, wobei für eine Verschlüsselung jeweils nur 3 davon benötigt werden. Diese können in beliebiger Reihenfolge in den 3 dafür vorgesehen Einkerbungen der Maschine eingesetzt werden. Außerdem kann auch jede Rotorscheibe 26 verschiedene Anfangspositionen einnehmen (nämlich eine, für jeden Buchstaben). Am Steckerbrett kann der elektronische Weg von insgesamt 6 Buchstabenpaaren mithilfe von Steckerkabeln ausgetauscht werden, sodass eine zusätzliche Verschlüsselung dieser erfolgt.

Chiffriermaschine Enigma

Verschlüsselung: Die Maschine muss laut Schüsselangaben vorbereitet werden. Wenn man dann die Buchstaben der Reihe nach eingibt, leuchtet für jeden Buchstaben der entsprechende Chiffrier-Buchstabe auf. Dieser wird abgeschrieben und dann der nächste Buchstabe auf der Tastatur gedrückt.

Entschlüsselung: Die Maschine wird wieder laut Schlüsselangaben vorbereitet. Man arbeitet wie bei der Verschlüsselung, nur wird jetzt der Chiffrierbuchstabe eingegeben, um dann am Leuchtfeld den entsprechenden Klartextbuchstaben ablesen zu können.

Schlüssel: Um den Schlüssel vollständig anzugeben müssen die Reihenfolge der Rotorscheiben, deren Startpositionen und die Steckerverbindungen vermerkt sein. Ein möglicher Schlüssel könnte so aussehen:

Rotorscheiben			Startpositionen		
V	II	IV	R	A	N
Steckerverbindungen					
AW	DE	FL	GX	NO	YZ

Übung 4: Lies *Kapitel 3.3.6: Enigma* (bis zum Beginn von *Kapitel 3.3.6.1: Schlüsselmenge der Enigma*) aus dem Theorieskript durch und beschreibe anschließend mit eigenen Worten die Funktionsweise im Inneren der Enigma. Die Erklärung kann auch mithilfe einer Skizze erfolgen. Tausche dann deine Beschreibung mit einer Klassenkollegin oder einem -kollegen aus und kontrolliert eure Arbeiten gegenseitig auf Fehler und Unklarheiten.

Übung 5: Versucht nun zu zweit die Anzahl der möglichen Schlüssel der Enigma zu berechnen. Beachtet dabei die Auswahl und Anordnung der Rotationsscheiben, die Grundstellungen der Scheiben und die Steckverbindungen. Wenn ihr nicht mehr weiterkommt oder eure Rechnungen kontrollieren wollt, gibt es die Lösung zur Aufgabe im Kapitel 3.3.6.1: Schlüsselmenge.

Auf der Website www.enigmaco.de wurde eine Veranschaulichung der Enigma realisiert, die verwendet werden kann, um Texte wie mit der Enigma zu ver- und entschlüsseln. Bearbeite folgende Aufgaben mithilfe der Website.

Aufgabe 7: Verwende folgenden Schlüssel um den Klartext `ARTHURSCHERBIUS` zu verschlüsseln:

Rotorscheiben			Startpositionen		
IV	I	V	L	D	X
Steckerverbindungen					
CH	DU	JK	NS	QZ	VW

Chiffriertext: _____

Was passiert, wenn du den erhaltenen Chiffriertext noch einmal mit demselben Schlüssel verschlüsselst? Was bedeutet das?

Übung 6: Verschlüssle einen Klartext mit der Enigma und gib einer Kollegin oder einem Kollegen den Chiffriertext und den dazugehörigen Schlüssel an. Versucht dann den Klartext wiederherzustellen.

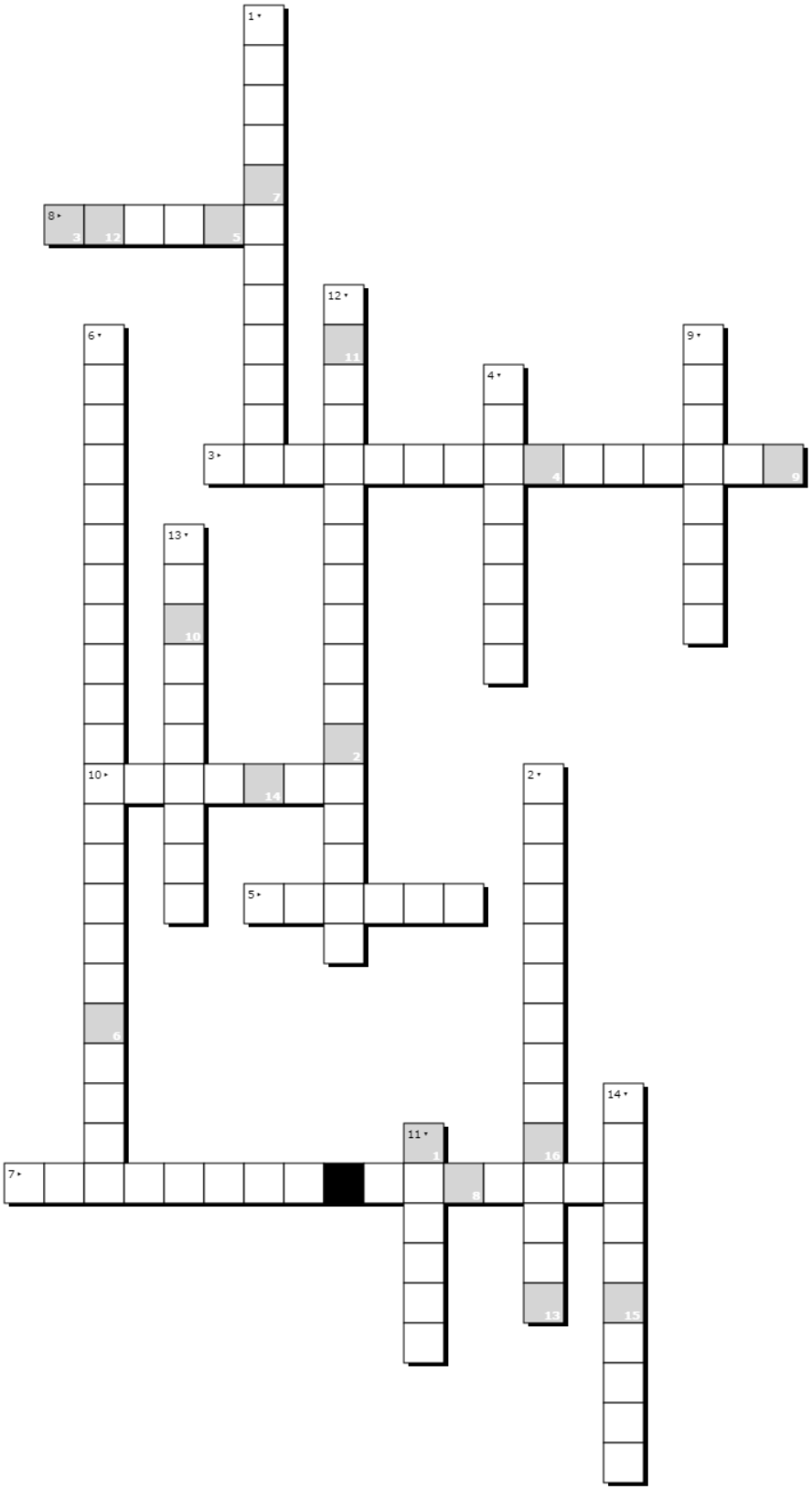
Aufgabe 8: Du hast eine Nachricht mit dem Geheimtext `HQXJAXDWNEY` abgefangen. Du weißt, dass der Schlüssel wie folgt aussieht:

Rotorscheiben			Startpositionen		
V	II	III	D	B	V
Steckerverbindungen					
AB	DF	GL	JS	UZ	WY

Wie lautet der Klartext? Natürlich bist du neugierig, was der Begriff der verschlüsselten Nachricht bedeutet und recherchierst das im Internet. Mach dir Notizen und besprecht danach in der Klasse, was ihr herausgefunden habt.

Das war auch schon der letzte Stopp unserer Zeitreise durch verschiedene Etappen der Verschlüsselung. Natürlich gab es auch noch viele andere Verschlüsselungsmechanismen im Laufe der Zeit, wir können sie jedoch nicht alle kennenlernen.

Auf der folgenden Seite ist ein Kreuzworträtsel, zur Wiederholung der kennengelernten geschichtlichen Verschlüsselungsmethoden.



1. Wissenschaft, die sich mit dem Knacken von Geheimschriften beschäftigt
2. Entschlüsselung
3. Ursprüngliches Ziel der Kryptographie
4. Die älteste Verschlüsslungsart, die wir kennenlernten
5. Verschlüsselungsart, die nach einem römischen Kaiser benannt ist
6. Hilft um z.B. die Verbesserung der Caesar-Verschlüsselung zu knacken
7. Hilfsmittel bei der Vigenere-Verschlüsselung
8. Name der Verschlüsselungsmaschine, die im zweiten Weltkrieg verwendet wurde
9. Polyalphabetische Form der Caesar-Verschlüsselung
10. Verschlüsselungsart mit Pergament und Holzstab
11. Erfinder der Maschine, die die Enigma knackte
12. Elemente der Enigma, die sich nach jeder Tastenbetätigung verändern
13. Klartext: "treffpunkt", schlüssel "zwei" (Vigenere)
14. Geheimtext: "sgfsqymotf" (Caesar)

1	2	3		4	5	6	7	8	9	10	11	12		13	14	15	16

Das Lösungswort ist ein Film, den du dir unbedingt ansehen solltest!

4.3 Eine neue Ära

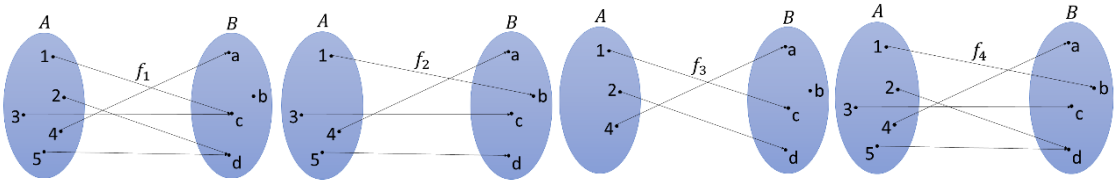
Mit der Erfindung des Computers kamen auch neue Anforderungen an die Verschlüsselungstechnik und so in den 1970er Jahren auch eine ganz neue Art von Verschlüsselung. Lies dir dazu *Kapitel 3.4: „Asymmetrische Verschlüsselung“* durch.

4.3.1 Wohin gehen die Pfeile?

Um diese neue Art der Verschlüsselungen verstehen zu können, benötigen wir mathematisches Wissen über bestimmte Eigenschaften von Funktionen. Löse folgende Aufgaben mithilfe von *Kapitel 3.5.2: „Funktionen: Injektivität, Surjektivität und Bijektivität“.*

Aufgabe 9: Ordne die Eigenschaften zu den passenden Abbildungen der Funktionen zu. Begründe deine Zuordnungen.

weder injektiv, noch surjektiv	injektiv, aber nicht surjektiv	surjektiv, aber nicht injektiv	bijektiv
☐	☐	☐	☐
☐	☐	☐	☐



Aufgabe 10: Sind die Funktionen injektiv, surjektiv oder bijektiv? Begründe deine Antworten.

- $f_1: \mathbb{R} \to [-1,1], f_1(x) = \sin(x)$
- $f_2: \mathbb{N} \to \mathbb{N}, f_2(x) = x^2$
- $f_3: \mathbb{R} \to \mathbb{R}, f_3(x) = 4x - 2$
- $f_4: \mathbb{R} \to \mathbb{R}, f_4(x) = x^5 - 6x + 3$

Übung 7: Überleg dir je ein Beispiel für eine Funktion, die

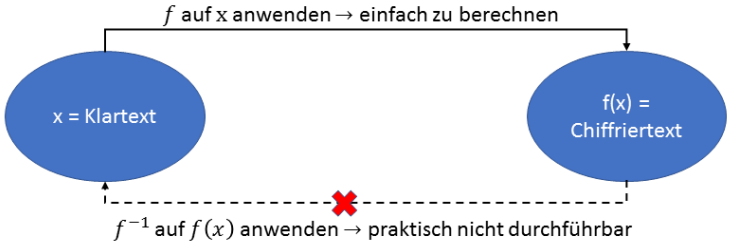
- weder injektiv, noch surjektiv ist.
- injektiv, aber nicht surjektiv ist.
- surjektiv, aber nicht injektiv ist.
- bijektiv ist.

Tauscht eure Beispiele mit denen eurer Nachbarn aus und versucht sie den Eigenschaften richtig zuzuordnen.

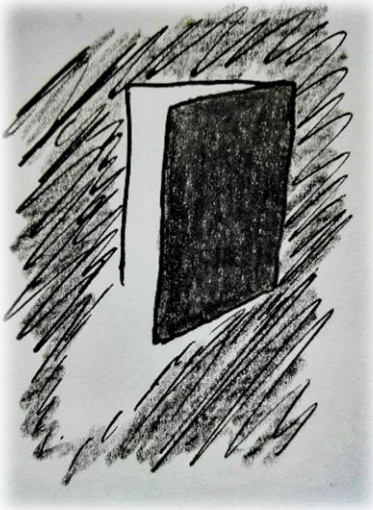
4.3.2 Hintertüren, Schnappschlösser und Briefkästen

Für die Ver- und Entschlüsselung bei asymmetrischen Verfahren werden Funktionen und ihre Umkehrfunktionen verwendet. Wir wollen, dass die Verschlüsselung einfach zu berechnen ist, die Umkehrfunktion aber nicht. Deshalb suchen wir eine Funktion, die einfach zu berechnen ist, mit einer Umkehrfunktion, die nicht schnell berechenbar ist. So eine Funktion nennt man Einwegfunktion. Eine exakte Definition dafür sehen wir im Theorieskript in *Kapitel 3.4.1: „Einwegfunktionen und Einwegfunktionen mit einer Hintertür“*.

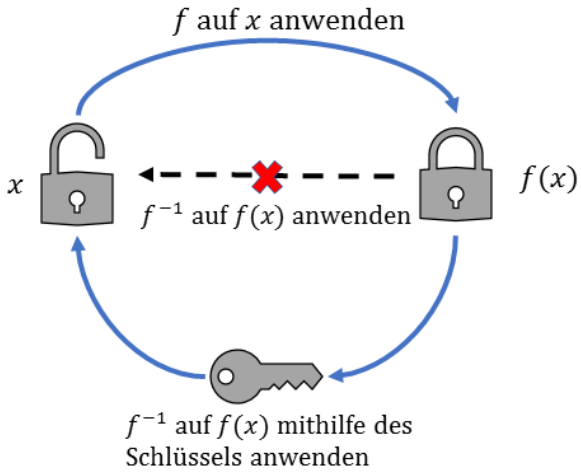
Eine Einwegfunktion könnte grafisch folgendermaßen dargestellt werden:



Das heißt, wenn wir eine Einwegfunktion zur Verschlüsselung verwenden würden, gäbe es gar keine Möglichkeit mehr den Klartext aus dem Chiffriertext zu entschlüsseln. Das ist natürlich auch nicht Sinn der Sache. Für die Empfängerin oder den Empfänger der Nachricht soll es möglich sein, den Klartext aus dem Chiffriertext zu ermitteln. Deshalb brauchen wir eine Hintertür. Die Hintertür soll es möglich machen die Nachricht zu entschlüsseln, allerdings nur für die gewünschten Adressaten. Das Wissen, wo sich diese Hintertür befindet, also wie man den Klartext aus dem Chiffriertext berechnen kann, bildet den privaten Schlüssel der Empfängerin bzw. des Empfängers. Die exakte Definition ist wieder im Theorieskript zu finden.



Aufgabe 11: Stelle die Einwegfunktion mit einer Hintertür (wie oben die Einwegfunktion) grafisch dar.



Veranschaulichen lässt sich die Einwegfunktion mit einer Hintertür an einem Schnappschloss: Die Funktion f beschreibt das Schließen des Schlosses. Es kann ohne großen Aufwand von jedem geschlossen werden. Der Schlüssel des Schlosses stellt die Hintertür, bzw. das Geheimnis dar. Eine Person, die den Schlüssel nicht besitzt, kann das Schloss, wenn es sicher genug ist, nicht einfach öffnen. Wenn man den Schlüssel hat, lässt es sich aber leicht und ohne Zeitaufwand öffnen. Dabei stellt die Öffnung des Schlosses die Anwendung der Umkehrfunktion f^{-1} dar. (Vgl. Freiermuth, Hromkovic, Keller, & Steffen, 2010, S. 239f)

Aufgabe 12: Als anderes anschauliches Beispiel für eine Einwegfunktion mit einer Hintertür könnte auch ein Briefkasten verwendet werden. Beschrifte und erkläre das Bild wie oben:

_____

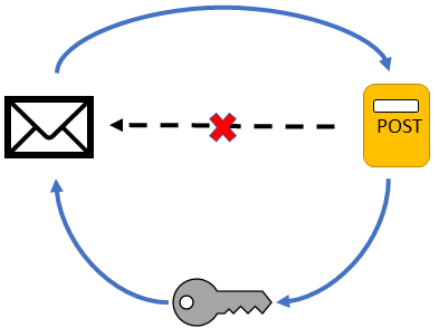
_____

_____

_____

_____

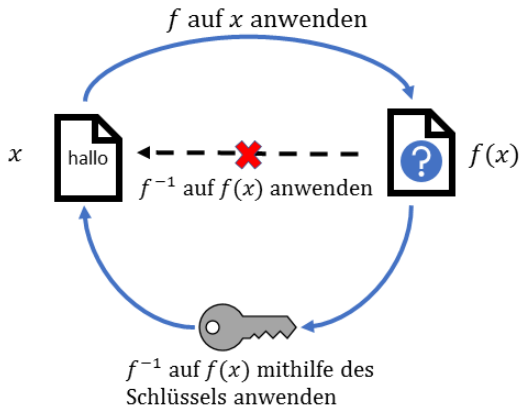
_____



Übung 8: Fallen dir noch andere Vergleiche aus dem täglichen Leben ein, die eine Einwegfunktion mit einer Hintertür darstellen? Diskutiere mit einer Kollegin oder einem Kollegen, ob eure Beispiele passend gewählt sind, oder es sich um doch keine Einwegfunktionen mit einer Hintertür handelt.

4.3.3 Was hat das alles mit asymmetrischer Verschlüsselung zu tun?

Für das Konzept der asymmetrischen Verschlüsselung verwenden wir die Einwegfunktion mit einer Hintertür genau wie oben, nur dieses Mal um eine Nachricht zu verschlüsseln. Bob kann die Funktion f veröffentlichen (= Bobs öffentlicher Schlüssel), sodass ihm jede und jeder eine verschlüsselte Nachricht senden kann. Nur er hat jedoch seinen privaten Schlüssel, nämlich genau den Schlüssel, mit dem er aus dem Chiffriertext $f(x)$ wieder die Klartextnachricht x erhalten kann. Lies *Kapitel 3.4.2: „Das Konzept der Public-Key-Kryptographie“.*



Aufgabe 13: Wie viele Schlüssel bzw. Schlüsselpaare würden mit symmetrischer und mit asymmetrischer Verschlüsselung jeweils für ein Netzwerk mit 1000 Personen benötigt werden?

Aufgabe 14: Angenommen es können genau 1999000 Schlüssel bzw. 999500 Schlüsselpaare verwendet werden, wie viele Personen können bei symmetrischer bzw. bei asymmetrischer Verschlüsselung jeweils im Netzwerk tätig sein?

4.3.4 Wieder im Kindergarten: Wir dividieren!

Lies *Kapitel 3.5.1.1: „Teilbarkeit, Division mit Rest“* und *3.5.1.2: „Größter gemeinsamer Teiler“*. Das meiste sollte dir schon bekannt sein, allerdings sind hier die exakten mathematischen Definitionen und Beweise gegeben.

Wir benötigen jetzt die Division mit Rest, d.h. du dividierst zwei ganze Zahlen und wenn du normalerweise ein Komma an deine Ergebniszahl hängst, um weiterzurechnen, schreibst du dir stattdessen einfach den Rest auf.
Zum Beispiel ergäbe die Division mit Rest für $5:2=2$ mit Rest 1. Das heißt, wir wissen nun dass $5\ div\ 2=2$ und $5\ mod\ 2=1$.
Ein schwierigeres Beispiel wäre

1	**9**	**6**	**3**	**4**	**2**	**:**	**1**	**3**	**=**	**1**	**5**	**1**	**0**	**3**
	6	6												
	0	1	3											
		0	0	4										
			0	4	2									
					3	**Rest**								

Anhand dieser Rechnung erfahren wir, dass $196342\ div\ 13=15103$ und $196342\ mod\ 13=3$.

Aufgabe 15: Führe für folgende Zahlen die Division mit Rest für $a:b$ durch und bestimme jeweils $a\ div\ b$ und $a\ mod\ b$:

a) $a=294, b=34$
b) $a=2453, b=5$
c) $a=4935, b=957$

Mit der Division mit Rest können wir jetzt den Euklidischen Alogrithmus durchführen:

$ggT(1076,572)$

$$1076=1\cdot 572+504$$
$$572=1\cdot 504+68$$
$$504=7\cdot 68+28$$
$$68=2\cdot 28+12$$
$$28=2\cdot 12+4$$
$$12=3\cdot 4+0$$

$$ggT(1076,572)=4$$

Für $ggT(a,b)$ wird also die Division mit Rest durchgeführt, sodass man $a = qb + r$ erhält. Dann berechnest du die Division mit Rest von b und r und so weiter. Der letzte Rest, der nicht 0 ist, ist dann der $ggT(a,b)$.

Aufgabe 16: Verwende den Euklidischen Algorithmus für folgende Beispiele:

a) $ggT(75,65)$
b) $ggT(729,612)$
c) $ggT(3043,2913)$
d) $ggT(1045,19)$
e) $ggT(10501,2938)$

Der Erweiterte Euklidische Algorithmus beschafft uns dann eine Darstellung des ggT als

$$ggT(a,b) = x \cdot a + y \cdot b \text{ mit } x,y \in \mathbb{Z}.$$

Wie funktioniert der Erweiterte Euklidische Algorithmus?
Wenn wir zum Beispiel die Zahlen 1076 und 572 gegeben haben, und den Erweiterten Euklidischen Algorithmus durchführen wollen, müssen wir zuerst den „normalen" Euklidischen Algorithmus verwenden. Den haben wir für diese Zahlen weiter oben schon berechnet. Allerdings schreiben wir uns jetzt bei jeder Zeile daneben, wie der erhaltene Rest, durch die anderen Zahlen ausgedrückt werden könnte:

$1076 = 1 \cdot 572 + 504$	$\Rightarrow$	$504 = 1076 - 1 \cdot 572$
$572 = 1 \cdot 504 + 68$	$\Rightarrow$	$68 = 572 - 1 \cdot 504$
$504 = 7 \cdot 68 + 28$	$\Rightarrow$	$28 = 504 - 7 \cdot 68$
$68 = 2 \cdot 28 + 12$	$\Rightarrow$	$12 = 68 - 2 \cdot 28$
$28 = 2 \cdot 12 + 4$	$\Rightarrow$	$4 = 28 - 2 \cdot 12$
$12 = 3 \cdot 4$		

Wir starten jetzt ganz unten mit dem Term $4 = 28 - 2 \cdot 12$ und ersetzen im ersten Schritt die Zahl 12 durch die vorletzte Zeile $12 = 68 - 2 \cdot 28$. Das fassen wir passend zusammen und ersetzen danach die Zahl 28 durch den Term der 3. Zeile von unten: $28 = 504 - 7 \cdot 68$ und so weiter:

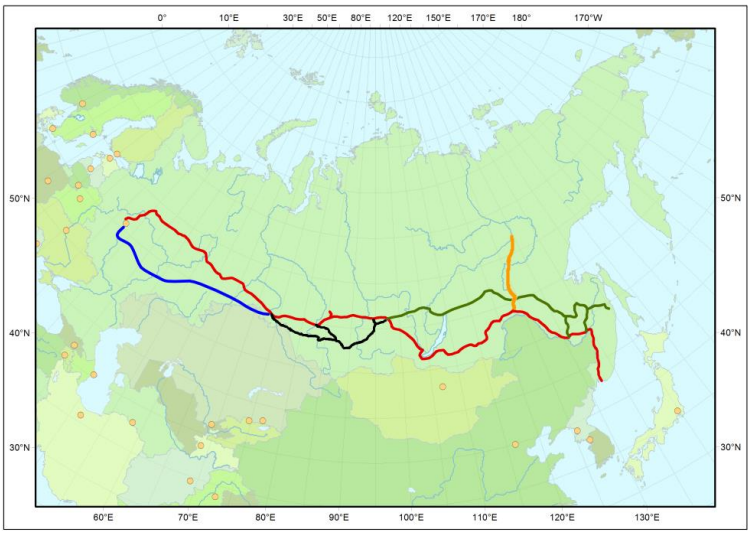
$$4 = 28 - 2 \cdot 12$$
$$4 = 28 - 2 \cdot (68 - 2 \cdot 28) \Leftrightarrow 4 = 5 \cdot 28 - 2 \cdot 68$$
$$4 = 5 \cdot (504 - 7 \cdot 68) - 2 \cdot 68 \Leftrightarrow 4 = 5 \cdot 504 - 37 \cdot 68$$
$$4 = 5 \cdot 504 - 37 \cdot (572 - 1 \cdot 504) \Leftrightarrow 4 = 42 \cdot 504 - 37 \cdot 572$$
$$4 = 42 \cdot (1076 - 1 \cdot 572) - 37 \cdot 572 \Leftrightarrow \mathbf{4 = 42 \cdot 1076 - 79 \cdot 572}$$

Diese Darstellung der Zahlen wird auch Vielfachsummendarstellung genannt. Das Lemma von Bézout besagt, dass zu allen $a, b \in \mathbb{N}$ so eine Darstellung existiert. Die genaue Formulierung des Lemmas findest du im Theorieskript im *Kapitel 3.5.1.3: „Euklidischer Algorithmus und Erweiterter Euklidischer Algorithmus“*.

Aufgabe 17: Verwende den Erweiterten Euklidischen Algorithmus für folgende Beispiele:

a) 75 und 65
b) 729 und 612
c) 3043 und2913
d) 1045 und 19
e) 10501 und 2938

4.3.5 Die längste Eisenbahn der Welt

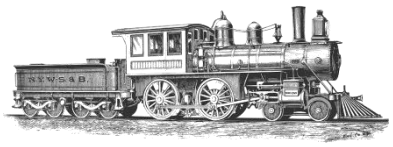


Die längste Eisenbahn der Welt ist die Transsibirische Eisenbahn. Die nicht ganz 10000 km lange Strecke geht durch Sibirien und verbindet Moskau mit dem Pazifik.
Fülle den leicht vereinfachten Fahrplan der Eisenbahn fertig aus:

STATION	FAHRZEIT (IN STUNDEN)	UHRZEIT (IN MOSKAU)
MOSKAU	0	17:00
KIROW	12	5:00
JEKATERINBURG	26	
NOWOSIBIRSK	46	
KRASNOJASK	58	
IRKUTSK	77	
BIROBIDSCHAN	133	
WLADIWOSTOK	149	

(Vgl. Becker, 2014)

Wie hast du die Uhrzeiten berechnet? Wie berechnet man z.B. die Uhrzeit, wenn seit 17 Uhr 77 Stunden vergangen sind?



Hätten wir z.B. den Ausgangspunkt 15:00 und wollen wissen, wie spät es in zwei Stunden ist, würden wir einfach $15 + 2 = 17$ rechnen und wissen, dass es dann 17 Uhr sein wird. Wenn wir aber $17 + 77 = 94$ rechnen, ergibt 94 Uhr keine sinnvolle Antwort.

Was wir tun könnten, wäre $77 : 24 \approx 3{,}208$ auszurechnen. Dann wissen wir also dass 3 Tage ($= 3 \cdot 24 = 72$ Stunden) vergehen und dann noch 5 Stunden ($77 - 72 = 5$) übrig bleiben. Also rechnen wir $17 + 5 = 22$ und erhalten als Ergebnis 22 Uhr.
Schneller wären wir, wenn wir statt der Division $77 : 24 \approx 3{,}208$ gleich die Division mit kleinstem Rest durchführen und $77 : 24 = 3$ mit Rest 5 erhalten – dann achten wir nur auf den Rest und können diesen zur Uhrzeit addieren. Das heißt wir verwenden eigentlich die modulo-Operation.

Wenn der Zug verspätet abfährt und die Ausgangsuhrzeit auf 21:00 verlegt wird, würden wir mit der gerade beschriebenen Rechnung $77\ mod\ 24 = 5$ und $21 + 5 = 26$, aber schon wieder eine ungültige Uhrzeit bekommen. Um die richtige Uhrzeit zu erhalten, müssten wir wieder $26\ mod\ 24 = 2$ rechnen.

Wenn wir zwei Zeiten auf diese Weise addieren, müssen wir also den zweiten Summand modulo 24 rechnen, das Ergebnis zum ersten Summand hinzufügen und dieses Ergebnis danach eventuell wieder modulo 24 rechnen. Eine andere Möglichkeit ist es, wenn wir die Summanden addieren und erst danach das Ergebnis modulo 24 rechnen:

$$(77 + 17)\ mod\ 24 = 94\ mod\ 24 = 22$$

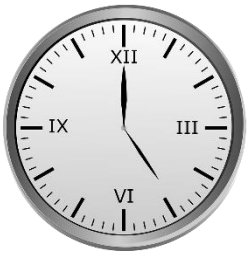
Diese Art der Addition heißt **modulare Addition**, die wir auch als $\mathbf{77} \oplus_{\mathbf{24}} \mathbf{17}$ schreiben.

Aufgabe 18: Berechne die Uhrzeiten aus dem Abfahrtsplan der Transsibirischen Eisenbahn erneut. Schreibe dazu die Rechnungen wie im Beispiel auf:

$$77 \oplus_{24} 17 = (77 + 17) mod\ 24 = 94\ mod\ 24 = 22$$

Aufgabe 19: Berechne die Ergebnisse:

a) $26 \oplus_{27} 26$
b) $0 \oplus_{14} 12$
c) $423 \oplus_{4} 214$
d) $1847 \oplus_{5} 23143$



Aufgabe 20:

a) Die Analoguhr zeigt 5 Uhr an. Welche Uhrzeit wird sie in 137 Stunden anzeigen?
b) Es ist Donnerstag. Welcher Wochentag ist in 102 Tagen?
c) Wenn jetzt Dezember ist, welchen Monat haben wir in 38 Monaten?

Um besser mit der Modularen Arithmetik umgehen zu können, brauchen wir einige Rechengesetze:

Es gilt, dass sich für Zahlen $z, a \in \mathbb{N}$ und $a > 0$ die Zahl $z \; mod \; a$ nicht verändert, wenn man vor der modulo-Rechnung ein Vielfaches von a zu z hinzuzählt.

Wenn z.B. $94 \; mod \; 24 = 22$, dann ist auch $(94 + 24) \; mod \; 24 = 22$. Es ist als würdest du zur Uhrzeit einen ganzen Tag hinzuzählen, das ändert natürlich die Uhrzeit nicht. Wenn es nach 94 Stunden 22 Uhr ist, dann muss es auch nach 94 Stunden + einen Tag 22 Uhr sein. Auch nach 94 Stunden + $2,3$ oder 125 Tagen ist es 22 Uhr.

Dieses Rechengesetz nennen wir **M1**.

Wenn wir den Fahrplan der Transsibirischen Eisenbahn noch einmal betrachten, sehen wir, dass es sowohl nach 77 gefahrenen Stunden, wie auch nach 149 Stunden, 22 Uhr ist. Zwischen 77 und 149 liegen 72 Stunden ($= 149 - 77$), was ein Vielfaches von 24 ($3 \cdot 24 = 72$) ist, weshalb nach **M1** klar ist, dass es dasselbe Ergebnis sein muss. Auf der Strecke von Irkutsk nach Wladiwostok vergehen genau 3 Tage.

Aufgabe 21:

a) Berechne $516 \; mod \; 13$ und $(516 + 26) \; mod \; 13$.
b) Berechne $1601 \; mod \; 16$.

Wenn du eine Aufgabe wie Aufgabe 20: b) bearbiten musst, kannst du statt $(1601 \; mod \; 16)$, $(1 + 1600) \; mod \; 16$ schreiben. 1600 ist klarerweise ein Vielfaches von 16, und $1 \; mod \; 16 = 1$. Aus **M1** folgt dann, dass $(1601 \; mod \; 16) = 1$.

Das zweite Rechengesetz zum modularen Rechnen haben wir eigentlich schon kennengelernt, wir haben es nur nicht als solches bezeichnet. Und zwar besagt **M2**, dass es keinen Unterschied macht, ob man die Summanden bei der modularen Addition zuerst zusammenzählt, und dann modulo rechnet, oder die beiden Summanden einzeln modulo rechnet, zusammenzählt und das Ergebnis wieder modulo rechnet.

Wir können z.B. die Rechnung $514 \; \oplus_{13} \; 425$ auf zwei Arten berechnen:

- $514 \; \oplus_{13} \; 425 = (514 \; mod \; 13 + 425 \; mod \; 13) \; mod \; 13 = (7 + 9) \; mod \; 13 = 16 \; mod \; 13 = 3$
- $514 \; \oplus_{13} \; 425 = (514 + 425) \; mod \; 13 = 939 \; mod \; 13 = \; 3$

Auch wenn die erste Art vielleicht etwas länger und nach mehr Schreibarbeit aussieht, kann es sehr hilfreich sein, diese Methode bei größeren Zahlen anzuwenden, da dann innerhalb der Rechnung die Zahlen immer kleiner bleiben. Vor Allem, wenn man keinen Taschenrechner zur Verfügung hat, ist die erste Methode oft angenehmer.

Aufgabe 22: Berechne folgende Aufgaben jeweils auf zwei unterschiedliche Arten:

a) $5403 \oplus_6 1934$
b) $1702 \oplus_{17} 34$
c) $25437 \oplus_{23} 282833$

Die modulare Multiplikation funktioniert analog zur modularen Addition. Ein Beispiel:

$$15 \odot_4 6 = (15 \cdot 6)\ mod\ 4 = 90\ mod\ 4 = 2$$

Analog zum zweiten Rechengesetz für modulares Rechnen, gibt es auch für die Multiplikation ein Gesetz **M3**, das besagt, dass die beiden Zahlen vor der Multiplikation modulo berechnet werden können und das Ergebnis dadurch nicht verändert wird.

Wir können z.B. die Rechnung $514 \odot_{13} 425$ wieder auf zwei Arten berechnen:

- $514 \odot_{13} 425 = (514\ mod\ 13 \cdot 425\ mod\ 13)\ mod\ 13 = (7 \cdot 9)\ mod\ 13 = 63\ mod\ 13 = 11$
- $514 \odot_{13} 425 = (514 \cdot 425)\ mod\ 13 = 218450\ mod\ 13 = 11$

Dass das Gesetz M3 verwendet werden darf, ist klar, da wir einfach schon während der Berechnung möglichst viele „13-Pakete“ subtrahieren, was natürlich den gleichen 13-Rest ergibt, also das Ergebnis der modulo-Rechnung nicht verändert.

Aufgabe 23: Berechne folgende Aufgaben jeweils auf zwei unterschiedliche Arten:

a) $5403 \odot_6 1934$
b) $1702 \odot_{17} 34$
c) $25437 \odot_{23} 282833$

4.3.6 Quadrate und Wurzeln

Auch beim modularen Rechnen kann man modular quadrieren und modular multiplizieren – wir müssen aber aufpassen, für 0 ist das modulare Quadrat nicht definiert!

Zum Beispiel sehen die **modularen Quadrate** für die Rechenoperation $\odot_8$ so aus:

$$1 \odot_8 1 = 1^2 mod\ 8 = 1$$
$$2 \odot_8 2 = 2^2 mod\ 8 = 4$$
$$3 \odot_8 3 = 3^2 mod\ 8 = 1$$
$$4 \odot_8 4 = 4^2 mod\ 8 = 0$$
$$5 \odot_8 5 = 5^2\ mod\ 8 = 1$$
$$6 \odot_8 6 = 6^2\ mod\ 8 = 4$$
$$7 \odot_8 7 = 7^2 mod\ 8 = 1$$

Alle Zahlen ≥ 8 können zuerst $mod\ 8$ gerechnet werden und so auf eine der Zahlen $0 - 7$ gebracht werden, also reicht es, wenn wir uns die Quadrate von $0 - 7$ ansehen, um alle Lösungen für Quadrate der Operation $\odot_8$ zu erhalten. Nur die Zahlen $0, 1$ und 4 sind Quadrate dieser Zahlen.

D.h. jede Zahl hat ein modulares Quadrat aber nicht jede Zahl ist ein modulares Quadrat einer Zahl.

Aufgabe 24: Berechne alle modularen Quadrate

a) $mod\ 6$
b) $mod\ 11$

Die **modulare Wurzel** einer Zahl ist ebenfalls analog zur uns bekannten Wurzel einer Zahl definiert. Z.B. ist 3 eine modulare Wurzel von 1 bezüglich $mod\ 8$, weil $3^2\ mod\ 8 = 1$. Wie wir im Beispiel schon sehen, kann aber eine Zahl mehrere modulare Wurzeln haben, z.B. hat 1 bezüglich $mod\ 8$ die Wurzeln $1, 3, 5$ und 7. Z.B. die Zahl 2 hat $mod\ 8$ aber gar keine modulare Wurzel.

Aufgabe 25: Berechne die modularen Wurzeln von

a) 2 bzgl. $mod\ 7$
b) 1 bzgl. $mod\ 9$

4.3.7 Ron Rivest, Adi Shamir und Len Adleman

„1977 nahmen die drei Personen, die den spektakulärsten Einzelbeitrag zur Public-Key-Kryptographie leisten sollten, Ronald Rivest, Adi Shamir und Leonard Adleman, die Herausforderung an und produzierten ein alle Erwartungen erfüllendes Public-Key-Kryptosystem. Der Prozess dauerte mehrere Monate, während derer Rivest Vorschläge machte, Adleman sie angriff und Shamir sich erinnert, zu beidem beigetragen zu haben. Im Mai 1977 wurden sie mit Erfolg gekrönt. Sie hatten entdeckt, wie ein einfaches Stück klassischer Zahlentheorie benutzt werden kann, um das Problem zu lösen.“ (Diffie zitiert nach Beutelspacher, Kryptologie: Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen, 2007, S. 101)

Der Name RSA leitet sich von den Anfangsbuchstaben der Erfinder ab.

RSA verwendet das Problem der Primfaktorzerlegung, um die Verschlüsselung sicher zu machen. Primzahlen zu multiplizieren ist effektiv berechenbar, allerdings ist es praktisch nicht lösbar für eine gegebene große Zahl die Primfaktoren zu berechnen. Es gibt aber kein Geheimnis, mit dem die Primfaktorzerlegung leichter zu lösen wäre, weshalb das nicht direkt die Verschlüsselung darstellt. (Vgl. Freiermuth, Hromkovic, Keller, & Steffen, 2010, S. 289f)

4.3.8 Wir verwenden RSA!

Als letzten Schritt, bevor wir nun endlich den RSA-Algorithmus verwenden können, müssen wir noch eine mathematische Funktion kennenlernen: Die **Euler'sche Phi-Funktion**.

$\phi(n)$ = die Anzahl der Zahlen, die teilerfremd zu n und $\leq n$ sind

n	$\phi(n)$	Zahlen, die $\leq n$ und teilerfremd zu n sind
1	1	1
2	1	1
3	2	1,2
4	2	1,3
6	2	1,5
10	4	1,3,7,9
15	8	1,2,4,7,8,11,13,14

Aufgabe 26: Berechne $\phi(n)$ für folgende Werte:

a) $n = 7$
b) $n = 18$
c) $n = 21$

Das Berechnen von $\phi(n)$ wird bei größeren Zahlen schnell anstrengend bzw. zeitintensiv. Zum Glück gibt es für Primzahlen Regeln, die die Berechnung sehr vereinfachen:

$\phi(p) = p - 1$ für eine Primzahl p
$\phi(p \cdot q) = (p - 1) \cdot (q - 1)$ für zwei verschiedene Primzahlen[24] p und q

Aufgabe 27: Berechne $\phi(n)$ für folgende Werte:

a) $n = 41$
b) $n = 77$
c) $n = 143$

[24] Siehe Kapitel 3.5.5: „Ein Satz von Euler" für den Beweis.

Jetzt können wir den RSA-Algorithmus verwenden:

Wie bekommt Bob nun einen privaten und einen öffentlichen Schlüssel?
Wir wenden die theoretische Anleitung aus *Kapitel 3.4.3.1: „Schlüsselerzeugung“* in einem praktischen Beispiel an:

Bob wählt $\boldsymbol{p = 3}$ und $\boldsymbol{q = 11}$. Dann erhält er $\boldsymbol{n = p \cdot q = 3 \cdot 11 = 33}$
und $\boldsymbol{\phi(n) = \phi(p \cdot q) = (p-1)(q-1) = 2 \cdot 10 = 20}$.
e kann z.B. als $\boldsymbol{e = 3}$ gewählt werden (3 und 20 sind teilerfremd)
Jetzt wendet er den erweiterten Euklidischen Alorithmus auf $\phi(n) = 20$ und $e = 3$ an $\Rightarrow \underbrace{3}_{e} \cdot \underbrace{7}_{d} + \underbrace{(-1)}_{k} \cdot \underbrace{20}_{\phi(n)} = \underbrace{1}_{ggt(e,\phi(n))} \Leftrightarrow \underbrace{3}_{e} \cdot \underbrace{7}_{d} \; mod \; \underbrace{20}_{\phi(n)} = 1$
Sein öffentlicher Schlüssel ist also das Zahlenpaar $n = 33$ und $e = 3$. Bobs privater Schlüssel ist $d = 7$.

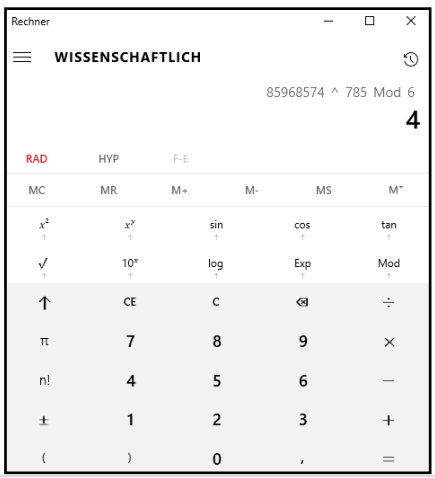
Wie verschlüsselt Alice die Nachricht, die sie an Bob senden will?
Auch hier ist die theoretische Ausführung im Theorieskript (*Kapitel 3.4.3.2: „Anwendung des RSA-Algorithmus“)* beschrieben. Wir machen im Beispiel von vorhin als Alice weiter:

Alice bekommet von Bob seine öffentlichen Schlüssel $n = 33$ und $e = 3$.
Nehmen wir an, Alice will die Klartextnachricht $m = 4$ versenden.
Sie berechnet $c = m^e \; mod \; n = 4^3 \; mod \; 33 = 64 \; mod \; 33 = 31$.
Diese Nachricht $c = 31$ versendet sie nun an Bob.

Was macht Bob, um die Nachricht wieder zu entschlüsseln?
Bob benutzt die im Theorieskript angegebene Formel:

Bob erhält von Alice die verschlüsselte Nachricht $c = 31$. Er verwendet außerdem seinen privaten Schlüssel $d = 7$:
$m_1 = c^d \; mod \; n = 31^7 mod \; 33 = 27512614111 \; mod \; 33 = 4$.
4 war auch die Klartextnachricht, die Alice verschlüsselte, also haben wir den Algorithmus richtig angewandt. ☺

Wie wir sehen, werden die Zahlen sehr schnell sehr groß, obwohl wir mit so kleinen Zahlen gestartet haben. Um solche große Zahlen modulo zu rechnen, eignet sich z.B. der in Windows vorinstallierte Taschenrechner sehr gut. Wenn man die wissenschaftliche Version des Rechners auswählt, kann man auch große Zahlen modulo rechnen, z.B. $85968574^{785} \; mod \; 6$:



Wie macht der Computer das?

Wir wissen bereits, dass wir z.B. bei der Rechnung $a^x \, mod \, p$ nicht unbedingt zuerst a^x berechnen müssen, sondern während dem Rechnen jedes Zwischenresultat modulo p berechnen können, um die Zahlen möglichst klein zu halten.

D.h. wir dürften folgendermaßen vorgehen:

$$a^x \, mod \, p = \underbrace{\big((a \, mod \, p) \cdot (a \, mod \, p) \cdot \ldots \cdot (a \, mod \, p)\big)}_{x \; Faktoren} \, mod \, p$$

Das wären dann also $x - 1$ Multiplikationen, die zu berechnen wären. Wenn die Zahl x sehr groß ist, kann es aber noch immer sein, dass es für den Computer zu viel Aufwand wäre auf diese Weise so viele Zahlen zu multiplizieren.

Darum verwendet der Computer einen zweiten Trick, um bei der Berechnung von modularen Potenzen Zeit zu sparen. Dazu sehen wir uns als Beispiel $x = 32$ an, d.h. wir brauchen a^{32}. Wenn man nun $\underbrace{a \cdot a \cdot \ldots \cdot a}_{32 \; Faktoren}$ berechnet, wären dazu 31 Multiplikationen nötig. Die Potenz kann aber auch anders dargestellt werden:

$$a^{32} = ((((a^2)^2)^2)^2)^2$$

Unter Verwendung dieser Eigenschaft, können wir a^{32} nun mit nur fünf Multiplikationen berechnen:

$$a^2 = a \cdot a$$
$$a^4 = a^2 \cdot a^2$$
$$a^8 = a^4 \cdot a^4$$
$$a^{16} = a^8 \cdot a^8$$
$$a^{32} = a^{16} \cdot a^{16}$$

Auch a^{40} kann auf diese Weise mit nur sechs statt 39 Multiplikationen berechnet werden:

Zuerst werden dieselben fünf Multiplikationen wie oben berechnet, und dann

$$a^{40} = a^{32} \cdot a^8$$

Der Computer verwendet zusätzlich noch einen Algorithmus, der ihm zeigt, welche Zwischenergebnisse er berechnen muss, um auf die gewünschte Zahl zu kommen. Wir Menschen können aber auch ohne diesen Algorithmus auf geeignete Werte kommen.

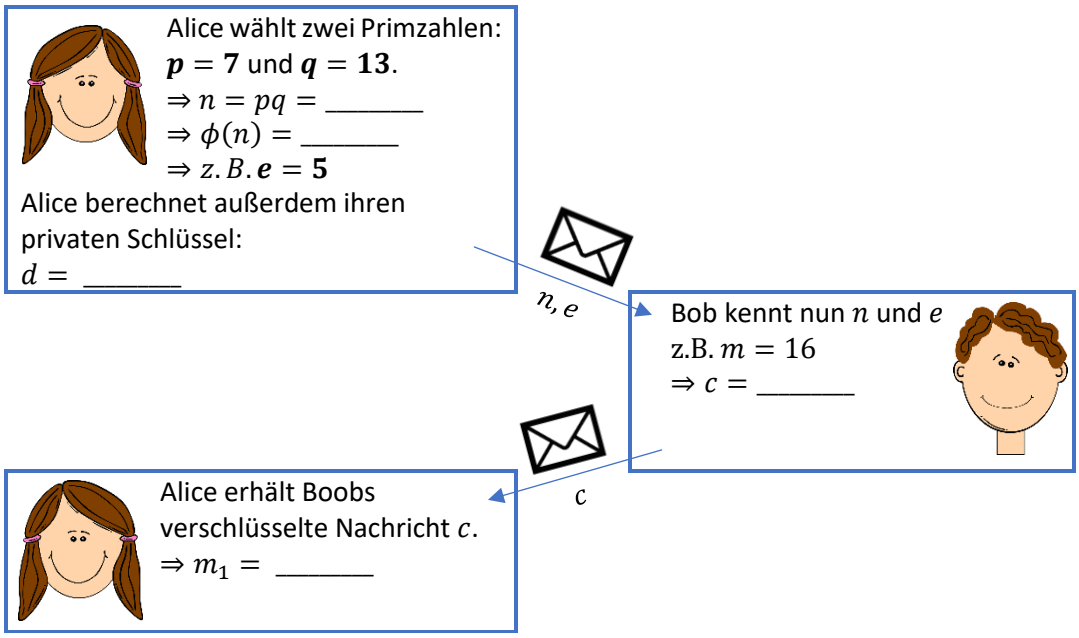
(Vgl. Freiermuth, Hromkovic, Keller, & Steffen, 2010, S. 201ff)

Aufgabe 28: Berechne folgenden Aufgaben wie oben:

a) a^{64} mit 6 Multiplikationen
b) a^{72} mit 7 Multiplikationen
c) a^{256} mit 8 Multiplikationen
d) a^{513} mit 10 Multiplikationen
e) a^{648} mit 11 Multiplikationen

In der Praxis wird beim RSA-Algorithmus natürlich schon mit sehr viel größeren Zahlen gestartet, d.h. die anfangs zu wählenden Primzahlen sind sehr viel größer. Für unsere Zwecke reicht es aber, wenn wir den Algorithmus mit kleineren Primzahlen verwenden, um zu sehen und zu verstehen, wie er funktioniert.

Aufgabe 29: Vervollständige folgende Darstellung einer RSA-Verschlüsselung:



Du wirst merken, dass bei richtiger Verwendung des RSA-Algorithmus immer $m = m_1$ gilt. Das ist ja auch wichtig, da das bedeutet, dass die Klartextnachricht wieder richtig entschlüsselt wurde. Wie immer in der Mathematik, dürfen wir aber nicht davon ausgehen, dass das immer zutrifft, nur weil es bei einigen Beispielen funktioniert.

Aufgabe 30: Berechne n, d, c und m_1, wenn folgende Werte vorgegeben sind:

a) $p = 3, q = 7, e = 5, m = 12$
b) $p = 13, q = 17, e = 19, m = 29$

Übung 8: Versuche mit einer Partnerin oder einem Partner ein Kommunikationsszenario mit RSA-Verschlüsselung durchzuspielen: Wechselt euch ab als sendende und empfangende Parteien. Gebt wirklich nur den öffentlichen Schlüssel bzw. die verschlüsselte Nachricht einander bekannt! Schafft ihr es wieder die richtige Klartextnachricht zu erhalten?

Um sicher gehen zu können, dass die RSA-Verschlüsselung wirklich funktioniert und sich immer die richtige Klartextnachricht aus dem Geheimtext entschlüsseln lässt, müssen wir formal beweisen, dass $m = m_1$ gilt.

Als Voraussetzung brauchen wir den so genannten Kleinen Satz von Fermat, mit dem wir einen Hilfssatz beweisen können, den wir dann schlussendlich für den Beweis der Korrektheit des RSA-Algorithmus benötigen.

Kleiner Satz von Fermat: „Für jede Primzahl p und jedes $a \in \mathbb{Z}\backslash\{0\}$ gilt
$a^{p-1} \; mod \; p = 1.$" (Freiermuth, Hromkovic, Keller, & Steffen, 2010, S. 301)

Der Beweis des Kleinen Satz von Fermat ist im Theorieskript im Kapitel 3.5.5: *„Ein Satz von Euler"* zu finden.

Hilfssatz: „Seien p und q zwei verschiedene Primzahlen und sei m eine natürliche Zahl $\leq pq$. Dann gilt für jede natürliche Zahl k:
$m^{k\cdot(p-1)\cdot(q-1)+1} \; mod \; p \cdot q = m.$"
(Beutelspacher, Kryptologie: Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen, 2007, S. 103)

Der Beweis des Hilfssatzes ist ebenfalls im Kapitel 3.5.5 angeführt.

Nun zum eigentlichen Beweis: Wir wollen zeigen, dass ein Klartext m, der mit dem oben beschriebenen RSA-Verfahrenen verschlüsselt und danach wieder zur Nachricht m_1 entschlüsselt wird, sich nicht verändert. Das heißt es soll $m = m_1$ gelten.

Beweis:

Die Formel zur Berechnung von m_1 ist

$$m_1 = c^d \ mod \ n.$$

Wir haben c mit der Formel $c = m^e \ mod \ n$ berechnet, die wir jetzt einsetzen können

$$m_1 = (m^e \ mod \ n)^d \ mod \ n.$$

Wegen (M3) können wir diesen Ausdruck folgendermaßen umformen

$$m_1 = (m^e)^d \ mod \ n.$$

Darauf können noch die Rechenregeln des Potenzierens angewendet werden

$$\boldsymbol{m_1 = m^{e \cdot d} \ mod \ n}.$$

Das heißt also es gilt $m_1 = m^{e \cdot d} \ mod \ n$, und wenn wir $m = m_1$ zeigen sollen, ist es gleichbedeutend dazu

$$m^{e \cdot d} \ mod \ n = m$$

zu zeigen.

Um die Korrektheit des RSA-Algorithmus zu zeigen, wollen wir jetzt überprüfen, ob der Term $m^{e \cdot d} \ mod \ n$ gleich dem Term m ist.

Bob hat e und d so gewählt, dass $e \cdot d = 1 + k \cdot \phi(n)$ gilt. Das können wir in den Term einsetzen:

$$\boldsymbol{m^{e \cdot d} \ mod \ n} = m^{1 + k \cdot \phi(n)} \ mod \ n$$

Bob hat außerdem n als $n = p \cdot q$ berechnet, wobei p und q zwei Primzahlen sind

$$m^{e \cdot d} \ mod \ n = m^{1 + k \cdot \phi(p \cdot q)} \ mod \ p \cdot q$$

Wegen der Eigenschaft der Euler'schen ϕ-Funktion, $\phi(p \cdot q) = (p - 1) \cdot (q - 1)$, wenn p und q Primzahlen sind, können wir schreiben

$$m^{e \cdot d} \ mod \ n = m^{1 + k \cdot (p-1) \cdot (q-1)} \ mod \ p \cdot q$$

Und aus unserem gerade bewiesenen Hilfssatz folgt dann

$$m^{e \cdot d} \ mod \ n = \boldsymbol{m}.$$

Somit ist die Nachricht m_1 nach der Dechiffrierung wieder dieselbe, wie die ursprüngliche Klartextnachricht m vor der Verschlüsselung.

(Vgl. Beutelspacher, Kryptologie: Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen, 2007, S. 111)

Aufgabe 1: Der gesuchte Chiffretext lautet „4145231113354243“. In lateinischen Buchstaben bedeutet der Name „Pythagoras“. Du hast z.B. schon den Satz des Pythagoras kennengelernt, der besagt, dass in einem rechtwinkeligen Dreieck die Kathetenquadrate zusammen so groß sind wie das Hypotenusenquadrat.

Aufgabe 2: Der Klartext lautet „ϵ ρ α τ ο σ θ ϵ ν η σ“, in lateinischen Buchstaben: „Eratosthenes“. Du hast in der Schule wahrscheinlich schon das „Sieb des Eratosthenes“ kennengelernt, das verwendet wird um die Primzahlen bis zu einer Zahl n zu finden.

Aufgabe 3: Nach der Verschlüsselung lautet der Text: „`hfjxfw hmnkkwj`“.

Aufgabe 4: Die Nachricht lautet: „`die ueberraschungsparty findet am samstag um acht uhr statt`“. Der Schlüssel, der verwendet wurde ist k = 7.

Aufgabe 5: In Klartext bedeutet die Nachricht: „`die verbesserung der caesar verschluesselung ist nicht mehr so einfach zu knacken`“
Der Schlüssel dazu sieht so aus:

a	b	c	d	e	f	g	h	i	k	l	m	n	o	r	s	t	u	v	z
m	*y*	*d*	*j*	*x*	*l*	*a*	*u*	*e*	*z*	*k*	*c*	*v*	*n*	*w*	*o*	*p*	*t*	*q*	*g*

Die Klartext-Buchstaben j, p, q, w, x, y und Chiffretext-Buchstaben b, f, h, i, r, s wurden weggelassen, da sie in der Nachricht nicht vorkommen und so auch nicht entschlüsselt werden konnten.
Wie kommt man darauf? Wenn du die Buchstaben zählst, merkst du, dass *x* deutlich öfter vorkommt als die anderen Buchstaben. Da *e* in deutschen Texten mit Abstand am öftesten vorkommt, können wir erraten, dass *e* als *x* chiffriert wurde. Dann sehen wir, dass von 3 Worten mit Länge 3 bei zweien ein *e* vorkommt. So kurze Wörter mit *e* werden sehr wahrscheinlich „der“, „die“, „des“, „dem“ oder „den“ sein. Da auch noch beide Wörter mit demselben Chiffrierbuchstaben, nämlich *j*, beginnen, können wir mit hoher Sicherheit sagen, dass *j* statt dem Buchstaben *d* eingesetzt wurde. Wir wissen jetzt, dass das erste Wort mit einem *d* beginnt, ein Buchstabe in der Mitte ist und mit einem *e* endet – da kann ja nur ein *i* in die Mitte passen. D.h. *i* wird im Geheimtext mit *e* ersetzt.
Dann können wir auch unsere gegebenen Hilfen verwenden: wir wissen, dass statt *c*, *d* im Text verwendet wurde. Es kommt insgesamt 5x *d* im Text vor, 3x davon mit dem gleichen Buchstaben danach (Kombination *du*). Im Theorieskript wurde das zwar nicht erwähnt, aber wir können erraten, dass normalerweise „ch“ (auch die Fälle mit „sch“ zählen hier dazu), die häufigste Kombination von *c* mit einem zweiten Buchstaben ist – *h* wurde also durch *u* ersetzt. Weitere Schritte:

- Wort „vedup“ = „nich_“: (nicht) *p* → *t*
- Wort „eop“ = „i_t“: (ist) *o* → *s*
- Wort „on“ = „s_“: (so) *n* → *o*
- 2x Wortanfang „qxw“ = „ve_“: (ver-) *w* → *s*
- …

Aufgabe 6:

- Der Geheimtext in der ersten Tabelle lautet `fttojqxizvoqwtlzi`.
- Der fehlende Klartext ist `dreiachtsiebensechs`.
- Der Schlüssel ist `nachricht`.

Aufgabe 7: Der Geheimtext ist `HHJBRJIVEMPTDRA`. Bei nochmaliger Anwendung desselben Schlüssels, ergibt sich wieder der Klartext `ARTHURSCHERBIUS`. Das heißt, man verwendet dieselben Schlüsseleinstellungen für die Ver- und Entschlüsselung, man muss also nicht zwischen den beiden Verfahren unterscheiden.

Aufgabe 8: Es entsteht der Klartext `TURINGBOMBE`.

Kreuzworträtsel:

1. Kryptanalyse
2. Dechiffrierung
3. Vertraulichkeit
4. Polybios
5. Caesar
6. Haeufigkeitsverteilung
7. Vigenere Quadrat
8. Enigma
9. Vigenere
10. Skytale
11. Turing
12. Rotationsscheiben
13. sninelyvjp
14. gutgemacht

Lösungswort: The Imitation Game

Aufgabe 9:

weder injektiv, noch surjektiv	injektiv, aber nicht surjektiv	surjektiv, aber nicht injektiv	bijektiv
f_1	f_3	f_4	f_2

Aufgabe 10:

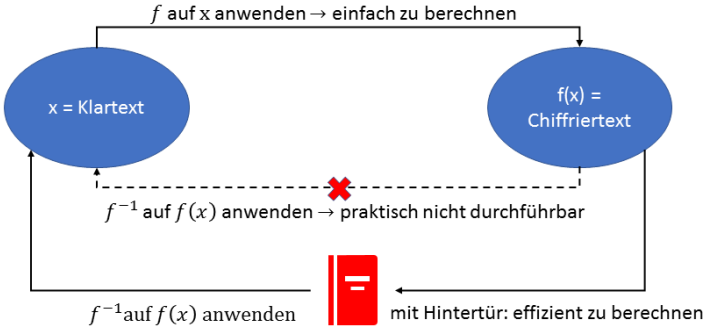
f_1 surjektiv, da $\sin(x)$ alle Werte in [-1,1] annimmt, aber nicht injektiv, weil z.B. $\sin(\pi) = \sin(3\pi) = 180°$

f_2 injektiv, weil die Quadrate natürlicher Zahlen nie gleich sind, aber nicht surjektiv, weil z.B. $\nexists x \in \mathbb{N}: x^2 = 2$.

f_3 bijektiv, die Umkehrfunktion ist $f_3^{-1}: \mathbb{R} \to \mathbb{R}, f_3^{-1}(x) = \frac{x+2}{4}$.

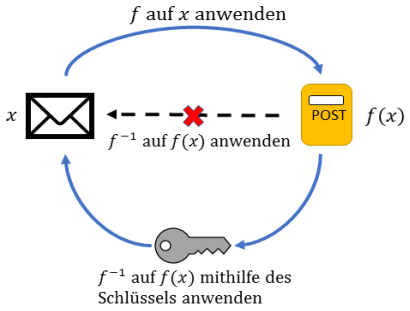
f_4 surjektiv, aber nicht injektiv, weil $f(0) = f(-1.57) = f(1.57) = 3$

Aufgabe 11:



Aufgabe 12:

Die Funktion f beschreibt das Einwerfen eines Briefes In den Briefkasten. Die Umkehrfunkton f^{-1}beschreibt Das Öffnen des Briefkastens.Der Briefkasten lässt sich Nur mit Schlüssel öffnen, also kommen nur Personen, die einen Schlüssel besitzen, zum Brief.



Aufgabe 13: Bei 1000 Personen braucht man mit asymmetrischer Verschlüsselung genau 1000 Schlüsselpaare, also 2000 Schlüssel.
Mit symmetrischer Verschlüsselung werden $\frac{n\cdot(n-1)}{2} = \frac{1000\cdot 999}{2} = 499500$

Aufgabe 14: Bei 1999000 Schlüsseln bzw. 999500 Schlüsselpaaren können 999500 Personen dem Netzwerk angehören, wenn es asymmetrisch verschlüsselt wird. Wenn es symmetrisch verschlüsselt wird, können 2000 Personen im Netzwerk sein, da $\frac{2000\cdot 1999}{2} = 1999000$

Aufgabe 15:
a) $294 : 34 = 8$ Rest $22, 294\ div\ 34 = 8, 294\ mod\ 34 = 22$
b) $2453 : 5 = 490$ Rest $3, 2453\ div\ 5 = 290, 2453\ mod\ 5 = 3$
c) $4935 : 957 = 5$ Rest $150, 4935\ div\ 957 = 5, 4935\ mod\ 957 = 150$

Aufgabe 16:

a) $ggT(75, 65) = 5$
b) $ggT(729, 612) = 9$
c) $ggT(3043, 2913) = 1$
d) $ggT(1045, 19) = 19$
e) $ggT(10501, 2938) = 1$

$$
\begin{aligned}
3043 &= 1\cdot 2913 + 130 && \Rightarrow && 130 = 3042 - 1\cdot 2913\\
2913 &= 22\cdot 130 + 53 && \Rightarrow && 53 = 2913 - 22\cdot 130\\
130 &= 2\cdot 53 + 24 && \Rightarrow && 24 = 130 - 2\cdot 53\\
53 &= 2\cdot 24 + 5 && \Rightarrow && 5 = 53 - 2\cdot 24\\
24 &= 4\cdot 5 + 4 && \Rightarrow && 4 = 24 - 4\cdot 5\\
5 &= 1\cdot 4 + \mathbf{1} && \Rightarrow && 1 = 5 - 1\cdot 4\\
4 &= 4\cdot 1 + 0
\end{aligned}
$$

Aufgabe 17:

a) $-6\cdot 75 + 7\cdot 65 = 5$
b) $21\cdot 729 - 25\cdot 612 = 9$
c) $-605\cdot 3043 + 632\cdot 2913 = 1$
d) $0\cdot 1045 + 1\cdot 19 = 19$
e) $1031\cdot 10501 - 3685\cdot 2938 = 1$

$$
\begin{aligned}
1 &= 5 - 1\cdot 4\\
1 &= 5 - 1\cdot(24 - 4\cdot 5) = -1\cdot 24 + 5\cdot 5\\
1 &= -1\cdot 24 + 5\cdot(53 - 2\cdot 24) = 5\cdot 53 - 11\cdot 24\\
1 &= 5\cdot 53 - 11\cdot(130 - 2\cdot 53) = -11\cdot 130 + 27\cdot 53\\
1 &= -11\cdot 130 + 27\cdot(2913 - 22\cdot 130) = 27\cdot 2913 - 605\cdot 130\\
1 &= 27\cdot 2913 - 605\cdot(3042 - 1\cdot 2913) = \mathbf{-605\cdot 3043 + 632\cdot 2913}
\end{aligned}
$$

Aufgabe 18:

STATION	FAHRZEIT (IN STUNDEN)	UHRZEIT (IN MOSKAU)
MOSKAU	0	17:00
KIROW	12	5:00
JEKATERINBURG	26	19:00
NOWOSIBIRSK	46	15:00
KRASNOJASK	58	3:00
IRKUTSK	77	22:00
BIROBIDSCHAN	133	6:00
WLADIWOSTOK	149	22:00

Aufgabe 19:

a) $26 \oplus_{27} 26 = (26 + 26) mod\ 27 = 52\ mod\ 27 = 25$
b) $0 \oplus_{14} 12 = (0 + 12)\ mod\ 14 = 12\ mod\ 14 = 12$
c) $423 \oplus_4 214 = (423 + 214)\ mod\ 4 = 1$
d) $1847 \oplus_5 23143 = (1847 + 23143)\ mod\ 5 = 0$

Aufgabe 20:

a) $5 \oplus_{12} 137 = (5 + 137)\ mod\ 12 = 10$
b) $0 \oplus_7 102 = (0 + 102)\ mod\ 7 = 4 \Rightarrow$ Donnerstag + 4 Tage = Montag
Es wäre auch möglich, die Wochentage mit Montag = 1, Dienstag = 2, usw. zu nummerieren, dann würde die Rechnung so aussehen:
$4 \oplus_7 102 = (4 + 102)\ mod\ 7 = 1 \Rightarrow 1 =$ Montag
c) Sei Jänner = 1, Februar = 2,…, Dezember = 12:
$12 \oplus_{12} 38 = (12 + 38)\ mod\ 12 = 2 \Rightarrow 2 = Februar.$

Aufgabe 21:

a) $516\ mod\ 13 = 9, (516 + 26)\ mod\ 13 = 9$
b) $1601\ mod\ 16 = (1600 + 1) mod\ 16 = 1$

Aufgabe 22:

a) $5403 \oplus_6 1934$ $(5403 + 1934) mod\ 6$
$= (5403\ mod\ 6 + 1934\ mod\ 6)\ mod\ 6$
$= (3 + 2)\ mod\ 6 = 5\ mod\ 6 = 5$
$(5403 + 1934)\ mod\ 6 = 7337\ mod\ 6 = 5$

b) $1702 \oplus_{17} 34$ $(1702 + 34)\ mod\ 17$
$= (1702\ mod\ 17 + 34\ mod\ 17)\ mod\ 17$
$= (2 + 0)\ mod\ 17 = 2\ mod\ 17 = 2$
$(1702 + 34)\ mod\ 17 = 1736\ mod\ 17 = 2$
$(1702 + 34)\ mod\ 17 =^{M1} 1702\ mod\ 17 =^{M1} 2\ mod\ 17 = 2$

c) $25437 \oplus_{23} 28283$ $(25437 + 282833) mod\ 23$
$= (25437\ mod\ 23 + 282833\ mod\ 23) mod\ 23$
$= (22 + 2)\ mod\ 23 = 24\ mod\ 23 = 1$
$(25437 + 2823833)\ mod\ 23 = 308270\ mod\ 23 = 1$

Aufgabe 23:

a) $5403 \odot_6 1934$ $(5403 \cdot 1934) mod\ 6 = (5403\ mod\ 6 \cdot 1934\ mod\ 6)\ mod\ 6$
$= (3 \cdot 2)\ mod\ 6 = 6\ mod\ 6 = 0$
$(5403 \cdot 1934)\ mod\ 6 = 10449402\ mod\ 6 = 0$

b) $1702 \odot_{17} 34$ $(1702 \cdot 34)\ mod\ 17 = (1702\ mod\ 17 \cdot 34\ mod\ 17)\ mod\ 17$
$= (2 \cdot 0)\ mod\ 17 = 0\ mod\ 17 = 0$
$(1702 \cdot 34)\ mod\ 17 = 57868\ mod\ 17 = 0$

c) $25437 \odot_{23} 28283$ $(25437 \cdot 282833) mod\ 23$
$= (25437\ mod\ 23 \cdot 282833\ mod\ 23) mod\ 23$
$= (22 \cdot 2)\ mod\ 23 = 44\ mod\ 23 = 21$
$(25437 \cdot 282833)\ mod\ 23 = 7194423021\ mod\ 23 = 21$

Aufgabe 24:

a)

$1^2\ mod\ 6 = 1$
$2^2\ mod\ 6 = 4$
$3^2\ mod\ 6 = 3$
$4^2\ mod\ 6 = 4$
$5^2\ mod\ 6 = 1$

b)

$1^2\ mod\ 11 = 1$
$2^2\ mod\ 11 = 4$
$3^2\ mod\ 11 = 9$
$4^2\ mod\ 11 = 5$
$5^2\ mod\ 11 = 3$
$6^2\ mod\ 11 = 3$
$7^2\ mod\ 11 = 5$
$8^2\ mod\ 11 = 9$
$9^2\ mod\ 11 = 4$
$10^2\ mod\ 11 = 1$

Aufgabe 25:

a) Die modularen Wurzeln von 2 bzgl. $mod\ 7$ sind 3 und 4.
b) Die modularen Wurzeln von 1 bzgl. $mod\ 9$ sind 1 und 8.

Aufgabe 26:

a) $\phi(7) = 6$ b) $\phi(18) = 6$ c) $\phi(21) = 12$

Aufgabe 27:

a) $\phi(41) = 41 - 1 = 40$
b) $\phi(77) = \phi(7 \cdot 11) = 6 \cdot 10 = 60$
c) $\phi(143) = \phi(13 \cdot 11) = 12 \cdot 10 = 120$

Aufgabe 28:

a) $a^{64} = (((((a^2)^2)^2)^2)^2)^2$
b) $a^{72} = a^{64} \cdot a^8$
c) $a^{256} = (((((((a^2)^2)^2)^2)^2)^2)^2)^2$
d) $a^{513} = (((((((((a^2)^2)^2)^2)^2)^2)^2)^2)^2 \cdot a$
e) $a^{648} = a^{512} \cdot a^{128} \cdot a^8$

Aufgabe 29:

$n = 91, \phi(n) = 72, d = 29, c = 74$

Aufgabe 30:

a) $n = 21, d = 5, c = 3, m_1 = 12$
b) $n = 221, d = 91, c = 198, m_1 = 29$

Abstract

Diese Diplomarbeit stellt eine Ausarbeitung des Themas Kryptographie für den Unterricht in einem Wahlpflichtfach oder einer ähnlichen Lernumgebung dar. Dazu werden zuerst die allgemeinen und gesetzlichen Aspekte eines Wahlpflichtfaches behandelt, dann erfolgt ein kurzer Überblick darüber, warum sich das Thema Kryptographie gut für den Wahlpflichtunterricht eigenen würde. Da im Lehramtsstudium Mathematik in den Pflichtlehrveranstaltungen keine Kryptographie vorgesehen ist, kann der darauffolgende Theorieteil auch zur Vorbereitung auf die Unterrichtssequenz für die Lehrerinnen und Lehrer dienen. Weiters ist es so geplant, dass auch die Schülerinnen und Schüler diesen Teil als Nachschlagewerk und Theorieskript verwenden können. Eine Aufbereitung des Stoffes, ähnlich einem Schulbuch, wird dann im letzten Kapitel zur Verfügung gestellt.

This diploma thesis elaborates on teaching Cryptography in the context of a compulsory optional subject or in a similar educational environment. After an explanation of the compulsory optional subject's general aspects and the legal framework, a brief overview will follow in which it's summed up why this topic would be well applicable for teaching in a compulsory optional subject. Because Cryptography is not part of the curriculum of the studies for teaching certificate in the field of mathematics, the following theoretical chapter could also be used by teachers for preparing lessons. Furthermore this chapter is supposed to be a reference book for students as well. A rework of the subjects similar to a school book will be provided in the last chapter.

Literaturverzeichnis

Becker, K. (24. Juli 2014). *Inf-Schule*. Abgerufen am 26. April 2017 von http://www.inf-schule.de/kommunikation/kryptologie/rsa/modrechnen/station_uhrenaddition

Beutelspacher, A. (2007). *Kryptologie: Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen.* Wiesbaden: Vieweg & Sohn Verlag | GWV Fachverlage GmbH.

Beutelspacher, A., Neumann, H., & Schwarzpaul, T. (2010). *Kryptografie in Theorie und Praxis: Mathematische Grundlagen für Internetsicherheit, Mobilfunk und elektronisches Geld.* Wiesbaden: Vieweg+Teubner | GWV Fachverlage GmbH.

Beutelspacher, A., Schwenk, J., & Wolfenstetter, K.-D. (2006). *Moderne Verfahren der Kryptographie.* Wiesbaden: Friedr. Vieweg & Sohn Verlag/GWV Fachverlage GmbH.

Buchmann, J. (2008). *Einführung in die Kryptographie.* Berlin Heidelberg: Springer-Verlag.

Bundesministerium für Bildung. (2004). *Lehrplan Mathematik*. Von https://www.bmb.gv.at/schulen/unterricht/lp/lp_neu_ahs_07_11859.pdf?5te97p abgerufen

Bundesministerium für Bildung. (19. Februar 2015). *AHS*. Von https://www.bmb.gv.at/schulen/bw/abs/ahs.html abgerufen

Curriculum Bachelor Mathematik. (Juli 2014). *Universität Wien.* Abgerufen am 23. April 2017 von http://studentpoint.univie.ac.at/fileadmin/user_upload/studentpoint_2011/Curricula/Bachelor/BA_Mathematik_Vers2014.pdf

Curriculum Informatik Bachelor. (28. Juni 2016). *Universität Wien.* Abgerufen am 23. April 2017 von http://studentpoint.univie.ac.at/fileadmin/user_upload/studentpoint_2011/Curricula/Bachelor/BA_Informatik.pdf

Curriculum Informatik Bachelor. (2017). *Technikum Wien*. Abgerufen am 23. April 2017

Curriculum Informations- und Kommunikationssysteme. (2017). *Technikum Wien*. Abgerufen am 23. April 2017 von https://www.technikum-wien.at/studium/bachelor/informations__und_kommunikationssysteme/informations-und-kommunikationssysteme-curriculum/

Curriculum Unterrichtsfach Mathematik. (27. Juni 2016). *Universität Wien.* Abgerufen am 23. April 2017 von http://studentpoint.univie.ac.at/fileadmin/user_upload/studentpoint_2011/Curricula/Lehramt/LA_BA_Mathematik.pdf

Deutsches Reichspatentamt. (8. Juli 1925). Abgerufen am 28. März 2017 von http://www.cdvandt.org/Enigma%20DE416219C1.pdf

Dorfmayr, D. A. (2007). *Von Cäsar bis RSA.* Universität Wien.

Ertel, W. (2007). *Angewandte Kryptographie.* München: Carl Hanser Verlag.

Freiermuth, K., Hromkovic, J., Keller, L., & Steffen, B. (2010). *Einführung in die Kryptologie: Lehrbuch für Unterricht und Selbststudium.* Wiesbaden: Vieweg + Teubner Verlag.

Gartner, L. (28. April 2010). *TU Freiberg*. Abgerufen am 4. März 2017 von http://www.mathe.tu-freiberg.de/~hebisch/cafe/kryptographie/haeufigkeitstabellen.html

Hebisch, U. (14. Mai 2010). *TU Freiberg*. Abgerufen am 4. März 2017 von http://www.mathe.tu-freiberg.de/~hebisch/cafe/kryptographie/bigramme.html

Humenberger, H. (1996). *Anwendungsorientierung im Mathematikunterricht - erste Resultate eines Forschungsprojekts.* Regensburg.

Jukna, S. (2008). *Crashkurs Mathematik: für Informatiker.* Wiesbaden: B.G. Teubner Verlag / GWV Facherlage GmbH.

Kurose, J., & Ross, K. (2013). *Computer Networking: A Top-Down Approach.* USA: Pearson Education, Inc.

Küsters, R., & Wilke, T. (2011). *Moderne Kryptographie: Eine Einführung.* Berlin: Vieweg+Teubner Verlag.

Lehrplan Mathematik WPF. (8. Juli 2004). *Bundesministerium für Bildung*. Abgerufen am 19. Februar 2017 von https://www.bmb.gv.at/schulen/unterricht/lp/lp_neu_ahs_29_11884.pdf?5s8x3x

Mastny, L. (2009). *Didaktische Perspektiven des fächerübergreifenden Unterrichts am Beispiel Bewegung und Sport und Physik.* Wien.

Rempe, L., & Waldecker, R. (2009). *Primzahltests für Einsteiger: Zahlentheorie - Algorithmik - Kryptographie.* Wiesbaden: Vieweg + Teubner | GWV Fachverlage GmbH.

Schenkl, K. (1859). *Griechisch-deutsches Schulwörterbuch.* Wien: Gerold.

Schichl, H., & Steinbauer, R. (2012). *Einführung in das mathematische Arbeiten.* Berlin Heidelberg: Springer-Verlag.

Schmeh, K. (2016). *Kryptographie: Verfahren, Protokolle, Infrastrukturen.* Heidelberg: dpunkt.verlag GmbH.

Schmidt, J. A. (1832). *Deutsch-griechisches Handwörterbuch.* Leipzig: Tauchnitz.

Schulorganisationsgesetz. (25. Juli 1962). *Bundeskanzleramt Rechtsinformationssystem*. Abgerufen am 21. Februar 2017 von https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10009265

Schulunterrichtsgesetz. (25. August 1986). *Bundeskanzleramt Rechtsinformationssystem*. Abgerufen am 21. Februar 2017 von

https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10009600

Singh, S. (2016). *Geheime Botschaften: Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet.* München: dtv.

Spitz, S., Pramateftakis, M., & Swoboda, J. (2011). *Kryptographie und IT-Sicherheit.* Wiesbaden: Vieweg+Teubner Verlag.

Tabellenverzeichnis

Abbildungsverzeichnis