

Inhaltsverzeichnis

1	Von Geheimschriften zu Kryptosystemen	3
	Geschichte und Grundbegriffe	4
	Funktionen	9
	Codierungen	13
	Kryptosysteme	17
	Zusammenfassung	26
2	Die Suche nach Sicherheit und modulares Rechnen	31
	Kryptoanalyse und der Begriff der Sicherheit	32
	Modulare Addition	34
	Algebraische Strukturen	40
	Modulare Multiplikation	47
	Monoide	48
	Gruppen	52
	Verallgemeinerungen vom Kryptosystem CAESAR	56
	Zusammenfassung	70
3	Entwurf und Kryptoanalyse von monoalphabetischen Kryptosystemen	75
	Der Begriff der monoalphabetischen Kryptosysteme	75
	Kryptoanalyse von monoalphabetischen Kryptosystemen	78
	Verbesserung zu monoalphabetischen Kryptosystemen	84
	Zusammenfassung	90
4	Polyalphabetische Kryptosysteme und deren Kryptoanalyse	95
	Das polyalphabetische Kryptosystem VIGENÈRE	95
	Kryptoanalyse von VIGENÈRE	100
	Statistische Kryptoanalyse von VIGENÈRE	106
	Der Euklidische Algorithmus	124
	Homophone Kryptosysteme	130
	Zusammenfassung	133
5	Perfekte Sicherheit und One-Time-Pad Kryptosysteme	139
	Die Entwicklung des ONE-TIME-PAD Kryptosystems	140
	Betrachtungen zur Sicherheit des ONE-TIME-PAD	142

Kryptoanalyse bei mehrfacher Verwendung des Schlüssels	143
Das mathematische Konzept der perfekten Sicherheit	144
Sicherheitsverlust bei mehrfacher Verwendung eines Schlüssels	154
Zusammenfassung	159
6 Die ENIGMA und moderne Kryptosysteme	163
Die bedeutende Geschichte der ENIGMA	163
Binärzahlen	167
Umwandlung zwischen Zehner- und Binärsystem	169
7 Der geheime Schlüsselaustausch und das Diffie-Hellman Protokoll	171
Modulares Potenzieren	178
Diffie-Hellman	183
Zusammenfassung	187
8 Komplexitätstheoretische Konzepte und Sicherheit	191
Messung der Berechnungskomplexität von Algorithmen	193
Zusammenfassung	208
9 Das Konzept der Public-Key Kryptographie	211
Schwer berechenbare Grapheigenschaften als Geheimnisse	216
Zahlentheoretische Eigenschaften als Geheimnisse	229
Ein Public-Key Kryptosystem zum Verschicken eines Bits	243
10 Anwendungen der Public-Key-Kryptographie und Kommunikationsproto- koll	247
Digitale Unterschrift von Dokumenten	247
Vergessliche Übertragung oder Münzwurf über das Telefon	249
Vergleich von zwei geheimen Zahlen	251
Zero-Knowledge-Beweissysteme	255
A Lösungen zu ausgewählten Aufgaben	263

Lektion 1

Von Geheimschriften zu Kryptosystemen

Sprachen sind aus dem Bedürfnis heraus entstanden, jemandem etwas mitzuteilen. Wir Menschen machen diese Erfahrung bereits früh im Leben. Erinnert euch zurück: Als Kleinkind versuchten wir verzweifelt mit wortähnlichen Lauten auf uns aufmerksam zu machen. Oft wurden unsere Äusserungen dabei aber missverstanden. Um Irrtümer zu vermeiden blieb uns nichts anderes übrig als sprechen zu lernen. Wir konnten nun also unserer Umgebung unsere Bedürfnisse mitteilen. Gleichzeitig verstanden wir auch, was die Leute uns mitteilen wollten, und wir konnten ihre Gespräche mitverfolgen.

Bald merkten wir aber, dass es da noch eine weitere Hürde zu überwinden gab. Wir verstanden zwar, was wir hörten, aber die komischen Zeichen, die die älteren Kinder und Erwachsenen benutzten, konnten wir nicht entziffern.

Seit dem ersten Schultag begann sich dieses Problem allmählich von ganz allein zu lösen: Wir zeichneten Buchstaben, reihten sie aneinander und bildeten daraus Wörter, Sätze und ganze Texte. Später lernten wir sogar fremde Sprachen zu verstehen und zu sprechen. Wir konnten uns also mit immer mehr Personen austauschen.

Nur ein kleines Problem gab es noch: Alles, was wir einer Person mitteilten, konnte auch von anderen Personen verfolgt werden. Manchmal waren diese Leute nicht befugt die Mitteilung zu hören. Wir mussten also nach einer Möglichkeit suchen, den anderen heimlich Nachrichten zukommen zu lassen, beispielsweise indem wir die Nachricht für Dritte unleserlich machten. Da gab es viele Möglichkeiten. Vielleicht kennt ihr noch den Trick mit der Zitrone und dem Bügeleisen? Mit Zitronensaft kann man eine unsichtbare Nachricht auf ein Blatt Papier schreiben. Um die Nachricht zu lesen, muss man mit dem Bügeleisen über das Blatt Papier fahren. Die Wärme bewirkt, dass der Zitronensaft braun und dadurch sichtbar wird. Der Nachteil dieser Methode ist, dass jeder, der den Trick kennt, diese Nachricht abfangen und lesen kann.

Ihr kennt aber sicher auch noch andere Möglichkeiten, um Nachrichten für andere unleserlich oder unverständlich zu machen. Vielleicht werdet ihr sogar Parallelen zu den Methoden in diesem Buch erkennen. Zuvor werden wir aber kurz in die Geschichte der Kryptographie eintauchen und uns einen für die Kryptographie geeigneten Wortschatz aneignen.

Geschichte und Grundbegriffe

Mit der Entdeckung der Schriften wurden erstmals schriftliche Mitteilungen zu Elementen einer Art Geheimsprache. Lesen und Schreiben unterrichteten meistens Priester unterschiedlicher Religionen, und deren Unterricht glich nicht selten einer Einweihung in die tieferen Geheimnisse des Priester- oder Beamtentums. Der Roman *Der Fünfte Berg* von Coelho (2007) stellt eine schöne belletristische Bearbeitung dieses Themas dar.

Jede Schrift basiert auf einer endlichen, nichtleeren Menge von ausgewählten Zeichen, die **Alphabet** genannt wird. Die Zeichen des Alphabets nennen wir auch **Symbole** oder **Buchstaben**. Ursprünglich stellten viele Zeichen Gegenstände und Tiere dar, mit der Zeit wurden diese immer stärker vereinfacht, bis sie schliesslich symbolischen Charakter annahmen. Die schriftlichen Mitteilungen erhält man, wenn man die Symbole in einer Folge anordnet. Diese Symbolfolgen nennen wir **Texte**.

Als Texte betrachten wir einerseits einzelne Buchstaben und Wörter aus einer Sprache, andererseits aber auch beliebig lange Aufsätze wie beispielsweise den Inhalt eines Buches. Für uns ist aber auch XYAAPQR ein Text, obwohl diese Folge von Buchstaben in einer natürlichen Sprache keine Bedeutung hat. Sobald es sich aber um die Codierung einer geheimen Information handelt, kann der Text eine Bedeutung haben.

Mit der sozialen Entwicklung der Gesellschaften war der Fortschritt in Bezug auf Lese- und Schreibkenntnisse dann aber nicht mehr zu bremsen, und der Anteil der Bevölkerung mit Schreibfähigkeit stieg stark an. In dieser Zeit entstand auch der Bedarf an der Entwicklung der Geheimschriften.

Auszug aus der Geschichte Unter einer Schrift versteht man ein System von graphischen Zeichen, das zur Kommunikation verwendet wird. Die Erfindung der Schrift betrachten wir als eine der fundamentalsten Entwicklungen der Menschheit, die Erhaltung und Überlieferung von Wissen zuverlässig über lange Zeitabschnitte ermöglicht hat. Aus dieser Sicht kann man die Geschichte der Sprachen auch als die Geschichte der Entwicklung von Zeichen (Symbolen) sehen.

Die Vorgänger der Zeichen waren Abbilder von Tieren und Menschen. Die ältesten Funde sind rund 20 000 Jahre alt. Eine der bekanntesten Fundstellen ist die Höhle von Lascaux in Frankreich. Manche Forscher fanden dort schon abstrakte Zeichen mit symbolischem Charakter, die bereits die Abstraktionsfähigkeit zeigten, die später zur Entwicklung von Zeichensystemen führte. Die bekannten Hochkulturen wie die Sumerer, Ägypter und das Reich der Mitte entwickelten bereits eigene Schriften. Die ältesten Schriftfunde sind 6000 Jahre alt und stammen aus Uruk in Mesopotamien.

Die Schrift diente der Verwaltung des Reichs im wirtschaftlichen Sinn. Die ersten Schriften waren **Bilderschriften**, in der die Gegenstände durch ihre Formen dargestellt wurden. Über **Wortschriften** sprechen wir dann, wenn ein Wort einem Zeichen entspricht, das nicht mehr „künstlerisch“ den entsprechenden Gegenstand darstellt. So entwickelten sich die Schriften im alten Ägypten, die der Mayas und der Eskimos zu den **Silbenschriften**, bei denen einzelne Zeichen ganzen Silben entsprechen. Die Entwicklung hat ihren Ursprung vermutlich in der Verwendung von einsilbigen Wörtern. Die heute am meisten verwendete **Buchstabenschrift** ordnet einzelnen Zeichen bestimmte Laute zu.

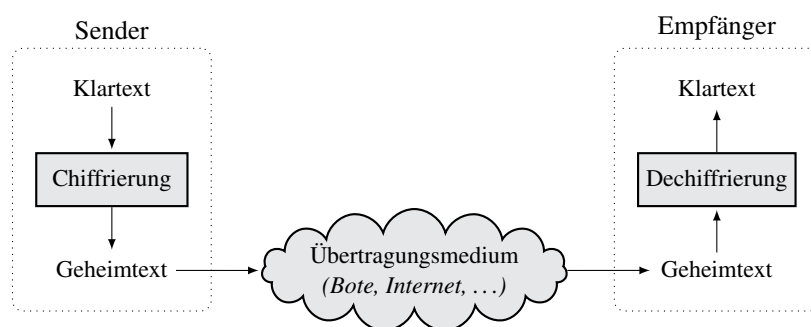


Abbildung 1.1 Dieses Schema zeigt den Kommunikationsschritt, bei dem der Sender dem Empfänger einen Geheimtext schickt. Die Übertragung des Geheimtextes wird durch ein Übertragungsmedium (zum Beispiel einen Boten oder das Internet) erfolgen.

In der voneinander unabhängigen Entwicklung von Schriften an unterschiedlichen Orten kam es oft zu gemischten Schriftarten. Die älteste bekannte reine Buchstabenschrift ist ungefähr 4000 Jahre alt und wurde in der Region von Syrien und Palästina – beeinflusst durch ägyptische Hieroglyphen – entwickelt. Die Mehrzahl der heutigen Alphabete (Zeichensysteme) in Europa haben ihren Ursprung im griechischen Alphabet, das über die Etrusken nach Italien gelangte und sich dort ungefähr 600 Jahre v. u. Z. zum lateinischen Alphabet entwickelte.

Die Informatik hat die Entwicklung von Alphabeten ins Extreme getrieben. Sie verwendet nur die Symbole 0 und 1 zur Darstellung von Daten und damit auch von allen Texten. Alles wird als Folge von diesen zwei Symbolen dargestellt, obwohl die Symbole 0 und 1 nichts mehr mit der gesprochenen Sprache gemeinsam haben.

Aufgabe 1.1 Finde Beispiele für heute verwendete Sprachen, die keine reine Buchstabenschrift verwenden.

Das Schema einer geheimen Kommunikation ist in Abbildung 1.1 gezeichnet. Wir werden es **Kommunikationsschema** nennen. Hier wollen zwei Leute schriftlich eine geheime Nachricht austauschen, wobei die Nachricht ein Text in einer natürlichen Sprache ist. Wir wollen nun die Kommunikation, die hier abläuft, in **Kommunikationsschritte** zerlegen. In einem Kommunikationsschritt schickt der **Sender** die Nachricht an den **Empfänger**. Diese Nachricht ist in einer Sprache verfasst, die beide verstehen, und sie wird im Folgenden mit **Klartext** bezeichnet. Die Rollen des Senders und Empfängers sind für einen Kommunikationsschritt fest zugeteilt und können erst in einem weiteren Kommunikationsschritt neu verteilt werden.

Beim Übertragen der Nachricht müssen Sender und Empfänger immer damit rechnen, dass etwas schiefgeht. Beispielsweise könnten sie es mit einem unzuverlässigen Boten zu tun haben oder sogar mit einem Gegner, der ihnen schaden will. Sender und Empfänger wollen aber auf jeden Fall verhindern, dass jemand, der die geheime Nachricht in die Hände bekommt, diese lesen kann. Sie müssen sich also etwas einfallen lassen. Deshalb erstellen die beiden eine **Geheimschrift**, die nur sie beide kennen und die somit ihr

gemeinsames Geheimnis ist. Eine solche Geheimschrift kann man als ein Paar von Algorithmen¹ ansehen, die wir Chiffrierung und Dechiffrierung nennen. Die **Chiffrierung** ist ein Verfahren, das einen gegebenen Klartext in einen Geheimtext umwandelt. Die **Dechiffrierung** ist ein Verfahren, welches das Ganze wieder rückgängig macht, nämlich einen Geheimtext in den Klartext zurückverwandelt. Der Geheimtext wird vom Sender mit Hilfe eines Übertragungsmediums zum Empfänger geschickt. Ein aktuelles Beispiel eines solchen Übertragungsmediums ist das Internet, welches eine sehr unzuverlässige Nachrichtenübertragung darstellt, denn jede E-Mail, die unverschlüsselt übers Internet gesendet wird, kann ohne weiteres abgefangen und gelesen werden. E-Mails können mit Postkarten verglichen werden. Weil sie in keinem Umschlag sind, könnte jeder, der die Postkarte in die Hände bekommt, die Nachricht auch gleich lesen.

Die Klartexte sind Folgen von Buchstaben eines Alphabets derjenigen Sprache, die für die Kommunikation verwendet wird. Wir verwenden hier meistens die deutsche Sprache, und dazu gehört das lateinische Alphabet,

$$\text{Lat} = \{ A, B, C, D, E, F, G, H, I, J, K, L, M, \\ N, O, P, Q, R, S, T, U, V, W, X, Y, Z \},$$

das von den meisten europäischen Sprachen benutzt wird. Leerzeichen, Punkte, Kommas und alle anderen Interpunktionszeichen werden im Klartext nicht verwendet. Wir werden sie deshalb einfach weglassen. Oft unterscheiden wir auch nicht zwischen Gross- und Kleinbuchstaben und verwenden nur Texte, die aus Grossbuchstaben bestehen. Für das Alphabet des Geheimtextes können beliebige Buchstaben, Zahlen oder andere bereits bestehende, aber auch selbst erfundene Symbole verwendet werden. Die Länge eines Textes ist die Anzahl der Zeichen der Buchstabenfolge. Somit ist die Länge des Textes ANNA genau vier.

Manchmal ist es hilfreich, eine feste Ordnung für die Zeichen eines Alphabets zu haben. Gerade im lateinischen Alphabet, wo die Buchstaben eine bestimmte Reihenfolge A, B, C, ..., X, Y, Z haben, ist es naheliegend, die **Ordnung Ord** eines Buchstabens anhand der Position in der Auflistung anzugeben. Die Ordnungen der Buchstaben aus Lat sind in Tabelle 1.1 gegeben. Sobald eine Ordnung auf Buchstaben definiert ist, können alle Wörter der entsprechenden Sprache systematisch aufgelistet werden.

Aufgabe 1.2 Betrachte das Alphabet $\{ A, B, C \}$. Liste alle Texte der Länge höchstens drei über diesem Alphabet auf. Die Texte AAA oder CBA sind Beispiel für Texte der Länge drei und BA hat die Länge zwei.

¹Ein **Algorithmus** ist die Beschreibung einer Vorgehensweise, die man auch als Rechenvorschrift bezeichnen kann. Die Anwendung eines Algorithmus bewirkt die Durchführung einer endlichen Anzahl von Rechenschritten. Die Beschreibung des Algorithmus kann als eine Folge von einfachen, allgemein verständlichen Instruktionen angesehen werden. Der Begriff Algorithmus ist einer der wichtigsten Begriffe in der Informatik. Eine genauere Festlegung dieses Begriffs findet ihr im Modul *Geschichte und Begriffsbildung*.

Tabelle 1.1 Die Ordnungen der Buchstaben aus dem Alphabet Lat.

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

Aufgabe 1.3 Wie bereits erwähnt, ermöglicht uns das Einführen der Ordnung auf Buchstaben eines bestimmten Alphabets, alle Wörter einer Sprache systematisch aufzulisten. Das bedeutet, die Wörter so aufzulisten, dass sie möglichst schnell gefunden werden. Ein Beispiel für eine solche Auflistung ist ein Wörterbuch.

Beschreibe genau, wie die Wörter in einem Wörterbuch sortiert sind. Aus dieser Beschreibung soll für zwei beliebige Wörter eindeutig hervorgehen, welches der beiden vor dem anderen aufgeführt ist und warum.

Hinweis für die Lehrperson An dieser Stelle könnte es hilfreich sein, Kenntnis von Wörtern und Alphabeten aus Lektion 1 des Moduls *Entwurf von endlichen Automaten*² zu haben. Diese ist jedoch nicht unbedingt erforderlich. Beachte, dass wir im Modul *Entwurf von endlichen Automaten* anstelle des Fachwortes „Text“ das Fachwort „Wort“ verwenden, weil dies in der Automatentheorie üblich ist. Hier ziehen wir aber die Bezeichnung „Text“ vor, weil die umgangssprachliche Verwendung dieses Begriffs näher an der hier betrachteten Bedeutung von Folgen von Buchstaben liegt.

Wenn dieses Modul den Schülern unbekannt ist, kann man sie darauf aufmerksam machen, dass jede endliche, nichtleere Menge von Symbolen ein **Alphabet** genannt werden darf. Die **Texte** über dem gewählten Alphabet sind dann alle endlichen Folgen von Symbolen dieses Alphabets. Wenn Texte als Buchstabenfolgen dargestellt werden, werden aber – im Unterschied zu Folgen, wie sie in der Mathematik vorkommen – keine Kommas zwischen den einzelnen Symbolen des Alphabets gesetzt. Dies überrascht nicht, weil wir es bereits vom Umgang mit Texten in den natürlichen Sprachen her gewohnt sind.

Die folgende Aufgabe ist nur für Klassen geeignet, die bereits die Grundlagen der Kombinatorik kennen.

Aufgabe 1.4 Wie viele Texte mit den folgenden Eigenschaften gibt es? Begründe deine Antwort.

- Anzahl der Texte der Länge drei über dem Alphabet $\{A, B, C\}$
- Anzahl der Texte der Länge fünf über dem Alphabet $\{0, 1, 2, 3\}$
- Anzahl der Texte der Längen 1 bis 3 über dem Alphabet $\{0, 1\}$
- Anzahl der Texte der Länge n über dem Alphabet $\{0, 1\}$, wenn n eine positive ganze

²Juraj Hromkovič (2008). *Lehrbuch Informatik. Vorkurs Programmieren, Geschichte und Begriffsbildung, Automatenentwurf*. Wiesbaden: Vieweg+Teubner.

	1	2	3	4	5
1	A	B	Γ	Δ	E
2	Z	H	Θ	I	K
3	Λ	M	N	Ξ	O
4	Π	P	Σ	T	Υ
5	Φ	X	Ψ	Ω	

Abbildung 1.2 Die Tabelle für die Geheimschrift von Polybios.

Zahl ist.

- (e) Anzahl der Texte der Länge 8 über dem Alphabet $\{A, B, C, D\}$ mit der zusätzlichen Bedingung, dass jedes Symbol in jedem Text genau zweimal vorkommt.
- (f) Anzahl der Texte der Länge 8 über dem Alphabet $\{0, 1, 2\}$, so dass die Texte genau vier Nullen und eine Eins enthalten.
- (g) Anzahl der Texte der Länge 4 über dem Alphabet $\{0, 1\}$, die mindestens so viele Symbole 1 wie 0 enthalten. Ein Beispiel für einen solchen Text ist 1011.
- (h) Anzahl der Texte der Länge 8 über dem Alphabet $\{0, 1, 2\}$, die mehr Nullen als Symbole 1 und 2 zusammen haben.

Eine der ersten Geheimschriften hat der griechische Schriftsteller Polybios 200 Jahre v. u. Z. entwickelt. Seine Chiffrierung ordnet jedem der 24 Symbole des griechischen Alphabets eine zweistellige Zahl zu. Jeder Buchstabe wird somit auf eine Folge von zwei Ziffern aus dem Alphabet $\{1, 2, 3, 4, 5\}$ abgebildet. Die genaue Zuordnung ist in Abbildung 1.2 dargestellt. Die Zeilen und Spalten der 5×5 -Tabelle sind jeweils mit den Zahlen 1 bis 5 durchnummeriert. Das Alphabet wird zeilenweise eingetragen. So erhält jeder Buchstabe eine Position, gegeben durch die Zeilen- und Spaltennummer. Das Θ beispielsweise, das sich in der zweiten Zeile und in der dritten Spalte befindet, besitzt die Position (2,3) und somit die *Codierung* 23.

Aufgabe 1.5 Chiffriere den Klartext $\text{HEPAKAE}\Sigma$ mit der Geheimschrift von Polybios.

Aufgabe 1.6 Das Folgende wurde mit der Geheimschrift von Polybios codiert:

25424541443543

Wie lautet der Klartext?

Das Chiffrierungsverfahren kann mit Hilfe der Tabelle in Abbildung 1.2 beschrieben werden. Dafür werden zwei neue Begriffe verwendet: Das Alphabet, das für den Klartext verwendet wird, wird mit **Klartextalphabet**, und das Alphabet, das für den Geheimtext verwendet wird, mit **Geheimtextalphabet** bezeichnet.

Geheimschrift POLYBIOS

Klartextalphabet:	Greek
Geheimtextalphabet:	{ 1, 2, 3, 4, 5 }
Chiffrierung:	Lies den Klartext von links nach rechts und ersetze jeden Buchstaben durch die Folge von zwei Ziffern aus dem Geheimtextalphabet { 1, 2, 3, 4, 5 }. Die erste Ziffer ist die Nummer der Zeile, in der sich der Buchstabe befindet. Die zweite Ziffer ist die Nummer der Spalte, in der sich der Buchstabe befindet.
Dechiffrierung:	<i>Siehe Aufgabe 1.7</i>

Aufgabe 1.7 Beschreibe umgangssprachlich analog zum Chiffrierungsverfahren das Dechiffrierungsverfahren der Geheimschrift von Polybios. Achte darauf, dass deine Beschreibung eindeutig ist.

Am Beispiel der Geheimschrift von Polybios haben wir ein allgemeines Schema aufgezeigt, mit dem eine Geheimschrift beschrieben werden kann. Mit den Angaben Klartextalphabet, Geheimtextalphabet, Chiffrierung und Dechiffrierung ist eine Geheimschrift vollständig definiert. Wir werden diese Darstellung im Folgenden das **Schema der Geheimschriften** nennen.

Bei der Beschreibung der Chiffrierung von Polybios ist der Begriff *Codierung* vorgekommen. Wir wollen nun klarstellen, was dieser Begriff genau bedeutet. Dazu brauchen wir den folgenden mathematischen Hintergrund.

Funktionen

Eine **Funktion** ist eine Abbildung, die alle Elemente einer Menge (genannt **Definitionsmenge**) auf Elemente einer anderen Menge (genannt **Wertemenge**) abbildet. Seien A und B zwei beliebige Mengen. Die Funktion $f: A \rightarrow B$ ordnet jedem Element der Menge A ein Element der Menge B zu. Die Elemente aus der Definitionsmenge A heißen **Argumente**, Elemente aus dem Wertemenge B nennen wir **Funktionswerte**.

Sei \mathbb{R} die Menge der reellen Zahlen. Mit \mathbb{R}^+ bezeichnen wir die Menge der positiven reellen Zahlen. Weiter werden wir die Menge $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ der natürlichen Zahlen, die Menge \mathbb{Z} der ganzen Zahlen und die Menge \mathbb{Q} der rationalen Zahlen betrachten. Analog zu \mathbb{R}^+ ist \mathbb{Z}^+ die Menge der positiven ganzen Zahlen und \mathbb{Q}^+ die Menge der positiven rationalen Zahlen.

Ein Beispiel für eine Funktion ist $f: \mathbb{R} \rightarrow \mathbb{R}$ ist $f(x) = 2x + 1$, wobei alle Zahlen aus \mathbb{R} auf Zahlen aus \mathbb{R} abgebildet werden. Konkret wird jede reelle Zahl $x \in \mathbb{R}$ auf den Funktionswert $2x + 1 \in \mathbb{R}$ abgebildet. Der Graph dieser Funktion entspricht einer Geraden wie in Abbildung 1.3 dargestellt. Diese Darstellung für Funktionen nennen

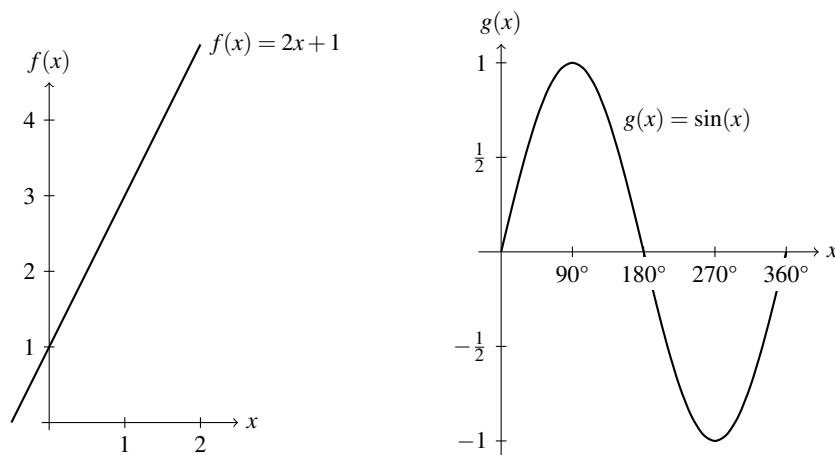


Abbildung 1.3 Der Graph der Funktion $f(x) = 2x + 1$ ist links dargestellt und der Graph der Funktion $g(x) = \sin(x)$ rechts.

wir **Funktionsgraph** der Funktion $f(x)$. Betrachten wir die gleiche Funktion als eine Abbildung von \mathbb{N} nach \mathbb{N} , erhalten wir anstelle einer Geraden eine Menge von Punkten. Diese Punkte liegen aber auch auf einer Geraden.

Die Funktion $g(x) = \sin(x)$ können wir als eine Funktion von \mathbb{R} nach \mathbb{R} betrachten oder auch als eine Funktion von \mathbb{R} nach $[-1, 1]$. Es ist schnell zu sehen, dass mehrere verschiedene x -Werte auf den gleichen Funktionswert der Sinusfunktion abgebildet werden. So werden beispielsweise $\sin(180)$ und $\sin(360)$ beide auf den gleichen Funktionswert 0 abgebildet, wie in Abbildung 1.3 zu sehen ist.

In der Lehre der Geheimschriften sind wir besonders an denjenigen Funktionen interessiert, bei welchen nie zwei oder mehr x -Werte auf den gleichen Funktionswert abgebildet werden. Jeder mögliche Funktionswert $f(x)$ soll somit nur einem einzigen x zugeordnet werden können.

*Eine Funktion f von A nach B heisst **injektiv**, wenn für beliebige zwei unterschiedliche Argumente x und y aus A die Funktionswerte $f(x)$ und $f(y)$ auch unterschiedlich sind. Das heisst, für unterschiedliche Argumente müssen die entsprechenden Funktionswerte unterschiedlich sein.*

Wenn für alle Argumente x und y , für die gilt, dass x nicht gleich y ist, die Funktionswerte $f(x)$ und $f(y)$ nicht gleich sein dürfen, bedeutet das, dass jeder Funktionswert $f(z)$ eindeutig auf sein Argument zurückgeführt werden kann. Zum Beispiel kann für die Funktion $f(x) = 2x + 1$, wenn der Funktionswert $f(x) = 11$ bekannt ist, das Argument

$x = 5$ eindeutig bestimmt werden:

$$\begin{array}{rcl} 2x + 1 = 11 & & | - 1 \\ 2x = 10 & & | : 2 \\ x = 5 & & \end{array}$$

Der Funktionswert 11 bestimmt also eindeutig den Wert 5 für das Argument x . Analog dazu kann bei der Funktion $f(x) = x^3$ für jeden Funktionswert x^3 eindeutig das x bestimmt werden. Wenn beispielsweise $f(x) = 8$ ist, dann ist x eindeutig gleich 2. Somit ist $f(x) = x^3$ auch eine injektive Funktion.

Graphisch erkennen wir eine injektive Funktion daran, dass ihr Graph geschnitten mit jeder beliebigen Geraden parallel zur x -Achse maximal einen Schnittpunkt hat. Somit gehört zu jedem Funktionswert y genau ein Argument x .

Aufgabe 1.8 Ist die Funktion $f: \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = x^2$ injektiv? Begründe deine Antwort.

Hinweis für die Lehrperson An dieser Stelle sollte deutlich gemacht werden, wie man die Injektivität oder die Nichtinjektivität einer Funktion begründet. Um zu zeigen, dass eine Funktion $f: A \rightarrow B$ nicht injektiv ist, reicht es, zwei unterschiedliche Werte x und y aus A zu finden, so dass $f(x) = f(y)$ gilt. Also reicht ein Beispiel mit zwei konkreten Werten x und y mit $x \neq y$ und $f(x) = f(y)$ aus, um die Nichtinjektivität zu zeigen. Aber um die Injektivität einer Funktion $g: C \rightarrow D$ zu begründen, muss man für *alle* Werte x und y aus C zeigen, dass $x \neq y$ zu $f(x) \neq f(y)$ führt.

Eine besonders wichtige Eigenschaft einer injektiven Funktion ist es, dass sie immer eine **Umkehrfunktion** besitzt, die einem Funktionswert $f(x)$ eindeutig den Wert x des Arguments zuordnet. Die Umkehrfunktion einer Funktion f wird meistens mit f^{-1} bezeichnet. Für die injektive Funktion $f(x) = 2x + 1$ zum Beispiel können wir die Umkehrfunktion f^{-1} wie folgt bestimmen: Da $f(x)$ der Funktionswert y ist, setzen wir $f(x) = y$ und bekommen so die Gleichung $y = 2x + 1$. Wenn wir diese Gleichung nach x auflösen, bekommen wir die Vorschrift, um von einem beliebigen Funktionswert y wieder auf das Argument x zu schliessen.

$$\begin{array}{rcl} y = 2x + 1 & & | - 1 \\ y - 1 = 2x & & | : 2 \\ \frac{y-1}{2} = x & & \end{array}$$

Somit ist die Umkehrfunktion $f^{-1}: \mathbb{R} \rightarrow \mathbb{R}$ durch $f^{-1}(y) = \frac{y-1}{2}$ gegeben.

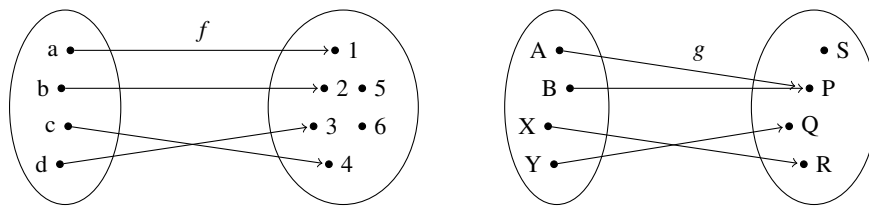


Abbildung 1.4 Die linke Darstellung zeigt eine injektive Funktion f . Die Funktion g – abgebildet auf der rechten Seite – ist dagegen nicht injektiv.

Aufgabe 1.9 Bestimme die Umkehrfunktion der linearen Funktion $f(x) = 6x - 8$.

Die Funktion f von $\{a, b, c, d\}$ nach $\{1, 2, 3, 4, 5, 6\}$ mit $f(a) = 1$, $f(b) = 2$, $f(c) = 4$ und $f(d) = 3$ ist eine injektive Funktion. Die visuelle Darstellung in Abbildung 1.4 zeigt, dass zu jedem Element der Wertemenge $\{1, 2, 3, 4, 5, 6\}$ höchstens ein Pfeil führt. Das heisst, auf keinen Funktionswert wird mehr als ein Element aus $\{a, b, c, d\}$ abgebildet. Diese Darstellung von Funktionen nennen wir **Mengendarstellung**.

Im Gegensatz dazu ist die Funktion g in Abbildung 1.4 nicht injektiv, da hier mehr als ein Element auf den gleichen Funktionswert abgebildet wird: Die Elemente A und B werden beide auf den Funktionswert P abgebildet, es gilt also $g(A) = g(B) = P$.

Wichtig ist, dass jedem Element der Menge A genau ein Element aus B zugeordnet wird. Bei den Mengendarstellungen, wie wir sie in Abbildung 1.4 haben, bedeutet dies, dass von jedem Element aus A genau ein Pfeil auf ein Element in B zeigen muss. Wenn aus einem oder mehreren Elementen aus A kein Pfeil nach B geht, dann handelt es sich nicht um eine Funktion, da eine Funktion definiert ist als eine Zuordnung, die *jedem* Argument $a \in A$ *eindeutig* einen Funktionswert $f(a) \in B$ zuordnet. Es handelt sich auch deshalb nicht um eine Funktion, wenn einem Element $a \in A$ mehr als ein Element aus B zugeordnet werden, da jedem Element *genau ein* Funktionswert zugeordnet sein muss. An der Mengendarstellung kann man sehr schnell erkennen, ob es sich um eine Funktion handelt oder nicht.

Ein weiterer Vorteil der Mengendarstellung ist, dass wir die Umkehrfunktion einer injektiven Funktion ganz einfach bestimmen können, indem wir die Richtung der Pfeile ändern. Dabei muss aber beachtet werden, dass wir nur dann eine Umkehrfunktion von B nach A erhalten, wenn in der ursprünglichen Funktion B keine Elemente enthält, zu denen kein Pfeil aus A führt. Eine Funktion besitzt also nur dann eine Umkehrfunktion, wenn auf jedes Element aus B ein Pfeil zeigt.

Die Funktion f in Abbildung 1.4 besitzt keine Umkehrfunktion, da bei einer Zuordnung von B nach A der Elemente $\{1, 2, 3, 4, 5, 6\}$ nach $\{a, b, c, d\}$ für die beiden Elemente 5 und 6 keine Funktionswerte bestimmt sind.

Aufgabe 1.10 Zeichne die folgenden Funktionen f jeweils in der Mengendarstellung auf und entscheide, ob es sich dabei um eine injektive Funktion handelt oder. Begründe deine Antwort.

- (a) $f: \{a, b, c\} \rightarrow \{X, Y, Z\}$, wobei $f(a) = Y$, $f(b) = X$ und $f(c) = Z$
- (b) $f: \{a, b, c\} \rightarrow \{A, B, C, D\}$, wobei $f(a) = B$, $f(b) = D$ und $f(c) = A$
- (c) $f: \{A, B, C\} \rightarrow \mathbb{N}$, mit $f(A) = 7$, $f(B) = 13$ und $f(C) = 7$

Aufgabe 1.11 Welche der folgenden Funktionen sind injektiv? Begründe deine Antworten beispielsweise mit der Darstellung als Funktionsgraph (falls die Funktion injektiv ist) oder finde zwei unterschiedliche Argumente, für die die Funktion den gleichen Funktionswert besitzt.

- (a) $f(x) = x^2$ für $f: \mathbb{R} \rightarrow \mathbb{R}$
- (b) $f(x) = x^2$ für $f: \mathbb{R}^+ \rightarrow \mathbb{R}^+$
- (c) $f(x) = \sin(x)$ für $f: \mathbb{R}^+ \rightarrow \mathbb{R}$
- (d) $f(x) = \cos(x)$ für $f: [0, 360] \rightarrow [-1, 1]$
- (e) $f(x) = 2^x$ für $f: \mathbb{R}^+ \rightarrow \mathbb{R}$
- (f) $f(x) = 2^x$ für $f: \mathbb{Z} \rightarrow \mathbb{R}$
- (g) $f(x) = \sqrt{x}$ für $f: \mathbb{R}^+ \rightarrow \mathbb{R}^+$
- (h) $f(x) = x^2 - 2x + 1$ für $f: \mathbb{R} \rightarrow \mathbb{R}$

Aufgabe 1.12 Eine Funktion $f: A \rightarrow B$ ist eine **monoton wachsende Funktion**, wenn für alle $a, b \in A$ mit $a < b$ gilt, dass $f(a) \leq f(b)$ ist. Ist jede monoton wachsende Funktion eine injektive Funktion?

Aufgabe 1.13 Eine Funktion $f: A \rightarrow B$ ist eine **streng monoton wachsende Funktion**, wenn für alle $a, b \in A$ mit $a < b$ gilt, dass $f(a) < f(b)$ ist. Begründe, weshalb eine streng monoton wachsende Funktion eine injektive Funktion ist.

Aufgabe 1.14 ★ Kann eine injektive Funktion $f: \mathbb{R} \rightarrow \mathbb{R}$ abwechselnd steigend und fallend sein?

Aufgabe 1.15 ★ Kann eine injektive Funktion $f: \mathbb{R} \rightarrow \mathbb{R}$ Extrema haben?

Codierungen

Zuvor haben wir darauf aufmerksam gemacht, dass wir in der Lehre der Geheimschriften besonders an injektiven Funktionen interessiert sind. Der Grund dafür ist, dass nur diejenigen Geheimtexte, die mittels einer injektiven Funktion chiffriert worden sind, eindeutig auf den Klartext zurückgeführt werden können. Deshalb ist es sinnvoll zu fordern, dass eine Chiffrierung eine injektive Funktion sein soll.

Chiffrierungen bilden Texte auf Texte ab – nämlich Klartexte auf Geheimtexte. Wie bei der Beschreibung der Chiffrierung von Polybios bereits erwähnt worden ist, dürfen die Alphabete des Klar- und des Geheimtextes jeweils unterschiedlich sein. Bei der Geheimschrift von Polybios wurden Buchstaben auf Zahlen abgebildet.

Wenn \mathcal{A} ein Alphabet ist, dann wird mit \mathcal{A}^* die Menge aller Texte bezeichnet, die aus den Symbolen aus \mathcal{A} zusammengestellt werden können. Mit jedem beliebigen Alphabet \mathcal{A} kann man auf diese Weise unendlich viele Texte schreiben. Somit ist die Menge der Texte \mathcal{A}^* mit den Symbolen aus \mathcal{A} unendlich gross. Zum Beispiel können wir mit dem Alphabet $\mathcal{A} = \{0, 1\}$, das nur aus den beiden Symbolen 0 und 1 besteht, die folgende unendliche Menge von Texten schreiben:

$$\mathcal{A}^* = \{0, 1, 00, 01, 10, 11, 000, 001, 010, 011, \dots\}.$$

Hinweis für die Lehrperson Weil wir die Grossbuchstaben des lateinischen Alphabets meistens für Mengen verwenden, wäre es verwirrend, diese auch für die Bezeichnung von Alphabeten zu brauchen. Zur Unterscheidung benutzen wir deshalb für Alphabete die Symbole \mathcal{A} , \mathcal{B} , \mathcal{C} usw. oder aber beschreibende Wörter wie Lat oder Greek.

Aufgabe 1.16 Für $\mathcal{A} = \{0, 1\}$ haben wir die Texte aus \mathcal{A}^* der Reihe nach aufgelistet, indem wir zuerst die kurzen und dann die längeren Texte aufgeführt haben. Für gleich lange Texte haben wir lexikographisch (wie in einem Wörterbuch) sortiert.

Schreibe die nächsten 10 Texte aus \mathcal{A}^* auf.

Aufgabe 1.17 Sei $\mathcal{B} = \{1, 2, 3, 4, 5\}$ ein Alphabet. Schreibe die 40 kürzesten Texte aus \mathcal{B}^* auf.

Wenn wir über Codierungen sprechen, unterscheiden wir zwischen der Codierung von Symbolen und der Codierung von Texten.

Seien \mathcal{A} und \mathcal{B} zwei Alphabete. Jede injektive Funktion von \mathcal{A} nach \mathcal{B}^ ist eine **Codierung von Symbolen** aus \mathcal{A} mittels Texten aus \mathcal{B}^* .*

Die Abbildung 1.2 beschreibt eine Codierung PolC des griechischen Alphabets

$$\text{Greek} = \{A, B, \Gamma, \Delta, E, Z, H, \Theta, I, K, \Lambda, M, \\ N, \Xi, O, \Pi, P, \Sigma, T, Y, \Phi, X, \Psi, \Omega\}$$

mittels Texten aus $\{1, 2, 3, 4, 5\}^*$. Somit gilt $\text{PolC}(A) = 11$, $\text{PolC}(B) = 12$, $\text{PolC}(\Gamma) = 13$, \dots , $\text{PolC}(\Psi) = 53$, $\text{PolC}(\Omega) = 54$. Diese Codierung von einzelnen Symbolen ist die Basis der Geheimschrift von Polybios, da jedes Symbol eindeutig mit zwei Ziffern chiffriert wird.

Alle Texte aus \mathcal{B}^* , die zur Codierung eines Symbols aus \mathcal{A} verwendet werden, nennt man **Codewörter**. Für die Geheimschrift von Polybios sind 11, 12, 13, \dots , 53, 54 die 24 Codewörter für die 24 Symbole des griechischen Alphabets.

Die Menge aller Codewörter für ein Alphabet \mathcal{A} bezüglich einer Codierung f wird **Code** für \mathcal{A} bezüglich f genannt und wird mit $\text{Code}(\mathcal{A}, f)$ bezeichnet. Somit haben wir zum Beispiel:

$$\text{Code}(\text{Greek}, \text{PolC}) = \{11, 12, 13, 14, 15, \dots, 54\}.$$

Die Codierung von einzelnen Buchstaben kann für die Codierung von Texten verwendet werden.

*Seien \mathcal{A} und \mathcal{B} zwei Alphabete. Eine **Codierung von Texten** aus \mathcal{A}^* mittels Texten aus \mathcal{B}^* ist jede injektive Funktion von \mathcal{A}^* nach \mathcal{B}^* .*

Das Chiffrierungsverfahren der Geheimschrift von Polybios entspricht einer Codierung. Wenn wir den Geheimtext in Stücke der Länge zwei schneiden und jeden Text (Codewort) von zwei Ziffern dem entsprechenden Symbol des griechischen Alphabets zuordnen, dann erhalten wir eindeutig den ursprünglichen Klartext. Dass die Chiffrierung von Polybios die Umsetzung einer injektiven Funktion ist, verdanken wir der Tatsache, dass alle Codewörter für die Buchstaben die gleiche Länge haben. Dadurch können wir eindeutig den Geheimtext in Stücke gleicher Länge zerlegen und mit diesen Stücken (Codewörtern) die ursprünglichen Symbole des Klartextes bestimmen.

Die Situation ändert sich, wenn bei der Chiffrierung einzelner Buchstaben nicht mit genügender Vorsicht vorgegangen wird. Betrachten wir zum Beispiel das lateinische Alphabet

$$\text{Lat} = \{A, B, C, D, \dots, X, Y, Z\}$$

von 26 Buchstaben. Wir definieren damit eine Chiffrierung

$$f: \text{Lat} \rightarrow \{0, 1, 2, \dots, 9\}^*$$

der Symbole von Lat durch die Abbildung der einzelnen Buchstaben $\square \in \text{Lat}$ auf die Ordnung des betreffenden Buchstabens $+1$. Das heisst $f(\square) = \text{Ord}(\square) + 1$. Die Ordnung $\text{Ord}(\square)$ eines Symbols \square ist dessen Position in unserer Auflistung der Symbole des Alphabets, wobei die Positionierung mit 0 startet. Somit gilt

$$f(A) = 1, \quad f(B) = 2, \quad \dots, \quad f(Z) = 26.$$

Die Zahlen $1, 2, 3, \dots, 26$ als Texte aus $\{0, 1, \dots, 9\}^*$ sind die Codewörter von f . Wenn wir f zur Chiffrierung der Texte aus Lat^* verwenden, dann wird unsere Chiffrierung keine Codierung. Betrachten wir beispielsweise den Geheimtext

114141.

Im Folgenden sehen wir drei mögliche Klartexte abhängig von der Einteilung des Geheimtextes in Codewörter:

$$\begin{array}{cccc|cccc|cccc} 1 & 14 & 14 & 1 & 11 & 4 & 1 & 4 & 1 & 11 & 4 & 14 & 1 \\ A & N & N & A & K & D & A & D & A & K & D & N & A \end{array}$$

Aufgabe 1.18 Finde eine andere Zerlegung des Geheimtextes 114141 in Codewörter, so dass ein neuer Klartext resultiert.

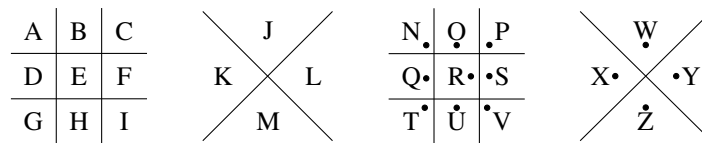


Abbildung 1.5 Das Schema für die Chiffrierung von Buchstaben mit der Geheimschrift FREI-MAURER. Die Buchstaben werden jeweils durch die Linien und Punkte in ihrer Umgebung chiffriert. So ist zum Beispiel $A = \sqcup$, $E = \square$, $M = \wedge$, $R = \square$, $Y = \lessdot$.

Aufgabe 1.19 Kannst du die Codierung der Symbole aus Lat leicht modifizieren (ohne dabei das Prinzip der Codierung durch die Ordnung zu verletzen), so dass aus der Chiffrierung von Klartexten aus Lat* eine Codierung wird?

Aufgabe 1.20 Betrachte die folgende Chiffrierung der Texte aus Lat*, in der die Codierung von Symbolen nicht nur vom Symbol selbst abhängt, sondern auch vom vorhergehenden Symbol im Klartext:

Ein Symbol aus Lat mit der Ordnung $i \in \{0, 1, \dots, 25\}$ wird folgendermassen codiert:

1. Wenn links von diesem Symbol im Klartext kein Vokal steht (das gilt natürlich auch für das erste Symbol des Klartextes), dann ersetze das Symbol durch das Symbol mit der Ordnung $25 - i$ aus Lat. So wird zum Beispiel A durch Z (Z durch A), B durch Y (Y durch B), C durch X (X durch C) usw. ersetzt.
2. Wenn aber vor dem Symbol im Klartext ein Vokal steht, ersetze das Symbol durch das nachfolgende Symbol in der Ordnung. So wird zum Beispiel A durch B, B durch C usw. ersetzt. Wenn man am Ende angekommen ist, dann beginnt man wieder von vorne. Man ersetzt also das Z durch A.

Somit wird der Klartext ANNA in den Geheimtext ZOMZ umgewandelt.

Kannst du den Geheimtext KLMBYRPT dechiffrieren? Entspricht diese Chiffrierung einer Codierung von Texten aus Lat* durch Texte aus Lat*?

Aufgabe 1.21 ATBASCH ist eine hebräische Geheimschrift, die um 600 v. u. Z. in Palästina verwendet wurde. Bei ATBASCH wird der erste Buchstabe des Alphabets (A) durch den letzten Buchstaben (Z) codiert, der zweite Buchstabe (B) durch den zweitletzten Buchstaben (Y) usw. Deciffriere den folgenden mit ATBASCH chiffrierten Geheimtext. Für die bessere Lesbarkeit wurden die Buchstaben gruppiert. Die Gruppierung hat nichts mit den tatsächlichen Wörtern und Leerzeichen zu tun.

```
ADVRW RMTVH RMWFM VMWOR XSWZH FMREV IHFNF MWWRV NVMHX
SORXS VWFNN SVRGZ YVIYV RNFMR EVIHF NYRMR XSNRI MRXSG
TZMAH RXSVI
```

Dieser Geheimtext basiert auf einem Zitat von Albert Einstein (1879–1955).

Die meisten alten Geheimschriften basieren auf der Codierung der Symbole durch einzelne andere Symbole. Die Freimaurer codierten im 16. Jahrhundert die Symbole mit den Bildsymbolen, wie in Abbildung 1.5 dargestellt. Dabei wird jeder Buchstabe durch ein Symbol ersetzt, das sich aus den Linien und Punkten in der Umgebung des Buchstabens

im Schema ergibt.

Somit wird zum Beispiel der Klartext FREIMAURER durch den folgenden Geheimtext chiffriert:

□ □ □ ▯ ^ ▯ ▯ □ □ □.

Aufgabe 1.22 Dechiffriere den folgenden mit FREIMAURER chiffrierten Text:

> □ < ▯ ▯ < ▯ ▯ ▯ □.

Aufgabe 1.23 Beschreibe FREIMAURER mit dem Schema der Geheimschriften. Deine Beschreibung soll das Klartextalphabet, das Geheimtextalphabet, das Chiffrierungs- und das Dechiffrierungsverfahren beinhalten.

Aufgabe 1.24 Wie wird mittels Morsezeichen chiffriert? Handelt es sich um eine Codierung?

Kryptosysteme

Die Geheimschriften basieren auf einem gemeinsamen Geheimnis der kommunizierenden Personen. Dieses Geheimnis ist die „Art und Weise“ der Chiffrierung, die üblicherweise auch die „Art und Weise“ der Dechiffrierung bestimmt. Keine dieser Geheimschriften kann jedoch lange verwendet werden, ohne dass man dabei das Risiko eingeht, das Geheimnis zu lüften und damit den Geheimtext für einen Gegner lesbar zu machen. Deshalb wird eine grössere Vielfalt von Chiffrierungen innerhalb eines Chiffrierungssystems bevorzugt. Diese erwünschte Vielfalt geben uns die **Kryptosysteme**. Die Geheimschriften sind durch eine injektive Funktion Chiff mit

$$\text{Chiff}(\text{Klartext}) = \text{Geheimtext}$$

bestimmt. Somit ist der Klartext das einzige Argument der Chiffrierungsfunktion Chiff .

Bei Kryptosystemen sprechen wir oft über **Verschlüsselung** statt über Chiffrierung, weil bei den Kryptosystemen die Verschlüsselungsfunktion Ver zwei Argumente hat: den Klartext und den Schlüssel. Der **Schlüssel** ist das zweite Geheimnis, das sich die kommunizierenden Personen teilen. Der Schlüssel kann verändert werden, ohne dass dabei die Verschlüsselungsart verändert wird. Damit enthält ein Kryptosystem mit der Verschlüsselung

$$\text{Ver}(\text{Klartext}, \text{Schlüssel}) = \text{Geheimtext}$$

durch die freie Wahl von Schlüsseln eine Vielfalt von Geheimschriften. Genauer ist für jeden festen Schlüssel s die Funktion Ver_s definiert durch

$$\text{Ver}_s(\text{Klartext}) = \text{Ver}(\text{Klartext}, s)$$

eine Chiffrierung. Das heisst, wenn der Schlüssel nicht verändert wird, also fest bleibt, ist das Kryptosystem eine gewöhnliche Chiffrierung.

Das Kryptosystem CAESAR

Das einfachste Kryptosystem, das in der Antike vom römischen Feldherrn Gaius Julius Caesar verwendet wurde, ist CAESAR. Dieses System nutzt die uns bereits bekannte Möglichkeit, die Symbole des lateinischen Alphabets in einer festen Ordnung aufzulisten. Jeder Buchstabe des Klartextes wird durch einen anderen Buchstaben im Geheimtext codiert. Vor der Ausführung der eigentlichen Kommunikation einigen sich der Sender und der Empfänger auf einen geheimen Schlüssel. Der Schlüssel ist eine Zahl $i \in \{0, 1, \dots, 25\}$ und wird als Abstand (in der Auflistung der Symbole des Alphabets) zwischen den Buchstaben des Klartextes und den entsprechenden Buchstaben im Geheimtext betrachtet.

Wenn der Schlüssel zum Beispiel $i = 3$ ist, dann wird A mit $\text{Ord}(A) = 0$ unabhängig von seiner Position im Klartext durch den Buchstaben D mit $\text{Ord}(D) = 3$ codiert, weil $\text{Ord}(D) - \text{Ord}(A) = 3$. Weiter wird B durch E, C durch F usw. codiert. Für die letzten drei Buchstaben X, Y und Z mit $\text{Ord}(X) = 23$, $\text{Ord}(Y) = 24$ und $\text{Ord}(Z) = 25$ werden zur Codierung die noch freien Symbole A, B und C verwendet. Man geht für die Codierung also wieder an den Anfang des Alphabets zurück.

Allgemein ausgedrückt bedeutet die Verwendung eines Schlüssels i , dass jeder Buchstabe mit dem um i Positionen nach hinten verschobenen Buchstaben im Alphabet codiert wird. Wenn für einen Buchstaben \square aus Lat, $\text{Ord}(\square) + i > 25$ ist, dann wird \square durch den Buchstaben mit der Ordnung $\text{Ord}(\square) + i - 25$ codiert. Das bedeutet, wenn man am Ende des Alphabets angelangt ist, beginnt man einfach wieder von vorne.

Die formale Beschreibung einer Geheimschrift besteht aus den folgenden vier Angaben: dem *Klartextalphabet*, dem *Geheimtextalphabet*, dem *Verschlüsselungs-* und *Entschlüsselungsverfahren*. Bei der Beschreibung von Kryptosystemen kommt zusätzlich noch die *Schlüsselmenge* hinzu. Wir gehen davon aus, dass der geheime Schlüssel vorher vereinbart wurde. Wir können also Kryptosysteme analog zu Geheimschriften mit dem **Schema der Kryptosysteme** beschreiben. Die formale Beschreibung von CAESAR sieht damit wie folgt aus:

Kryptosystem CAESAR	
Klartextalphabet:	Lat
Geheimtextalphabet:	Lat
Schlüsselmenge:	$\{0, 1, 2, \dots, 25\}$
Verschlüsselung:	Ersetze für jeden vorher vereinbarten Schlüssel i jeden Buchstaben \square des Klartextes durch den Buchstaben $\triangle \in \text{Lat}$ mit $\text{Ord}(\triangle) = \text{Ord}(\square) + i$ falls $\text{Ord}(\square) + i \leq 25$ oder mit $\text{Ord}(\triangle) = \text{Ord}(\square) + i - 25$ falls $\text{Ord}(\square) + i > 25$.
Entschlüsselung:	Ersetze jeden Buchstaben \triangle des Geheimtextes durch den Buchstaben $\square \in \text{Lat}$ mit $\text{Ord}(\square) = \text{Ord}(\triangle) - i$ falls $\text{Ord}(\triangle) - i \geq 0$ oder mit $\text{Ord}(\square) = \text{Ord}(\triangle) - i + 25$ falls $\text{Ord}(\triangle) - i < 0$.

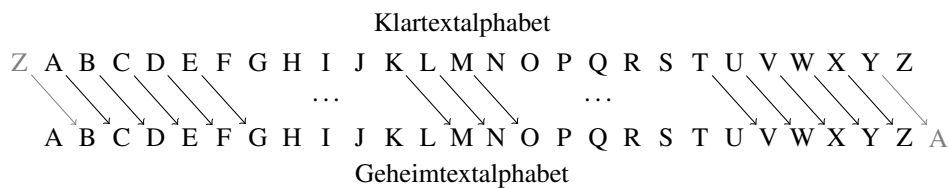


Abbildung 1.6 Darstellung der Verschlüsselung mit CAESAR mit dem Schlüssel 2.

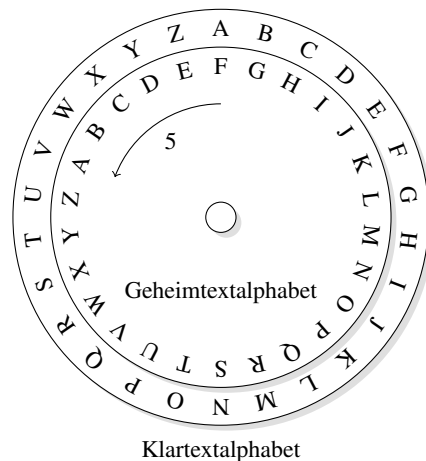


Abbildung 1.7 Mit diesen beiden Scheiben kann die Ver- und Entschlüsselung mit CAESAR einfach ausgeführt werden. Der Schlüssel (hier 5) bestimmt die Anzahl der Buchstaben, um die die innere Scheibe im Gegenuhrzeigersinn gedreht wird. Danach werden die Klartextbuchstaben auf der äusseren Scheibe durch die Geheimtextbuchstaben der inneren Scheibe codiert.

Die Darstellung in Abbildung 1.6 zeigt die Codierung der Buchstaben im Klartext durch die um den Schlüssel 2 verschobenen Buchstaben. So wird beispielsweise der Buchstabe A durch C und der Buchstabe B durch D codiert. Die Darstellung in Abbildung 1.7 zeigt die Verschiebung mit dem Schlüssel 5 anhand zweier drehbarer Ränder. Man kann diese Räder aus Karton basteln und mit einer Verschlussklammer zusammenheften. Dann kann man die innere Scheibe zum Beispiel um fünf Buchstaben im Gegenuhrzeigersinn drehen und bekommt so die Codewörter mit dem Schlüssel 5. Diese Darstellungsform wird nach ihrem Erfinder **Caesar-Scheibe** genannt.

Wenn wir zum Beispiel den Klartext JULIUS mit dem Schlüssel 5 verschlüsseln, erhalten wir den folgenden Geheimtext:

OZQNZX.

Da der Buchstabe J die Ordnung 9 hat, wird daraus der Buchstabe O mit der Ordnung $9 + 5 = 14$ usw.



Abbildung 1.8 Dieses Kommunikationsschema zeigt den Kommunikationsschritt, bei dem die Übertragung einer verschlüsselten Nachricht gezeigt wird. Um den Klartext zu verschlüsseln oder den Kryptotext zu entschlüsseln brauchen beide Kommunikationspartner zusätzlich einen gemeinsamen geheimen Schlüssel.

Aufgabe 1.25 Entschlüssele den Kryptotext

UZVMVIELEWKZJKUVJYVIQVEJXIFVJJKVWVZEUZE ,

der mit CAESAR und dem Schlüssel 17 verschlüsselt worden ist.

Aufgabe 1.26 Der folgende Kryptotext ist mit dem Kryptosystem CAESAR verschlüsselt worden. Entschlüssele den Kryptotext, indem du den Schlüssel bestimmst.

MIFUHAYXCYMIHHYMWBYCHNMCHXQCLHCWBNTOMJUYN .

Aufgabe 1.27 Um das Jahr 1980 herum wurde in den Newsgroups des Internets die ROT13-Chiffrierung verwendet, um zum Beispiel Pointen von Witzen zu verschleiern. ROT13 ist eine Geheimschrift, die dem Kryptosystem CAESAR unter der Verwendung eines festen Schlüssels mit dem Wert 13 entspricht.

Was ist das Besondere am Schlüssel mit dem Wert 13 beim Kryptosystem CAESAR?

Das Kryptosystem CAESAR hat 26 Schlüssel und enthält damit 26 Geheimschriften, jeweils eine pro Schlüssel. Natürlich lohnt es sich nicht den Schlüssel mit dem Wert 0 zu verwenden, weil dann der Geheimtext identisch mit dem Klartext ist. Wir behandeln 0 trotzdem als einen potenziellen Schlüssel, weil wir später CAESAR mit einem anderen Kryptosystem kombinieren werden und sich dann die 0 als nützlich erweisen wird.

Im Folgenden werden wir uns nur noch mit Kryptosystemen beschäftigen. Wie wir später erklären werden, bieten einzelne Geheimschriften zu wenig Sicherheit und sind deshalb für die meisten Kommunikationsaufgaben nicht verwendbar. Das Schema der Verwendung von Kryptosystemen aus Abbildung 1.8 erhalten wir durch eine leichte Modifikation des Schemas für Geheimschriften. Für die Chiffrierung im Kryptosystem verwendet der Sender einen Schlüssel, weswegen wir von **Verschlüsselung** sprechen. Der Empfänger braucht ebenfalls den Schlüssel zur Dechiffrierung, deswegen sprechen wir von der **Entschlüsselung**. Für das Fachwort Geheimtext haben wir auch ein neues

Synonym – Kryptotext.

Wenn wir ein Kryptosystem vollständig beschreiben wollen, dann müssen wir Folgendes angeben:

- (1) *das Alphabet der Klartexte,*
- (2) *das Alphabet der Kryptotexte,*
- (3) *die Menge aller Schlüssel,*
- (4) *das Verschlüsselungsverfahren*

$$\text{Ver}(\text{Klartext}, \text{Schlüssel}) = \text{Kryptotext}$$

und

- (5) *das Entschlüsselungsverfahren*

$$\text{Ent}(\text{Kryptotext}, \text{Schlüssel}) = \text{Klartext}.$$

Die letzten drei Teile der Beschreibung eines Kryptosystems können geheim gehalten werden. Bei einer grossen Vielfalt von Schlüsseln kann es reichen, wenn nur der Schlüssel geheim gehalten wird. Das ist aber sicherlich bei CAESAR nicht der Fall, weil es kein grosser Aufwand ist, alle 25 nichttrivialen Schlüssel³ auszuprobieren.

Das Kryptosystem SKYTALE

Das älteste bekannte Kryptosystem wurde ungefähr 500 Jahre v. u. Z. in Sparta entwickelt und verwendet. Die Spartaner waren in ihren zahlreichen Schlachten immer wieder darauf angewiesen, Befehle und Nachrichten zu übermitteln, die vor dem Gegner geheim gehalten werden mussten. Dazu verwendeten die Spartaner als Kryptosystem die SKYTALE.

Dieses System setzt voraus, dass Sender und Empfänger jeweils in Besitz eines Holzstabes mit genau demselben Durchmesser sind. Um eine Nachricht zu verschlüsseln wickelt der Sender einen schmalen Papierstreifen spiralartig um den Holzstab. Die Spartaner haben damals Papyrus oder Pergament benutzt. Im nächsten Schritt kann das Papier mit der geheimen Nachricht beschrieben werden, und zwar von links nach rechts, so dass auf jeder Windung nur genau ein Buchstabe oder ein Leerzeichen steht. In Abbildung 1.9 wird eine Nachricht aus Sparta gezeigt, die mittels SKYTALE verschlüsselt worden ist. Die Spartaner wollten ihren Verbündeten die folgende Nachricht übermitteln: „*Morgen beginnt die grosse Schlacht. Wir werden bei Sonnenaufgang vom Osten her angreifen.*“

³Die nichttrivialen Schlüssel sind alle Schlüssel mit Ausnahme von jenem mit dem Wert 0. Ein trivialer Schlüssel ist ein naheliegender Schlüssel. In unserem Fall ist es also der Schlüssel mit dem Wert 0, weil bei einer solchen Verschlüsselung der Kryptotext dem Klartext entspricht.

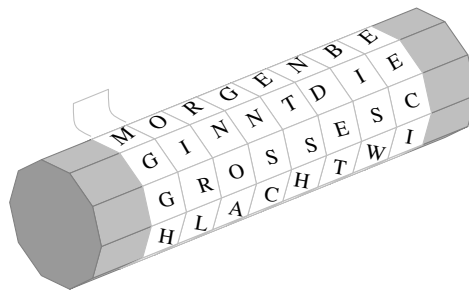


Abbildung 1.9 Die Skytale war eines der ersten Kryptosysteme und wurde ca. 500 v. u. Z. von den Spartanern entwickelt und verwendet.

Bevor die Nachricht auf den Papierstreifen geschrieben wird, muss man noch alle Leerzeichen und Satzzeichen entfernen. Die einzigen Leerzeichen, die nach dem Verschlüsseln übrig bleiben, sind die Leerzeichen am Schluss des Textes, wenn die letzte Zeile auf der Skytale nicht mehr gefüllt werden kann. Natürlich ist die Nachricht, sobald man den Papierstreifen wieder vom Holzstab entfernt, nicht mehr auf den ersten Blick lesbar. Es ist dann nur noch ein langer Papierstreifen mit vielen Buchstaben. Ein Empfänger mit einem Holzstab mit dem gleichen Durchmesser kann den Klartext jedoch ganz leicht wiederherstellen, indem er den Papierstreifen spiralartig um sein Holzstück wickelt und die Nachricht so entschlüsselt.

Natürlich könnte man den Text auch ohne Holzstab entschlüsseln. Wenn man weiss, wie viele Zeichen auf einer Windung sind, dann ist dies auch gar nicht schwer. Wenn der Holzstab beispielsweise einen Umfang von sechs Buchstaben hat, dann liest man einfach jeden sechsten Buchstaben auf dem Papierstreifen ab: zuerst die Buchstaben an den Positionen 1, 7, 13, 19, 25, ..., dann die Buchstaben an den Positionen 2, 8, 14, 20, 26, ... und so weiter. Als Letztes werden die Buchstaben an den Positionen 6, 12, 18, 24, 30, ... gelesen. Damit ist der Kryptotext auf dem Papierstreifen entschlüsselt. Der Schlüssel beim SKYTALE ist die Anzahl der Buchstaben, die beim Lesen „übersprungen“ werden, also die Anzahl der Buchstaben auf einer Windung.

Bei der Verschlüsselung mit SKYTALE muss man aber etwas aufpassen. Bevor wir das Problem aufzeigen, möchten wir uns genau anschauen, wie man ohne einen Holzstab verschlüsselt. Dazu betrachten wir nochmals das Beispiel aus Abbildung 1.9. Wir sehen, dass der Papierstreifen acht Mal um den Holzstab gewickelt worden ist. Das ergibt acht Windungen. Also schreiben wir unseren Text einfach zeilenweise in acht Spalten auf und bekommen die somit die Figur in Abbildung 1.10. Der Schlüssel ist die Anzahl der Zeilen. Der Kryptotext besteht aus der Folge der spaltenweise gelesenen Buchstaben, also

```
MGGHREAOEFOIRLWUMRERNOAESFOANGSCROGSN ETSHDNATG NDET
ENNER BISWNEGNE EECIBNVHI
```

für das Beispiel in Abbildung 1.10.

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

Abbildung 1.10 Ein mit SKYTALE verschlüsselter Text mit Schlüssel 10.

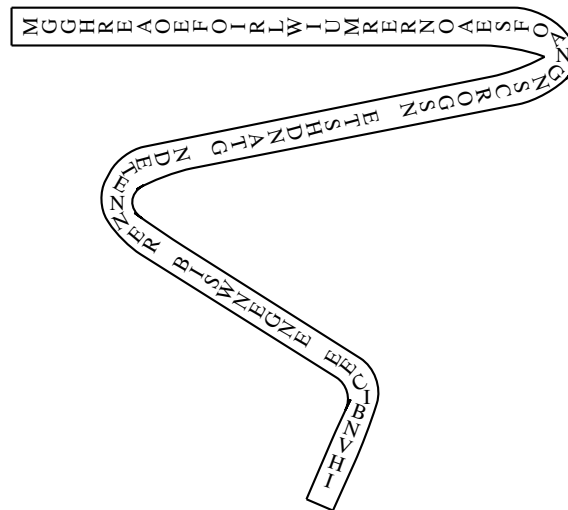


Abbildung 1.11 Der Papierstreifen der Skytale.

Wir sehen, dass am Schluss der fünften, sechsten, siebten und achten Spalte jeweils ein Leerzeichen steht, weil der Text nicht das ganze Rechteck ausfüllt. Im Kryptotext (das heisst auf dem abgewickelten Streifen, siehe Abbildung 1.11) sieht man die Leerzeichen natürlich auch.

Aufgabe 1.28 Nehmen wir an, du findest den Papierstreifen aus Abbildung 1.11 auf dem Boden und du weisst, dass der Text mit SKYTALE verschlüsselt worden ist. Den Schlüssel kennst du aber nicht. Inwiefern helfen dir die Leerzeichen, den Text mit wenigen Handgriffen zu entschlüsseln? Wie könnten die Spartaner das Problem mit den Leerzeichen umgehen, also einen Kryptotext schreiben, der keine Leerzeichen enthält?

Um die Leerzeichen zu vermeiden gibt es viele Möglichkeiten. In unserem Beispiel haben wir einen Text von 75 Buchstaben. Wenn man den Schlüssel frei wählen darf – was normalerweise der Fall ist, weil man ja die Buchstabengrösse der Anzahl der Zeilen

```

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

```

Abbildung 1.12 Ein mit SKYTALE verschlüsselter Text mit Schlüssel 5.

anpassen kann –, könnte man zum Beispiel 5 wählen, damit man genau 15 Spalten bekommt, wie in Abbildung 1.12. Die Leerzeichen sind also verschwunden. Was passiert aber, wenn der Schlüssel vorgegeben ist? Wenn man ohne einen Holzstab mit SKYTALE verschlüsseln möchte, muss man zuerst die Anzahl der Spalten berechnen.

Kryptosystem SKYTALE

Klartextalphabet:	Lat
Geheimtextalphabet:	Lat
Schlüsselmenge:	$\{1, 2, \dots, n\}$, wobei n die Länge des Klartextes ist.
Verschlüsselung:	Sei $s \in \{1, 2, \dots, n\}$ der Schlüssel. Schreibe den Klartext zeilenweis in $\lceil \frac{n}{s} \rceil$ (das heisst, berechne $\frac{n}{s}$ und runde auf die nächste ganze Zahl auf) Spalten auf. Der Kryptotext besteht aus der Folge der spaltenweise gelesenen Buchstaben in dieser Anordnung des Klartextes.
Entschlüsselung:	Schreibe den Text spaltenweise in s Zeilen auf. Den Klartext bekommst du, indem du den so angeordneten Text zeilenweise abliest.

Aufgabe 1.29 Die Spartaner wollen einen Text mit 75 Buchstaben mit SKYTALE verschlüsseln. Sie haben zwar keinen Holzstab zur Hand, aber sie beschliessen, dass sie den Schlüssel 7 wählen. Wieviele Spalten wird es geben, wenn sie so wenig Leerzeichen wie nur möglich haben möchten?

Aufgabe 1.30 Auf einem Papierstreifen steht der folgende mit SKYTALE verschlüsselte Kryptotext:

```

ETIFIITNUTNFGENKURRELEODIERSILIMSEANIE
MRECREMRHSNSSAPSTCBRCRHEUHORRNHNIEGEG

```

- Welches ist hier der Schlüssel?
- Wie lautet der Klartext?
- Wie viele Schlüssel müssen hier im schlimmsten Fall probiert werden, um den richtigen zu finden? Das heisst, wie viele mögliche Schlüssel gibt es?

Die Verschlüsselung mit SKYTALE ist ein Beispiel für eine Verschlüsselung, bei der die Buchstaben im Kryptotext die gleichen sind wie im Klartext, aber an einer anderen Stelle (Position des Textes) stehen. Um die Buchstaben zu vertauschen kann man aber auch noch andere Vorgehensweisen wählen. Man könnte zum Beispiel im Rechteck

M O R E N I S T E R R O S E T A G
 R G E N I S T E R R O S E T A G
 G E N I S T E R R O S E T A G

Abbildung 1.13 Eine andere Art den Klartext anzuordnen

aus Abbildung 1.12 die Spalten nicht immer von oben nach unten ablesen, sondern beispielsweise jede zweite Spalte von unten nach oben ablesen. Wir würden dann den Kryptotext

```
MEWNTEEIGORRRNNHAWOGESEUERFRSNBEDGANAE
SEGCNNGRGBHINLEVEIOIANTCSMFEOOHDITNSN
```

erhalten. Man könnte sogar den Klartext von Anfang an ganz anders anordnen, wie zum Beispiel in Abbildung 1.13. Den Kryptotext bekommt man dann zum Beispiel, wenn man die Buchstaben zeilenweise in dieser Anordnung abliest.

```
MIGTONSRREARETEOSGGDS
```

Aufgabe 1.31 Wie kann man diesen Kryptotext wieder entschlüsseln?

Aufgabe 1.32 Erfinde noch ein weiteres Verschlüsselungsverfahren, bei dem nur die Buchstaben vertauscht werden, und beschreibe es mit dem Schema für Kryptosysteme.

Die Verfahren CAESAR und SKYTALE basieren auf zwei ganz verschiedenen Verschlüsselungsideen. Während das Verfahren von CAESAR eine Codierung der einzelnen Buchstaben ist, wo Symbol für Symbol ersetzt wird, werden beim Verfahren der SKYTALE überhaupt keine Buchstaben ersetzt, sondern nur die Positionen der Symbole im Text verändert.

Aufgabe 1.33 Warum entspricht die Verschlüsselung der SKYTALE mit einem festen Schlüssel einer injektiven Funktion?

Die Kryptosysteme CAESAR und SKYTALE haben beide eine kleine Anzahl von möglichen Schlüsseln. Das bedeutet natürlich, dass jemand, der nicht im Besitz des Schlüssels ist, aber über das verwendete Kryptosystem Bescheid weiss, schnell einen Schlüssel nach dem anderen durchprobieren kann. Im schlimmsten Fall muss er alle Schlüssel ausprobieren, aber wenn die Anzahl Schlüssel eines Kryptosystems klein ist, hält sich der Aufwand in Grenzen.



Abbildung 1.14 Das Kryptosystem RICHÉLIEU. Links ist eine Lochkarte für einen Klartext mit zwanzig Buchstaben abgebildet. Wird die Lochkarte auf den Kryptotext gelegt, der in der Mitte dargestellt ist, erhält man den Klartext, der rechts abgebildet ist.

Das Kryptosystem RICHÉLIEU

Das Kryptosystem RICHÉLIEU, das im 17. Jahrhundert von Kardinal Richelieu erfunden worden ist, ist im Gegensatz zu den beiden vorher beschriebenen Systemen ein Kryptosystem mit sehr vielen möglichen Schlüsseln. Die Folge davon ist, dass das System nicht einfach mittels Durchprobieren aller möglichen Schlüssel zu knacken ist. Um mit RICHÉLIEU zu verschlüsseln, verwendet man als Schlüssel eine Lochkarte wie in Abbildung 1.14 dargestellt. Das ist eine Karte mit Feldern, die in einer bestimmten Anzahl von Zeilen und Spalten angeordnet sind. Einige dieser Felder auf der Lochkarte sind Löcher. Die Anzahl der Löcher muss genau der Länge des Klartextes, der verschlüsselt werden soll, entsprechen. Die Lochkarte dient als Schablone. Um zu verschlüsseln, wird diese Lochkarte auf eine leere Karte gelegt, und in einem ersten Schritt wird der Klartext von links nach rechts in diese Lochfelder geschrieben. In einem zweiten Schritt wird die Schablone entfernt, und die noch nicht beschriebenen Felder werden mit irgendwelchen Buchstaben aus dem Alphabet aufgefüllt, so dass schliesslich die ganze Karte voll ist, wobei in jedem Feld ein Buchstabe steht (siehe Abbildung 1.14). Diese Karte mit einem Buchstaben an jeder Position ist der Kryptotext. Man kann also nicht mehr unterscheiden, welcher Buchstabe zum Klartext gehört und welcher später hinzugefügt worden ist. Auf den ersten Blick scheint das Ganze wie ein grosses Durcheinander von Buchstaben. Einem Besitzer des Schlüssels beziehungsweise der Lochkarte ist es jedoch ganz leicht möglich diesen Kryptotext zu entschlüsseln: Er legt die Lochkarte wie eine Schablone auf den Kryptotext und liest die Buchstaben, die durch die Lochkarte nicht abgedeckt sind, zeilenweise von links nach rechts ab. Auf diese Weise erhält er den Klartext (siehe Abbildung 1.14).

Aufgabe 1.34 Wie viele Schlüssel hat das Kryptosystem RICHÉLIEU bei einer Lochkarte von $n \times m$ Feldern?

Zusammenfassung

Die Verwendung von abstrakten Zeichen hat zur Entwicklung der Schriften geführt. Die Basis einer Schrift ist ein Alphabet. Ein Alphabet ist eine Menge von Zeichen, die

auch Buchstaben oder Symbole genannt werden. Texte in einer Schrift sind Folgen von Buchstaben des Alphabets der Schrift.

Die zwei Parteien einer Kommunikation bezeichnen wir als Sender und Empfänger. Das Ziel des Senders ist es, eine Nachricht an den Empfänger zu schicken. Bei der Nachricht handelt es sich um einen Text in einer natürlichen Sprache, welche beide verstehen. Ein solcher Text wird Klartext genannt. Da der Sender verhindern will, dass seine Nachricht auf dem Weg zum Empfänger von irgendjemandem gelesen wird, wandelt er den Klartext in einen Kryptotext (Geheimtext) um. Diese Umwandlung wird Chiffrierung genannt. Die Chiffrierung ist im Allgemeinen ein Algorithmus, der einen gegebenen Klartext in einen Kryptotext umwandelt. Dieser Kryptotext wird anschliessend vom Empfänger mit einem Dechiffrierungsverfahren wieder in den ursprünglichen Klartext zurückverwandelt. Zu bemerken ist, dass beim Chiffrieren das Alphabet des Klartextes und das Alphabet des Kryptotextes unterschiedlich sein dürfen.

Jede Geheimschrift ist durch die Chiffrierung und die Dechiffrierung eindeutig bestimmt. Beispiele für Geheimschriften sind POLYBIOS und FREIMAURER.

Man muss unterscheiden zwischen Codierungen von Symbolen und Codierungen von Texten. Wenn die einzelnen Buchstaben unabhängig von ihrer Umgebung im Klartext auf Buchstaben oder Texte aus einem Alphabet abgebildet werden, handelt es sich um eine Codierung von Symbolen des Klartextalphabets. Mit dieser Codierung von Symbolen kann man dann ganze Texte codieren.

Von Codierungen wird gefordert, dass sie injektive Funktionen sind. Eine injektive Funktion bildet zwei unterschiedliche Argumente auf zwei unterschiedliche Funktionswerte ab. Die Injektivität ist notwendig, weil sie garantiert, dass ein chiffrierter Text – also ein Kryptotext – beim Dechiffrieren eindeutig wieder auf den ursprünglichen Klartext abgebildet wird.

Kryptosysteme bestehen aus einer Vielfalt von Geheimschriften. Diese Vielfalt wird dadurch erzeugt, dass bei jeder Chiffrierung ein zusätzliches Argument eingeführt wird, das wir Schlüssel nennen. Der Schlüssel ist ein Geheimnis zwischen Sender und Empfänger. Er wird sowohl zum Chiffrieren als auch zum Dechiffrieren gebraucht, deshalb sprechen wir von Verschlüsselung und Entschlüsselung. Beispiele für Kryptosysteme aus der Antike sind CAESAR und SKYTALE.

Hinweis für die Lehrperson Das Ziel dieser Lektion ist es nicht nur, einen Einblick in die Geschichte der Kryptologie zu geben und ein paar Geheimschriften und einfache Kryptosysteme zu vermitteln. Diese Lektion hat ihren Schwerpunkt in der Bildung von mehreren grundlegenden Begriffen der Kryptologie. Es soll darauf geachtet werden, dass diese Begriffe richtig verstanden werden und dass die Schülerinnen und Schüler sie richtig verwenden. Auch das Verständnis der Konzepte der Injektivität und der Umkehrfunktionen aus der Mathematik soll gesichert werden und ihre Rolle in der Kryptologie verdeutlicht werden.

Kontrollfragen

1. Wie sind die Schriften entstanden? Welche unterschiedlichen Schriftarten kennen wir?

2. Welche Bedeutung können die Zeichen eines Alphabets haben?
3. Was ist ein Alphabet aus mathematischer Sicht?
4. Was sind Texte aus mathematischer Sicht?
5. Was ist eine Funktion? Wie sieht man an der Mengendarstellung von Funktionen oder im Funktionsgraph, dass eine Funktion injektiv ist?
6. Was ist eine Geheimschrift? Wie kann eine Geheimschrift eindeutig und vollständig beschrieben werden?
7. Welche Geheimschriften kennst du?
8. Wie unterscheidet sich ein Kryptosystem von einer Geheimschrift?
9. Was ist der wesentliche Unterschied zwischen CAESAR und SKYTALE?
10. Wieso sollte eine Chiffrierung injektiv sein? Wie nennt man eine injektive Chiffrierung?

Kontrollaufgaben

1. Wie viele Texte mit folgenden Eigenschaften gibt es?
 - (a) Texte bestehend aus fünf Symbolen aus Lat?
 - (b) Texte aus Lat mit einer Länge kleiner gleich drei?
 - (c) Texte aus dem Alphabet $\{0, 1\}$ der Länge 10?
 - (d) Texte mit den Symbolen A, B, C, D und E, die mit A beginnen und mit B enden und die Länge 7 haben?
 - (e) Texte aus dem Alphabet $\{X, Y, Z\}$, die drei X, vier Y und zwei Z enthalten.
 - (f) Texte der Länge 3 aus dem Alphabet $\{A, B, C\}$, die mehr A's als die beiden anderen Buchstaben enthalten.
2. Dechiffriere den folgenden Text, der mit POLYBIOS chiffriert worden ist.
2444112511
3. Entschlüsse den folgenden Text mit CAESAR und dem Schlüssel mit Wert 6.
IGKYGXOYZKOTLGIN
4. Welche der folgenden Funktionen sind injektiv? Begründe deine Antworten beispielsweise mit der Darstellung als Funktionsgraph (falls die Funktion injektiv ist) oder finde zwei unterschiedliche Argumente, für die die Funktion den gleichen Funktionswert besitzt.
 - (a) $f(x) = x^3$ für $f: \mathbb{R} \rightarrow \mathbb{R}$
 - (b) $f(x) = x^2 - 4x + 3$ für $f: \mathbb{R} \rightarrow \mathbb{R}$
 - (c) $f(x) = |x|$ für $f: \mathbb{R} \rightarrow \mathbb{R}$
 - (d) $f(x) = \frac{1}{x}$ für $f: \mathbb{R}^+ \rightarrow \mathbb{R}$
 - (e) $f(x) = \log_{10}(x)$ für $f: \mathbb{R}^+ \rightarrow \mathbb{R}$
5. Betrachte die Chiffrierung $\text{Cod}: \{A, B, C\} \rightarrow \{1, 2, 3, 4, 5\}$ mit $\text{Cod}(A) = 1134$, $\text{Cod}(B) = 134$ und $\text{Cod}(C) = 25$. Diese Chiffrierung von Symbolen wird also verwendet, um die Texte aus $\{A, B, C\}$ durch Texte aus $\{1, 2, 3, 4, 5\}$ zu chiffrieren. Ist diese Chiffrierung eine Codierung?

6. Gegeben sind zwei injektive Funktionen $f: A \rightarrow B$ und $g: B \rightarrow D$. Warum ist die Funktion $f(g(x))$ eine injektive Funktion von A nach D ?
7. Nutze die Eigenschaft der Injektivität in der obigen Aufgabe, um die Geheimschrift ROT13 mit der Geheimschrift FREIMAURER zu kombinieren, so dass eine neue Geheimschrift entsteht. Zuerst soll der Klartext mit ROT13 codiert werden, und auf diesen Geheimtext soll dann noch FREIMAURER angewendet werden.
- Gib das Schema der auf diese Weise erhaltenen Geheimschrift an.
 - Chiffriere deinen Namen mit dieser Geheimschrift.
 - Dechiffriere den folgenden Geheimtext:
 $\square \square \square \square \langle \square \square \square \square \rangle$.
 - Chiffriere den in Kontrollaufgabe 7(c) erhaltenen Klartext mit ROT13. Vergleiche den erhaltenen Geheimtext mit dem Geheimtext aus Kontrollaufgabe 7(c). Was fällt dir auf? Wie kannst du dir das erklären?
8. Betrachte das folgende Kryptosystem mit den Schlüsseln (i, j) , wobei $i \in \{0, 1, \dots, 25\}$ und $j \in \{1, 2, \dots, 25\}$. In einem ersten Schritt wird der Klartext mit CAESAR und dem Schlüssel i verschlüsselt. Im zweiten Schritt wird der auf diese Weise erhaltene Text mit SKYTALE und dem Schlüssel j verschlüsselt.
- Wie viele Schlüssel hat dieses Kryptosystem?
 - Beschreibe die Vorgehensweise bei der Entschlüsselung.
 - Verschlüssele den folgenden Text mit dem Schlüssel $(3, 4)$:
 UEBUNGMACHTDENMEISTER
 - Entschlüssele das folgende Zitat von Charlie Chaplin mit dem Schlüssel $(5, 8)$. Die Symbole \square stehen für Leerzeichen auf dem Band der Skytale.
 JFFYNAJLNSSQXJS\squareSISFYWJ\squareYJNHJQW\squareFRHMNTY\squareLRMYSWF\square
 - Entschlüssele den folgenden Kryptotext. Du hast schon herausgefunden, dass $i = 8$ ist.
 LMAASLMPCAWKMWZTSKAPQKSIWPXCVPNTN
 UWITMIQMUMVMVJVQAEBPBEMOKBQQIMZMP
 PMVAKETVMLLBSMBWCMQLMVAKBZMCZVKP
- Was ist j ? Wie lautet der Klartext?
9. Diese Aufgabe kann nur mit Programmierkenntnissen gelöst werden. Schreibe ein Programm, das einen Text mit CAESAR und beliebig gewähltem Schlüssel verschlüsseln und entschlüsseln kann.
10. In kryptographischen Anwendungen arbeiten wir oft mit ganzzahligem Teilen. Der Ausdruck

$$x \text{ div } y$$

bezeichnet das ganzzahlige Teilen von x durch y . Den Rest der ganzzahligen Division bezeichnen wir mit dem Ausdruck

$$x \text{ mod } y.$$

Somit ist zum Beispiel

$$72 \text{ div } 7 = 10 \quad \text{und} \quad 72 \text{ mod } 7 = 2.$$

Wir verwenden die mod-Notation zur Beschreibung von Chiffrierungen von einzelnen Symbolen.

- (a) Sei $\mathcal{A} = \{A, B, C, D, E\}$. Die Ordnung von A in \mathcal{A} ist $\text{Ord}(A) = 0$, die Ordnung von B in \mathcal{A} ist $\text{Ord}(B) = 1$ usw.

Wir definieren eine Funktion $f: \mathcal{A} \rightarrow \mathcal{A}$ für jedes $x \in \mathcal{A}$ wie folgt:

$$f(x) = \text{das Symbol aus } \mathcal{A} \text{ mit der Ordnung } (\text{Ord}(x)^2 \bmod 5).$$

Somit ist zum Beispiel $f(D) = E$ weil $\text{Ord}(D) = 3$ und

$$3^2 \bmod 5 = 9 \bmod 5 = 4.$$

Ist f eine Codierung der Buchstaben aus \mathcal{A} ?

- (b) Betrachte das Alphabet $\mathcal{A} = \{A, B, C, D, E, F\}$. Definiert sei für jedes Element $x \in \mathcal{A}$ die Funktion

$$g(x) = \text{das Symbol aus } \mathcal{A} \text{ mit der Ordnung } (\text{Ord}(x)^2 \bmod 6).$$

Ist g eine Codierung von Symbolen aus \mathcal{A} nach \mathcal{A} ?

- 11.** Seien \mathcal{A} und \mathcal{B} zwei Alphabete und sei $\text{Cod}: \mathcal{A} \rightarrow \mathcal{B}^*$ eine Codierung der Symbole aus \mathcal{A} durch Texte aus \mathcal{B}^* . Ein Text α heisst **Präfix** eines Textes β , falls β mit dem Text α anfängt. Der Text KRYPTO ist zum Beispiel ein Präfix vom Text KRYPTOSYSTEM. Eine Codierung Cod heisst **präfixfrei**, wenn es keine Buchstaben X und Y gibt, so dass $\text{Cod}(X)$ ein Präfix von $\text{Cod}(Y)$ ist. Ist diese Eigenschaft der Präfixfreiheit einer Codierung von Buchstaben für uns interessant? Begründe deine Antwort sorgfältig.

Anhang A

Lösungen zu ausgewählten Aufgaben

Aufgabe 1.2 A, B, C, AA, AB, AC, BA, BB, BC, CA, CB, CC, AAA, AAB, AAC, ABA, ABB, ABC, ACA, ACB, ACC, BAA, BAB, BAC, BBA, BBB, BBC, BCA, BCB, BCC, CAA, CAB, CAC, CBA, CBB, CBC, CCA, CCB, CCC

- Aufgabe 1.4**
- a) Es gibt $3^3 = 27$ Texte der Länge drei über dem Alphabet $\{A, B, C\}$, weil an jeder der drei Stellen jedes der drei Symbole vorkommen kann.
- b) Es gibt $4^5 = 1024$ Texte der Länge fünf über dem Alphabet $\{0, 1, 2, 3\}$, weil wir für jede der 5 Positionen des Textes 4 Möglichkeiten haben.
- c) Es gibt $2 + 2^2 + 2^3 = 14$ Texte der Längen 1 bis 3 über dem Alphabet $\{0, 1\}$.
- d) Es gibt 2^n Texte der Länge n über dem Alphabet $\{0, 1\}$.
- e) Es gibt $\frac{8!}{2^4} = 2520$ oder $\binom{8}{2} \cdot \binom{6}{2} \cdot \binom{4}{2} \cdot \binom{2}{2} = 2520$ Texte der Länge 8 über dem Alphabet $\{A, B, C, D\}$ mit der zusätzlichen Bedingung, dass jedes Symbol in jedem Text genau zweimal vorkommt, denn für die zwei Symbole A kann man aus 8 Plätzen 2 auswählen, für das Symbol B bleiben noch 6 Stellen übrig, für C 4 Stellen und das D wird auf die restlichen beiden Stellen verteilt.
- f) Es gibt $\frac{8!}{4!3!} = 280$ oder $\binom{8}{4} \cdot \binom{4}{1} \cdot \binom{3}{3} = 280$ Texte der Länge 8 über dem Alphabet $\{0, 1, 2\}$, so dass die Texte genau vier Nullen und eine Eins enthalten, denn für die vier Nullen muss man 4 Stellen aus 8 auswählen und aus den übrigen 4 Stellen wird eine Stelle für die Eins ausgewählt und die übrigen drei Stellen werden mit je einer Zwei besetzt.
- g) Es gibt $\binom{4}{2} + \binom{4}{3} + \binom{4}{4} = 6 + 4 + 1 = 11$ Texte der Länge 4 über dem Alphabet $\{0, 1\}$, die mindestens so viele Symbole 1 wie 0 enthalten, denn solche Texte haben entweder zwei, drei oder vier Einsen.
- h) Es gibt $\binom{8}{5} \cdot 2^3 + \binom{8}{6} \cdot 2^2 + \binom{8}{7} \cdot 2 + \binom{8}{8} = 577$ Texte der Länge 8 über dem Alphabet $\{0, 1, 2\}$ mit mindestens 5 Nullen, also so dass die Texte mehr Nullen als Symbole 1 und 2 zusammen haben. Sobald die Stellen für die Nullen bestimmt sind, dürfen die restlichen Stellen jeweils beliebig durch eine Eins oder eine Zwei besetzt werden.

Aufgabe 1.5 1211125311543

Aufgabe 1.6 Der Klartext lautet ΚΡΥΠΤΟΣ (Kryptos).

Aufgabe 1.8 Die Funktion $f(x) = x^2$ ist nicht injektiv, weil zum Beispiel für die Argumente -2 und 2 die Funktionswerte identisch sind. Es gilt $f(-2) = 4 = f(2)$.

Aufgabe 1.9 $f^{-1}(y) = \frac{y+8}{6}$

Aufgabe 1.12 Nein, denn $y = 5$ ist zum Beispiel auch eine monoton wachsende Funktion, aber für jedes Argument ist der Funktionswert gleich. Also ist die Funktion nicht injektiv.

Aufgabe 1.13 Seien x und y zwei Argumente aus A mit $x \neq y$. Das heisst, es gilt entweder $x < y$ oder $x > y$. Weil f eine streng monoton wachsende Funktion ist, gilt also im ersten Fall $f(x) < f(y)$ und im zweiten Fall $f(x) > f(y)$. Daraus folgt aber, dass in jedem Fall $f(x) \neq f(y)$ gilt, was uns die Injektivität der Funktion f beweist.

Aufgabe 1.17

$$\mathcal{B}^* = \{1, 2, 3, 4, 5, 11, 12, 13, 14, 15, 21, 22, 23, 24, 25, 31, 32, \\ 33, 34, 35, 41, 42, 43, 44, 45, 51, 52, 53, 54, 55, 111, \\ 112, 113, 114, 115, 121, 122, 123, 124, 125, \dots\}$$

Aufgabe 1.19 Man könnte zum Beispiel vor jene Codewörter, die nur aus einer Ziffer bestehen, eine Null schreiben. Somit haben dann alle Codewörter die Länge 2.

Oder man könnte zu jedem Codewort 9 addieren, damit alle Codewörter die Länge 2 haben. Dann hätten wir

$$f(A) = 10, \quad f(B) = 11, \quad \dots, \quad f(Z) = 35.$$

Aufgabe 1.20 Der Klartext lautet POLYBIOS. Ja, diese Chiffrierung ist eine Codierung.

Aufgabe 1.21 Der Klartext lautet:

ZWEID INGES INDUN ENDLI CHDAS UNIVE RSUMU NDDIE MENSCH
HLICH EDUMM HEITA BERBE IMUNI VERSU MBINI CHMIR NICHT
GANZS ICHER

Aufgabe 1.22 Der Klartext lautet KRYPTOLOGIE.

Aufgabe 1.25 Der folgende Klartext stammt aus den Memoiren von *Giacomo Girolamo Casanova*

DIEVERNUNFTISTDESHERZENS GROESSTEFINDIN .

Aufgabe 1.26 Der Schlüssel ist 20 und der Klartext lautet:

SOLANGEDIESONNESCHEINTSINDWIRNICHTZUSPAET

Aufgabe 1.27 Bei der ROT13-Chiffrierung wird zum Beispiel A auf N und N wieder auf A abgebildet. Die Buchstaben werden also in Buchstabenpaare aufgeteilt und bei der Verschlüsselung wird jeder Buchstabe auf seinen „Partner“ abgebildet. Das heisst, wenn man die Verschlüsselung zweimal hintereinander auf einen Klartext anwendet, bekommt man wieder denselben Klartext.

Aufgabe 1.28 Da wir aus dem ursprünglichen Text alle Leerzeichen entfernt haben, wissen wir, dass die Leerzeichen auf dem Papierstreifen dadurch entstanden sind, dass die letzte Zeile auf der Skytale nicht bis zum Ende mit Buchstaben gefüllt worden ist. Das wiederum heisst, dass diese Leerzeichen alle nebeneinander liegen müssen. Wenn man zu der Anzahl Buchstaben zwischen zwei Leerzeichen noch Eins addiert, dann bekommt man also den Schlüssel.

Aufgabe 1.29 Die Spartaner müssen den Text auf 11 Spalten aufteilen.

Aufgabe 1.30 Der Schlüssel ist 5 und der Klartext lautet

EINKLEINERSCHRITTFUERMICHABEREINGROSSE
RSPRUNGFUERDIEMENSCHHEITNEILARMSTRONG

Da der Kryptotext keinen sinnvollen Text darstellt, ist der Schlüssel weder 1 noch 75 (die Länge des Textes). Es gibt auch keine Leerzeichen zwischen zwei Buchstaben. Das bedeutet, dass alle Zeilen beim Verschlüsseln gefüllt worden sind. Es könnte höchstens sein, dass in der letzten Zeile und Spalte ein Feld leer geblieben ist. Das wäre nämlich ein Leerzeichen ganz am Schluss des Kryptotextes und das sehen wir nicht. Wenn wir zuerst annehmen, dass kein Leerzeichen am Schluss steht, dann haben wir $75 = 3 \cdot 5 \cdot 5$ Buchstaben, die auf ein Rechteck zu verteilen sind. Wir könnten also 3, 5, 15 und 25 als mögliche Schlüssel haben. Falls es am Schluss ein Leerzeichen hätte, dann hätten wir $76 = 2 \cdot 2 \cdot 10$ Zeichen, das heißt, wir müssten zusätzlich noch die Schlüssel 2, 4, 10 und 20 ausprobieren. Also müssten wir schlimmstenfalls insgesamt 7 Schlüssel ausprobieren.

Aufgabe 1.34 Jedes Loch auf der Lochkarte kann entweder offen oder zu sein. Insgesamt haben wir $n \times m$ Felder, also gibt es $2^{m \cdot n}$ Schlüssel.