Mathematik in der Praxis: Kryptologie

von Enrico Thomae

Wie, du studierst Mathe? Was willst du denn damit werden?, wurde ich des Öfteren während meines Studiums gefragt. Im Unterton und Gesichtsausdruck ließen sich weitere Fragen ablesen *Wozu braucht man das denn?* und *Muss man das studieren? Plus, Minus, Mal - das kann doch jedes Kind*. Als ich dann auch die Frage, ob ich vielleicht Lehrer werde wolle verneinte, hatten die meisten nur noch ein beileidiges Lächeln für mich übrig.

Diese Reihe von Artikeln über Mathematik in unserem Alltag soll zeigen, dass Mathematik mehr ist als die Hilfswissenschaft zu der sie von Ingenieuren gerne degradiert wird. Mathematik begegnet uns jeden Tag und überall. Kein Handy würde funktionieren ohne Codierungstheorie, kein Geldautomat ohne Kryptologie, keine Maschine ohne Geometrie, keine Bank ohne Stochastik, kein Satellit ohne Numerik und kein Windrad ohne Analysis.

In den folgenden Artikeln sollen zunächst am Beispiel der Kryptologie einige mathematische Zusammenhänge und deren Anwendung in der Praxis vorgestellt werden.

Einleitung
oder: Von der Steinzeit bis ins Internet

Jeder Mensch hat Geheimnisse. Schon unsere Vorfahren im alten Äqypten 3000 v.Chr. wussten über die Macht von Informationen und versuchten sie vor bestimmten Menschen zu verbergen. Die ersten Versuche reichten von durchsichtiger Tinte, über Geheimsprachen bis hin zu Hieroglyphen, die bis heute Rätsel aufgeben. Schnell musste man sich neue Verfahren einfallen lassen, da die Sicherheit der bekannten Verfahren stark mit deren Geheimhaltung verknüpft war. Sobald man weiß, dass mit Zitronensaft Geschriebenes sichtbar wird, sobald man es über eine Kerze hält, ist es nicht schwer leere Zettel lesbar zu machen. Da die physikalischen Möglichkeiten zum Geheimhalten oder besser gesagt, zum Verstecken von Informationen überschaubar sind, kann man einfach alle durchprobieren.

Kerckhoffs'sches Prinzip:
Die Sicherheit eines Verschlüsselungsfahrens darf nicht auf der Geheimhaltung des Verfahrens beruhen.

Als Caesar vor dem Problem stand, dass seine geheimen Befehle an die weit über Europa verteilte Armee abgefangen wurden und der Feind somit bestens informiert war, benutzte er eine der ersten Verschlüsselungsverfahren, die sogenannte Caesar-Chiffre.

Dabei verschiebt man jeden Buchstaben im Alphabet um eine feste Anzahl k nach rechts, um den Text unlesbar zu gestalten. Aus HALLO wird mit $k = 3$, wie Caesar es wählte, der Geheimtext KDOOR. Mathematisch gesehen können wir diese Chiffre wie folgt beschreiben. Wir ordnen jedem Buchstaben eine Zahl gemäß folgender Tabelle zu.

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

Um einen Buchstaben m zu Verschlüsseln benutzt man die Verschlüsselungsfunktion

$$V(m) = (m+k) \bmod 26,$$

wobei k der geheime Schlüssel ist und $c = V(m)$ der Geheimtext. Zum Entschlüsseln benutzt man die entsprechende Entschlüsselungsfunktion $E(c) = (c-k) \bmod 26$.

Man nennt die Caesar-Chiffre ein symmetrisches Verschlüsselungsverfahren, da beide Schlüssel zum Ver- und Entschlüsseln, also k und $-k$, geheim gehalten werden müssen. Man sieht außerdem, dass sich beide leicht auseinander herleiten. Dieses Prinzip - auch klassische Kryptographie genannt – prägte bis 1976 alle Verschlüsselungsverfahren. Wie jeder in den unten gestellten Aufgaben überprüfen kann, ist die Caesar-Chiffre nicht schwer zu brechen. Da es nur 26 Möglichkeiten für den geheimen Schlüssel k gibt, kann man einfach alle durchprobieren. Diesen einfachsten aller Angriffe nennt man *Brute Force* (übersetzt: rohe Gewalt). Man musste sich also bald neue Chiffren einfallen lassen, für die die Anzahl der geheimen Schlüssel k so groß ist, dass es nicht mehr möglich ist, einfach alle durchzuprobieren. So ist der Nachfolger der Caesar-Chiffre – die Viginere Chiffre – schon wesentlich sicherer. Hier benutzt man mehrere Cäsar-Chiffren parallel, was die Anzahl der möglichen Schlüssel stark erhöht. Doch Mathematiker fanden bessere Angriffe, so kann man zum Beispiel statistisch untersuchen welcher Buchstabe wie oft im Geheimtext vorkommt. Das Ergebnis

vergleicht man mit der statistischen Verteilung der verwendeten Sprache – so tritt das *e* in deutschen Texten am Häufigsten auf – und kann somit auf den geheimen Schlüssel schließen. Kryptographen, die neue Chiffren entwarfen und Kryptanalytiker, die Angriffe dagegen suchen, leisteten sich einen ständigen Wettlauf.

Kryptologie = Kryptographie + Kryptanalyse

Ein voläufiger Höhepunkt dieser Entwicklung war die im Zweiten Weltkrieg von den Deutschen verwendete ENIGMA. Diese Chiffre war so kompliziert, dass sie nur maschinell mit Hilfe erster Computer gebrochen werden konnte. Ab diesem Zeitpunkt war die Rechenleistung von Computern wesentliches Sicherheitskriterium. Auch die heute meistbenutzte symmetrische Chiffre AES (Advanced Encryption Standard) muss der steigenden Leistungsfähigkeit von Computern angepasst werden.

Das klingt alles sehr danach, als ob Sicherheit relativ ist und nur von der Geschwindigkeit der Computer abhängt. Gibt es keine perfekte Sicherheit? Das heißt, eine Chiffre die nicht einmal mit Brute Force zu brechen ist, auch wenn man den schnellsten Computer der Welt zur Verfügung hat? Doch, die gibt es! Das sogenannte *One Time Pad* ist eine perfekte symmetrische Chiffre.

Eine Chiffre heißt perfekt sicher, wenn der Geheimtext c keinerlei Informationen über den zugehörigen Klartext m verrät. Das bedeutet, dass die Wahrscheinlichkeit m zu raten, unter der Bedingung c zu kennen, genauso groß ist, wie m ohne Kenntnis von c zu raten: $\mathrm{P}(m|c) = \mathrm{P}(m)$.

Möchte man zum Beispiel ein Wort $m = m_1m_2m_3$ der Länge 3, das nur aus Nullen und Einsen besteht $m_i \in \{0,1\}$, mit dem One Time Pad verschlüsseln, so wählt man sich einen zufälligen Schlüssel $k = k_1k_2k_3$ mit $k_i \in \{0,1\}$ und bildet den Geheimtext $c = c_1c_2c_3$ indem man die einzelnen Stellen einfach aufaddiert $c_i = m_i + k_i \mod 2$. Brute Force bringt uns hier nicht weiter, da die Anzahl der möglichen Schlüssel genauso groß ist wie die Anzahl der möglichen Klartexte. Damit kann man den Geheimtext c durch unterschiedliche Wahl des Schlüssels k auf jeden möglichen Klartext zurückführen. Man ist hinterher genauso schlau wie vorher. Eigentlich könnten wir an diesem Punkt aufhören uns über Kryptologie Gedanken zu machen. Denn was will man mehr als ein perfektes Verschlüsselungsverfahren, dass man beweisbar nicht brechen kann?

Zwei Dinge stören uns in der Praxis. Zum einen muss die Schlüssellänge genauso groß sein wie die Nachrichtenlänge, falls man perfekte Sicherheit will. Eine E-Mail

zu verschlüsseln bedarf also eines Schlüssels, der genauso lang ist wie die E-Mail. OK, das mag noch machbar sein. Aber nun kommt ein zweites Problem hinzu, dass die gesamte symmetrische Kryptographie betrifft: das Schlüsselaustauschproblem.

Da bei symmetrischen Verfahren sowohl der Schlüssel k_V zum Verschlüsseln, als auch der Schlüssel k_E zum Entschlüsseln geheim sind, müssen Alice und Bob[2] die geheimen Schlüssel auf einem geheimen sicheren Kanal austauschen, bevor sie sich damit Nachrichten schicken können. Die beiden könnten sich zum Beispiel an einem geheimen Ort treffen. Doch wenn der Schlüssel genauso lang ist wie die Nachricht, dann können sich die Beiden auch gleich am geheimen Ort treffen um ihre Nachricht auszutauschen.

Das Problem wird noch deutlicher, wenn wir uns heutige Anwendungsgebiete der Kryptologie betrachten. Die PIN auf der Geldkarte ist zum Beispiel verschlüsselt gespeichert, da sonst jeder Kartendieb sofort auch im Besitz des PINs wäre. Online Banking muss verschlüsselt erfolgen, da sonst jeder unsere Daten abfangen könnte. Wir schreiben verschlüsselte E-Mails. Wir melden uns in sozialen Netzwerken mit unserem Passwort an. Die Übertragung sowie die Speicherung des Passworts sollte verschlüsselt sein, da sonst der Netzwerkbetreiber unser Passwort kennt. Da viele von uns immer wieder ähnliche Passwörter benutzen, könnte er damit mehr erfahren, als uns lieb ist. Nun ist es aber unmöglich, sich mit all diesen Personen zu treffen und geheime Schlüssel auszutauschen. Wollte man, dass jeder in Deutschland mit jedem einen geheimen Schlüssel austauscht, so wären das ungefähr $3 \cdot 10^{15}$ – in Worten 3 Billiarden – Schlüsselpaare. Jeder von uns müsste 81 Millionen verschiedener Schlüssel speichern und sobald ein neuer Bürger geboren wird, müssten man sich mit diesem treffen, um einen geheimen Schlüssel auszutauschen. Was für ein Stress! Dass wir dennoch mit allen verschlüsselt kommunizieren können, haben wir einer Entdeckung von 1976 zu verdanken – der asymmetrischen Kryptographie.

Im Unterschied zur symmetrischen Kryptographie muss der Schlüssel k_V zum Verschlüsseln nicht mehr geheim gehalten werden. Bob kann sich ein Schlüsselpaar (k_V, k_E) erzeugen und k_V öffentlich bekannt geben. Das heißt, jeder kann Bob verschlüsselte Nachrichten schicken, ohne vorher einen Schlüssel geheim mit ihm auszutauschen. Aber nur Bob, der im Besitz des geheimen Schlüssels k_E ist, kann diese Nachrichten entschlüsseln. Das Schlüsselaustauschproblem ist damit gelöst. Das Herzstück asymmetrischer Chiffren sind sogenannte Einwegfunktionen. Wie genau diese funktionieren soll Gegenstand in der nächsten Ausgabe sein.

[2]Um der Mathematik etwas Leben einzuhauchen sagt man nicht *A* schickt eine Nachricht an *B* sondern man benutzt Alice und Bob.

Aufgaben

Caesar Chiffre 1

Ein befreundeter Kryptologe verwendet die Caesar-Chiffre und lässt Ihnen die Nachricht

U O S X O Q O R O S W X S C C O W O R B

zukommen. Da Du als gewiefter Codebrecher bekannt bist, benötigst Du zum Knacken der Nachricht sicherlich nicht lange, oder?

Caesar Chiffre 2

Ein ziemlich verbeulter römischer Soldat trifft von weit her mit folgender Nachricht im römischen Senat ein.

M E F Q D U J W A Y Y F Z M O T D A Y

Den Schlüssel hat er auf seiner Reise leider vergessen. Kannst Du den Senatoren helfen, die Nachricht zu entschlüsseln?

Schlüsselpaare

Angenommen es leben 81 757 600 Menschen in Deutschland. Jeder möchte mit Jedem ein Paar geheimer Schlüssel $(k_V; k_E)$ austauschen. Wieviele Schlüsselpaare müsste man insgesamt austauschen?

Literatur:

Wer sich für die Geschichte der Kryptologie interessiert, dem sei eines der populärwissenschaftlichen Bücher „*Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet*“ von Simon Singh und Klaus Fritz (Deutscher Taschenbuch Verlag) oder „*Verschlüsselte Botschaften: Geheimschrift, Enigma und Chipkarte*“ von Rudolf Kippenhahn empfohlen. Beide widmen sich ausführlicher den älteren Methoden der Kryptologie, gehen aber auch auf modernere Verfahren ein.

Für einen besseren Überblick über die Ideen der moderneren Verfahren eignet sich besonders das Buch „*Moderne Verfahren der Kryptographie: Von RSA zu Zero-Knowledge*“ von Albrecht Beutelspacher, Jörg Schwenk und Klaus-Dieter Wolfenstetter (Vieweg-Verlag). Wie man beim Namen von Albrecht Beutelspacher schon vermuten kann, ist dieses Buch anschaulich und unterhaltsam zugleich, ohne dabei die notwendige Gründlichkeit zu verletzen.