THEMENSPEZIAL: KRYPTOLOGIE

Ob Kriegslist oder Liebesbrief – geheime Botschaften wecken Neugier. Wenn ein Absender sicherstellen möchte, dass nur der rechtmäßige Empfänger seine Nachricht versteht, so kann er diese verschlüsseln. Seit der Antike hat es unzählige Versuche gegeben, dafür sichere Methoden zu entwickeln, doch fast alle wurden irgendwann aufgedeckt. Im Wettlauf zwischen den Entwicklern neuer Verfahren und jenen, die sie entschlüsseln, sind die Erstgenannten oft nur eine Nasenlänge voraus.

Verschlüsselungsverfahren nutzen Methoden der Mathematik und der Informatik. Längst ist daraus eine eigene Wissenschaft entstanden, die Kryptologie, nach dem griechischen Wort „kryptos" für geheim. Es verwundert kaum, dass diese „Wissenschaft des Geheimen" auch Laien fasziniert. Dafür spricht eine Vielzahl an populären Filmen wie etwa Dan Browns Bestseller „The Da Vinci Code – Sakrileg". Historisch korrekt erzählt „Enigma – das Geheimnis" die Geschichte der Entschlüsselung der Wehrmachts-Chiffriermaschine. Der mit vier Oscars ausgezeichnete Film „A Beautiful Mind – Genie und Wahnsinn" zeichnet die Lebensgeschichte des Mathematik-Nobelpreisträgers John Nash nach.

Diese Popularisierung der Kryptologie geht Hand in Hand mit ihrer zunehmenden Verbreitung im Alltag. Während das Thema früher vor allem für das Militär eine Rolle spielte, steigt der Bedarf in der Informationsgesellschaft: Information ist zur Handelsware geworden, und die Kryptologie bietet ihr Geleitschutz. Das gilt nicht nur für den besonders sensiblen Finanzbereich, sondern für jede digitale Kommunikation, vom einfachen Handy-Telefonat bis zum Einkauf im Internet. Die dabei eingesetzten Verschlüsselungsverfahren sind komplex und nur IT-gestützt zu bewältigen. Die grundlegenden Verschlüsselungsprinzipien selbst sind jedoch häufig verblüffend einfach und haben sich im Laufe der Geschichte nur wenig verändert.

Einige kryptologische Methoden können deshalb im Unterricht schon ab der Sekundarstufe 1 demonstriert werden:

Historische Geheimbotschaften

Skytale

Bereits vor über 2.500 Jahren verwendeten die Spartaner ein militärisches Verschlüsselungsverfahren, das heute unter dem Namen Skytale bekannt ist. Hierfür wurde ein Pergamentstreifen um einen Stab gewickelt. Nachdem die Botschaft auf das Band geschrieben wurde, wickelte man es wieder ab und überbrachte es dem Empfänger. Der Stab verblieb beim Absender. Die Botschaft konnte nur von einer Person gelesen werden, die einen

Stab mit gleichem Umfang besaß. Gelangte die Botschaft in die Hände einer anderen Person, konnte sie die Nachricht nicht lesen, da die Buchstaben scheinbar willkürlich auf dem Pergamentstreifen angeordnet waren.

Caesarchiffre

Der 100 v. Chr. geborene römische Feldherr Gaius Julius Caesar ist Namensgeber einer einfachen Verschlüsselungsmethode, die sich Caesarchiffre nennt. Caesar benutzte für seine militärische Korrespondenz eine Verschiebung des Alphabets um drei Buchstaben, so dass die einzelnen Vokale und Konsonanten einer Botschaft durch die Buchstaben ersetzt wurden, die im Alphabet drei Stellen später folgten. Bei dieser Methode wird beispielsweise aus dem A ein D und aus dem B ein E. Mit Caesarchiffre verschlüsselt, liest sich das Wort „Mathematikunterricht" so: „Pdwkhpdwlnxqwhuulfkw".

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**
Geheimtext: **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**

Ein einfacher Caesar-Schlüssel lässt sich mit zwei verschieden großen, runden Scheiben bauen, auf deren Rändern das Alphabet aufgetragen wird. Zunächst legt man sie so übereinander, dass sich gleiche Buchstaben gegenüberstehen. Dreht man die Scheiben gegeneinander, so steht beispielsweise das „A" einer Scheibe über dem „D" der anderen. So lassen sich die Buchstaben der verschlüsselten Nachricht leicht ablesen.

Weil die Caesarchiffre auf der Verschiebung eines einzigen Alphabets beruht, zählt man sie zu den so genannten monoalphabetischen Verschlüsselungsmethoden. Diese lassen sich relativ leicht dechiffrieren, indem man sich nach der Häufigkeit von Vokalen oder Konsonanten richtet. Immer wieder vorkommende Zeichen stehen wahrscheinlich für häufige Vokale wie e oder a.

Enigma

Die Enigma (griechisch „Rätsel") ist eine der bekanntesten Chiffriermaschinen der Geschichte. Sie wurde von der deutschen Wehrmacht im Zweiten Weltkrieg eingesetzt und beruht auf dem Prinzip der polyalphabetischen Verschlüsselung. Äußerlich ähnelt die Enigma einer Schreibmaschine. Sie besteht aus einer Tastatur, einem Satz von drei austauschbaren Walzen und einem Lampenfeld zur Anzeige. Durch die Walzen werden je nach ihrer Position elektrische Kontakte hergestellt, die im Anzeigenfeld einen bestimmten Buchstaben aufleuchten lassen. Die Walzen drehen sich nach jedem Tastendruck. Jeder Buchstabe wird also anders verschlüsselt („polyalphabetisch").

Wie komplex die vielfache Verschlüsselung ist, zeigt die Geschichte der Enigma: Obwohl das erste Modell bereits im Jahr 1918 gebaut wurde, konnte die Methode erst 1943 vollständig aufgedeckt werden. Wissenschaftler aus Großbritannien, Polen, Frankreich und den USA arbeiteten dafür unter dem Decknamen „Ultra" zusammen. Sie benötigten Rechenmaschinen, die bis zu zwei Meter hoch und fünf Meter breit waren. Die Entschlüsselung der Botschaften trug wesentlich zum Sieg der Alliierten über das Deutsche Reich bei. Die Enigma kann heute noch im Deutschen Museum in München oder im Museum für Kommunikation in Berlin besichtigt werden.

Kryptologie und moderne Technologie

Eine Botschaft der Enigma wäre für heutige Rechner eine Kleinigkeit. In wenigen Sekunden hätten sie die Nachricht entschlüsselt. Computer werden immer schneller und leistungsfähiger, und auch die Chiffriermethoden nehmen an Komplexität stetig zu. Kryptologen sorgen heute dafür, dass Sicherheitsstandards ständig an die neuesten technischen Entwicklungen angepasst werden. Die meisten modernen Verfahren, etwa die DES-Methode („Data Encryption Standard"), zerlegen Texte vor der Verschlüsselung in einzelne Blöcke. Anschließend werden diese mit Schlüsseln von beträchtlicher Bit-Länge in mehreren Schleifen kodiert. Dauerhaft sind auch diese Verfahren nicht unangreifbar. Das belegen immer wieder Nachrichten über Hacker wie Anonymous oder LulzSec, die für sicher gehaltene Barrieren scheinbar mühelos überwinden. Der Kampf um Datensicherheit ähnelt einem fortwährenden Tauziehen, bei dem beide Teams ihre Kräfte regelmäßig erweitern. Mal ist eine Seite im Vorteil, mal die andere.

Zwei grundlegende Prinzipien

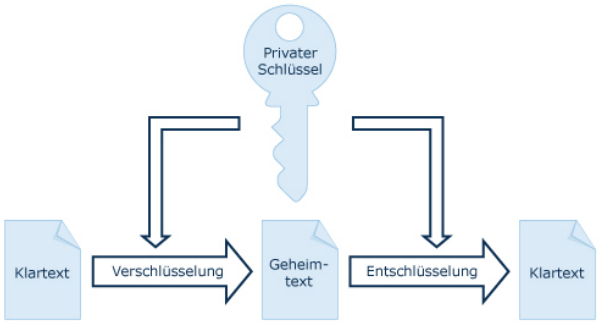
Das **Kerckhoff'sche Prinzip** (1883) besagt, dass eine Verschlüsselungsmethode durchaus bekannt sein darf. Ein Außenstehender weiß demnach, dass beispielsweise die Caesarchiffre genutzt wurde. Unbekannt ist nur der Schlüssel selbst, in diesem Fall die Anzahl der Stellen, um welche die Konsonanten und Vokale im Alphabet verschoben wurden.

Beim **Security by Obscurity-Prinzip** dagegen bleibt die Verschlüsselungsmethode unbekannt. Wie ein Haustürschlüssel unter dem Blumentopf: Jeder könnte ihn benutzen, wenn er wüsste, wo er sich befindet. In der Praxis werden häufig beide Prinzipien miteinander verbunden. Sowohl der Schlüssel als auch die Verschlüsselungsmethode bleiben unbekannt.

Symmetrische und asymmetrische Verschlüsselung

Symmetrische Verschlüsselung

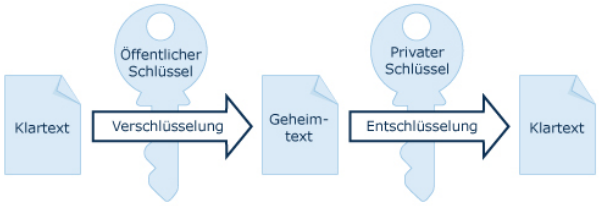
Symmetrische Verschlüsselungsverfahren wie die Caesarchiffre und die Enigma, aber auch moderne Blockchiffren wie DES setzen voraus, dass Absender und Empfänger den gleichen Schlüssel verwenden. Wird dieser Schlüssel bekannt, ist keine Datensicherheit mehr gegeben. Deshalb können sich Sender und Empfänger nicht öffentlich über den Schlüssel verständigen.



Symmetrische Verschlüsselung: Sender und Empfänger verwenden den gleichen Schlüssel, der geheim bleiben muss.

Asymmetrische Verschlüsselung: Die RSA-Methode

In den 1970er Jahren entwickelten Ronald L. Rivest, Adi Shamir und Leonard Adleman am amerikanischen MIT die nach ihren Initialen benannte RSA-Methode. Sie wird auch Public-Key-Verschlüsselung genannt, weil sie mit einem öffentlich einsehbaren Schlüssel arbeitet. Sie zählt zu den asymmetrischen Verfahren, weil Sender und Empfänger zwei unterschiedliche Schlüssel verwenden. Der Schlüssel, der zum Kodieren verwendet wird, ist nicht dazu geeignet, die Botschaft zu dechiffrieren – ähnlich einem Schlüssel, mit dem man eine Tür zwar verschließen, aber nicht öffnen kann. Der Kodierschlüssel heißt auch „Public Key". Nur mit dem zweiten Schlüssel, dem „Private Key", den allein der Empfänger kennt, kann die Nachricht wieder in Klartext umgewandelt werden. Die RSA-Methode widerlegte die bis dato unter Mathematikern weit verbreitete Ansicht, dass ein Public-Key-Verfahren prinzipiell unmöglich sei.



Asymmetrische Verschlüsselung: Zwei unterschiedliche Schlüssel werden genutzt. Der „Public Key" wird zum Verschlüsseln und der „Private Key" zur Entschlüsselung der Nachricht verwendet.

Ablauf einer Public-Key-Verschlüsselung (s. Schaubild):

1. Der Empfänger (A) möchte vom Absender (B) eine kodierte Botschaft erhalten.
2. A entwickelt anhand eines Rechenverfahrens zwei Schlüssel: einen „öffentlichen" und einen „geheimen".
3. A übermittelt B den öffentlichen Schlüssel.
4. B chiffriert seine Botschaft mit dem öffentlichen Schlüssel und übermittelt sie an A. Andere Personen kennen möglicherweise den öffentlichen Schlüssel, können die Botschaft aber trotzdem nicht entschlüsseln.
5. A dechiffriert die Nachricht mit dem privaten Schlüssel.

Bei der asymmetrischen Verschlüsselung können sich Sender und Empfänger öffentlich über den Schlüssel austauschen. Nach diesem Prinzip funktioniert zum Beispiel das im Internet verbreitete https-Protokoll: Obwohl jede Internetverbindung von Dritten belauscht werden kann, bleibt die Verschlüsselung sicher, solange der Private Key nicht übermittelt wird. Die RSA-Methode hat jedoch einen Nachteil: Computer benötigen deutlich mehr Rechenzeit, um sie anzuwenden. In modernen Computersystemen wird daher meist eine Mischung aus symmetrischen und asymmetrischen Verfahren angewendet. Mit der RSA-Methode wird der Schlüssel auf sichere Weise ausgetauscht. Anschließend kommt er in einem symmetrischen Verfahren zur Anwendung.

Der Rechenweg der RSA-Verschlüsselung ist relativ einfach. Mit kleineren Zahlen können bereits Schüler der Sekundarstufe 1 eigene Schlüssel generieren und einander verschlüsselte Botschaften schicken.

THEMENSPEZIAL: VORSCHLAG ZUR UNTERRICHTSGESTALTUNG

Rechenweg zur Entwicklung eines RSA-Schlüssels in der Sekundarstufe 1:

Es werden zwei verschiedene Primzahlen p und q zufällig gewählt und das Produkt der beiden berechnet: n = p * q, also zum Beispiel p = 5, q = 11 und entsprechend n = 5 * 11 = 55. Dies ist die Größe des Zahlenrings, mit dem die verschlüsselte Botschaft in Zahlen umgewandelt wird. Um alle Zahlen und Buchstaben einer chiffrierten Nachricht verschlüsseln zu können, sollte n größer als 36 sein, um mindestens 26 Buchstaben und 10 Ziffern abzubilden. In der Realität sind die Primzahlen größer, um die Sicherheit der Methode zu gewährleisten.

Dann wird ein zufälliger Wert e gewählt, der kleiner n und teilerfremd zu (p-1)*(q-1) = (5-1)*(11-1) = 4*10 = 40 ist, zum Beispiel e = 3.

Die beiden öffentlichen Schlüssel stehen fest: n = 55 und e = 3.

Berechnung des privaten Schlüssels:

Zu e wird das modular Inverse d gesucht. Es soll gelten:

(e*d) mod ((p-1)*(q-1)) = 1. Mit anderen Worten: Das Ergebnis aus (e*d)-1 soll ein Vielfaches von (p-1)*(q-1), demnach von 40, sein. In diesem Fall ist die kleinste Zahl, auf die dies zutrifft, d = 27, denn (3*27)-1 = 80.

d = 27 ist der private Schlüssel.

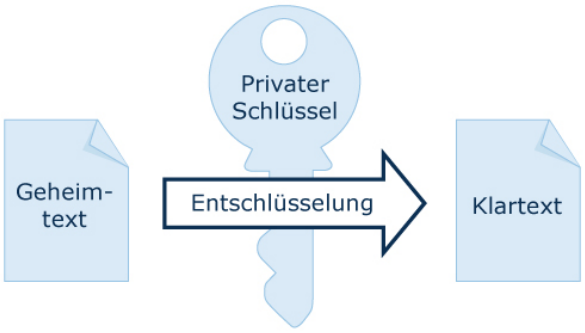
Die Primzahlen p und q werden nicht mehr benötigt. Um den Schlüssel geheim zu halten, sollten sie nicht weitergegeben werden.

Zusammenfassung:

Öffentlicher Schlüssel: n = 55 und e = 3
Privater Schlüssel: d = 27 (und ebenfalls n = 55)

Verschlüsselung:

Die Botschaft wird in Zahlen umgewandelt, also A=1, B=2, …Z=26, dann folgen die Ziffern 0=27, 1=28 bis 9=36. Das Wort „Geheimbotschaft" lautet diesem Prinzip zufolge „07 05 08 05 09 13 02 15 20 19 03 08 01 06 20". In der Realität ist die Verschlüsselung weitaus komplexer.



Um ein Klartext-Zeichen M zu verschlüsseln, berechnet man $C = M^e \bmod n$. Verschlüsselt heißt das Wort „13 15 17 15 14 52 08 20 25 39 27 17 01 51 25".

Für die Dekodierung spielt e keine Rolle mehr, stattdessen kommt der private Schlüssel d zum Einsatz: $M = C^d \bmod n$.

Internettipps für Schüler und Lehrer:

- Schülerkrypto: Jährlicher Workshop an der Universität Bonn für Schüler der Klassen 10-13 und ihre Lehrer: **http://cosec.bit.uni-bonn.de/students/events/11sky/**
- Mystery Twister C3: Offener Kryptografie-Wettbewerb mit Aufgaben aller Schwierigkeitsniveaus: **http://www.mysterytwisterc3.org/**
- Cryptoportal für Lehrer: Plattform für Lehrer, die sich zum Thema Kryptografie austauschen oder Unterrichtsmaterial hochladen und diskutieren möchten: **http://www.cryptoportal.org/**
- Cryptool: Freie Verschlüsselungssoftware, mit der verschiedene kryptografische Verfahren angewendet werden können: **www.cryptool.de**
- Enigma: Ausführlicher Wikipedia-Artikel zu Geschichte, Bedienung und Entzifferung der berühmten Codiermaschine: **http://de.wikipedia.org/wiki/Enigma_%28Maschine%29**

BERUFSSPEZIAL: KRYPTOLOGEN UND IT-SICHERHEITSFACHLEUTE

Mit Mathematik Daten schützen - Für ausgewiesene Kryptologie-Experten stehen die Chancen auf dem Arbeitsmarkt gut, denn Unternehmen aller Branchen investieren zunehmend in die Sicherheit beziehungsweise Verschlüsselung ihrer Daten und Informationen. Von den Spezialisten werden sehr gute Mathematikkenntnisse und mindestens ein solides Basiswissen in Kryptologie erwartet. Das Berufsspezial zeigt, wie der vielfältige Berufsalltag von Kryptologen aussieht.

Eignungstests für die IT-Branche gibt es unter http://www.ruhr-networker.de/itair_test.0.html.

Ausbildungsberufe - Verschlüsseln mit Haupt- und Realschulabschluss

Wichtige Einsatzfelder für Kryptologie-Experten sind die Bereiche IT-Sicherheit und Datenschutz von Unternehmen sowie die staatlichen und militärischen Informationsdienste, also der Bundesnachrichtendienst (BND), das Bundesamt für Sicherheit in der Informationstechnik (BSI) und das Verteidigungsministerium.

FachinformatikerIn der Fachrichtung Anwendungsentwicklung

Fachinformatiker mit der Fachrichtung Anwendungsentwicklung können als Programmierer entweder in einem Unternehmen eingesetzt werden oder für Hersteller von Datensicherheitssoftware arbeiten. Zu ihren Aufgaben gehört es, die Unternehmenssoftware kontinuierlich auf Sicherheitslücken zu überprüfen und Anwender in Software- und Sicherheitsfragen zu schulen und zu beraten. Deshalb sollten sie neben ihrer IT-Kompetenz auch Interesse an der Kommunikation und Zusammenarbeit mit Menschen mitbringen. Für einen Ausbildungsplatz wird mindestens ein Realschulabschluss mit guten Noten vorausgesetzt

Beamtin/Beamter im mittleren technischen Dienst der Fernmelde- und elektronischen Aufklärung des Bundes

Beamte im mittleren technischen Dienst der Fernmelde- und elektronischen Aufklärung des Bundes suchen bei Bundeswehr oder BND nach sicherheitspolitisch relevanten Informationen aus dem Ausland. Diese werden an die Bundesregierung weitergegeben, die sich anhand dieser Daten ein Bild der internationalen Lage machen kann. In der Abteilung Elektronische Aufklärung untersuchen die Beamten unter anderem Funksignale sowie die Signale von Ortungssystemen und Radarstationen, während es in der Fernmeldeaufklärung um Signale, die Nachrichten beinhalten, geht. Für die Laufbahn im mittleren Dienst wird der Realschul- oder ein Hauptschulabschluss mit abgeschlossener technischer Berufsschulausbildung (z.B. Elektrotechnik) vorausgesetzt.

Akademische Berufe - Kryptologie studieren

Einige Universitäten haben an ihren mathematischen Fakultäten mittlerweile Lehrstühle für Kryptologie oder IT-Sicherheit eingerichtet. Ein Studienschwerpunkt „Kryptologie" ist jedoch keine notwendige Vorraussetzung, um als Kryptologe zu arbeiten. Viele Fachkräfte sind Absolventen eines Mathematik- oder Elektrotechnikstudiengangs.

Schüler, die sich für die vielfältigen Berufsmöglichkeiten von Kryptologen interessieren, können sich unter den Absolventen des Studiengangs „IT-Sicherheit" der Ruhr-Universität Bochum umsehen: **http://www.hgi.rub.de/hgi/alumni/alumnipictures/**.

IT-Sicherheitsberater

IT-Sicherheitsunternehmen beraten Firmen aller Branchen in Bezug auf den Schutz ihrer Daten. Zunächst findet eine Situationsanalyse vor Ort statt, gefolgt von einem Katalog empfohlener Maßnahmen zur Verbesserung der Datensicherheit. Wird eine Sicherheitslücke entdeckt bzw. konnte diese bereits von Hackern ausgenutzt werden, unterstützen die IT-Sicherheitsberater ihre Kunden beim Krisenmanagement. Kryptologie gehört dabei zum theoretischen Hintergrundwissen, der Berater wendet sie jedoch nicht selbst praktisch an. Voraussetzung für den Berufseinstieg ist in der Regel ein technisches oder naturwissenschaftliches Studium. Im Beratungsgespräch müssen die IT-Experten auch auf Menschen zugehen und ihnen zuhören können.

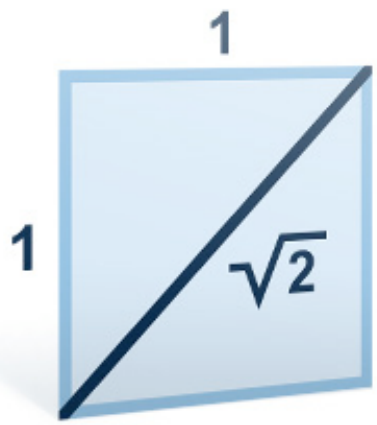
DER NEUE GRAFIKRECHNER FX-CG20 MIT FARBDISPLAY

Der neue Grafikrechner FX-CG20 bereichert den Mathematik-Unterricht, indem er neue Funktionen mit intuitiver Bedienbarkeit verbindet. Der weltweit erste Grafikrechner mit einem hochauflösenden Farb-Display bietet die Möglichkeit, Bilder mathematisch zu analysieren: Indem Schüler auf Fotos oder Video-Ausschnitten Hilfspunkte einzeichnen, können sie auf experimentellem Wege Funktionen finden. Über die Berechnung von Flugkurven oder der Analyse architektonischer Bögen erhalten die Schüler einen Zugang zu realistischen mathematischen Fragestellungen. Im Jahr 2011 gewann der FX-CG20 die Comenius-EduMedia-Medaille für pädagogisch, inhaltlich und gestalterisch herausragende Bildungsmedien.

Für den Lehrer: Unterrichtsgestaltung mit der FX-CG20 Manager-Software

Für einen effektiven Einsatz des Grafikrechners FX-CG20, der Schüler aktiv in den Unterricht einbindet und eine bequeme Unterrichtsvorbereitung erlaubt, sorgt der „FX-CG20 Manager". Die gemeinsam mit

Pädagogen entwickelte Software ermöglicht einen direkten Austausch zwischen Grafikrechner und PC. Mithilfe des Tastendruckprotokolls und der Screenshot-Funktion können Lehrer am Computer Rechenschritte durchgehen, dokumentieren und in ihre Arbeitsmaterialien integrieren. Im Zusammenspiel mit einem Projektor oder über den PC werden sie in die Lage versetzt, Schülern visuelle Hilfestellungen anzubieten und sie zu motivieren, eigene Lösungswege vorzustellen. Aufgaben und Übungsmaterial zum FX-CG20 bietet das didaktische Begleitmaterial.



ZAHL ZUM STAUNEN: WURZEL 2

„Wenn wir im Unterricht über die Wurzel aus 2 sprechen, kann ich meinen Schülern verdeutlichen, dass die Mathematik auch ihre rätselhaften Seiten hat", erklärt Stefan Goltz, Schulkoordinator bei Casio und ehemaliger Mathematiklehrer am Städtischen Gymnasium Bad Segeberg. „Nicht jede Zahl ist endlich, und nicht jede Zahl lässt sich vollständig niederschreiben." Wie π oder die Eulersche Zahl hat Wurzel 2 unendlich viele Nachkommastellen. Sie ist also ebenfalls eine irrationale Zahl, aber im Gegensatz zu ihnen algebraisch.

„Auch die Legende von der Entdeckung der Wurzel aus 2 ist spannend: Die Pythagoreer, eine Gruppe von Wissenschaftlern um Pythagoras, wollten herausfinden, in welchem Verhältnis Zahlen zueinander stehen. Sie gingen davon aus, dass sich jedes in der Natur vorkommende Verhältnis in Form eines Bruchs mit ganzen Zahlen in Zähler und Nenner ausdrücken lässt. Hippasos aus Metapont, ein Schüler von Pythagoras, versuchte, die Länge der Diagonalen eines Quadrats mit den Seitenlängen 1 auszudrücken. Hippasos folgerte, dass die Länge – Wurzel 2 – sich nicht als Bruch darstellen lässt. Diese Erkenntnis kostete ihn möglicherweise das Leben. Denn die Pythagoraeer sollen von der neuen Erkenntnis derart erschüttert gewesen sein, dass sie Hippasos als Ketzer im Meer ertränkten.

2000 v. Chr. kämpften auch die Sumerer mit dem Phänomen Wurzel 2 und schätzten sie auf 1,41. Die Babylonier näherten sich dem heutigen Wert (1,4142135623 …) bis an die fünfte Nachkommastelle an. Tatsächlich hat Wurzel 2 weitere Bezüge zur Realität. So lässt sich mit ihrer Hilfe das Verhältnis der beiden Seitenlängen eines Blattes im DIN-A-Format mit $1:\sqrt{2}$ beschreiben. Halbiert man das Blatt entlang der längeren Seite, entsteht wieder ein Blatt im DIN-A-Format. Auch in der Musik spielt Wurzel 2 eine Rolle: Halbiert man eine Oktave, ergibt sich ein so genannter Tritonus. Die Frequenzen der beiden Töne, die einen Tritonus bilden, zum Beispiel C und Fis, stehen ebenfalls im Verhältnis Wurzel 2 zueinander.