Johannes Buchmann und Nina Bindel

Verschlüsselung und die Grenzen der Geheimhaltung

Verschlüsselung ist eine Technik zur Geheimhaltung von Informationen. Sie wird seit Jahrhunderten genutzt – lange Zeit vor allem vom Militär. Im Zeitalter des Internet ist Verschlüsselung allgegenwärtig. Täglich nutzen wir Methoden zur Geheimhaltung, ohne uns dessen bewusst zu sein: zum Beispiel bei Einkäufen und Banktransaktionen im Internet, beim Bezahlen mit der EC-Karte oder bei der Nutzung von Pay-TV.

Aber wie funktioniert Verschlüsselung? Was sind die Grundlagen der Kryptographie, der Wissenschaft der Verschlüsselung? Unterscheiden sich heute verwendete Methoden von früheren Verfahren? Wie hat sich Verschlüsselung im Lauf der Jahrhunderte weiterentwickelt? Gibt es Grenzen der Geheimhaltung?

1 *Verschlüsselung vor dem Internetzeitalter: Kunst und Wissenschaft*

Vor mehr als 2500 Jahren verschlüsselten die Spartaner mit der Skytale (Abb. 1). Zur Verschlüsselung diente ein Holzstab. Auf den Stab wickelte der Absender ein Pergamentband oder einen Lederstreifen wendelförmig auf. Er schrieb die Botschaft längs des Stabs auf das Band und wickelte es dann wieder ab. Das Band ohne Stab war der verschlüsselte Text. Wenn der Empfänger einen Stab mit demselben Durchmesser wie der Sender hatte, konnte er die Nachricht entschlüsseln, indem er das Band auf diesen Stab wickelte. Wer den Durchmesser nicht kannte, konnte die Nachricht nicht entschlüsseln.

Nach diesem Prinzip funktionieren alle *symmetrischen Verschlüsselungsverfahren*: Sender und Empfänger kennen einen geheimen Schlüssel. Der Sender verschlüsselt einen *Klartext* mit diesem Schlüssel. Dabei entsteht ein *Chiffretext*. Der Sender schickt den Chiffretext an den Empfänger.

Abbildung 1. Skytale von Sparta

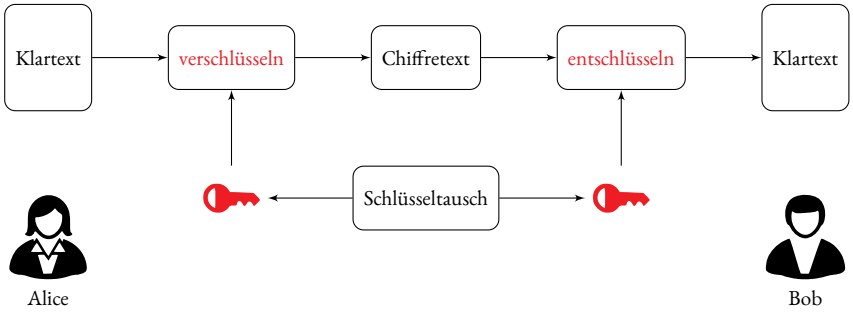

Abbildung 2. Symmetrische Verschlüsselung

Der Empfänger benutzt den geheimen Schlüssel, um den Chiffretext wieder zu entschlüsseln und den Klartext zu bekommen. Bei der Skytale ist der geheime Schlüssel der Durchmesser des Stabs.

Um ein symmetrisches Verschlüsselungsverfahren anwenden zu können, müssen sich Sender und Empfänger vorher auf einen geheimen Schlüssel einigen. Diesen Vorgang nennt man *Schlüsselvereinbarung* oder *Schlüsselaustausch*. Natürlich muss die Schlüsselvereinbarung so geschehen, dass niemand außer dem Sender und dem Empfänger Kenntnis von dem Geheimnis bekommen kann. Zum Beispiel können vertrauenswürdige Kuriere den geheimen Schlüssel überbringen.

Ein anderes bekanntes Beispiel für ein antikes Verschlüsselungsverfahren ist die Caesar-Chiffre. Caesar verschlüsselte Nachrichten, indem er jeden Buchstaben aus dem Klartext durch den Buchstaben ersetzte, der drei Positionen weiter im Alphabet steht. So wird zum Beispiel A durch D ersetzt oder E durch H. Dieses Verschlüsselungsverfahren wurde noch während des amerikanischen Bürgerkrieges (1861–1865) genutzt. Dabei wurde eine Chiffrierscheibe eingesetzt, wie sie in Abb. 3 zu sehen ist. Die Buchstaben im inneren Kreis werden bei der Verschlüsselung jeweils durch die Buchstaben im äußeren Kreis ersetzt. Dabei wird klar, dass Buchstaben am Ende des Alphabets durch Buchstaben am Anfang des Alphabets ersetzt werden, also X durch A, Y durch B und Z durch C. So wird zum Beispiel der Klartext KRANICH zum Chiffretext NUDQLFK. Der geheime Schlüssel ist der Abstand zwischen Klartext- und Chiffretextbuchstaben, in der Originalversion von Caesar also 3.

Wie sicher ist dieses Verschlüsselungsverfahren? Der verschlüsselte Text zeigt keinen unmittelbaren Zusammenhang zum Klartext. Wer das Prinzip der Verschlüsselung nicht kennt, tappt im Dunkeln, was dieser Chiffretext bedeuten soll. Wer aber das Verschlüsselungsprinzip, jeden Buchstaben durch einen anderen zu ersetzen, der eine feste Anzahl von Positionen weiter im Alphabet steht, kennt, der erhält den Klartext durch Ausprobieren aller 26 Möglichkeiten. Voraussetzung dafür, dass ein solches Verschlüsselungsverfahren Schutz bietet, ist also *Security by Obscurity*: nicht nur der Schlüssel, sondern auch das Verschlüsselungverfahren bleibt geheim. Aber selbst das genügt hier nicht. Eine sogenannte Häufigkeitsanalyse erlaubt die Entschlüsselung. Dabei wird die Häufigkeit der Buchstaben im Chiffretext ermittelt. Der häufigste Buchstabe entspricht dem häufigsten Buchstaben in der Ausgangssprache. Im Deutschen ist das E. Der zweithäufigste

Abbildung 3. Beispiel einer Chiffrierscheibe – Reproduktion einer Chiffrierscheibe wie sie im amerikanischen Bürgerkrieg (1861–1865) genutzt wurde. CSA steht für „Confederate States of America", S. S. steht für „Secret Service"

Buchstabe in Verschlüsselungen von deutschen Texten entspricht den zweithäufigsten Buchstaben in deutschen Texten, nämlich N. Der Chiffretext gibt also Informationen über den Klartext preis und kann erfolgreich entschlüsselt werden.

Wie können dann sichere Verschlüsselungsverfahren konstruiert werden? Diese Frage stellte sich auch schon Gottfried Wilhelm Leibniz im 17. Jahrhundert. Er entwickelte das Konzept für eine *Machina Deciphratoria*. Sie wurde zwar nie verwendet, ist aber ein Vorläufer der Verschlüsselungsmaschine *Enigma*, die im 20. Jahrhundert eine wichtige Rolle spielte. Die Enigma wurde von dem deutschen Elektroingenieur Arthur Scherbuis 1918 patentiert und danach vom deutschen Militär verwendet. Diese Maschine, die in Abb. 4 gezeigt ist, sieht aus wie eine Schreibmaschine. Der Klartext wird auf einer Tastatur eingegeben.

In der Enigma befinden sich mindestens drei und in späteren Exemplaren vier drehbar angeordnete Walzen. Sie haben auf beiden Seiten 26 elektrische Kontakte für die 26 Buchstaben des Alphabets. Die Kontakte sind im Inneren der Walze in verschiedenen Varianten verdrahtet,

Abbildung 4. Enigma mit vier Rotoren (Enigma T „Tirpitz")

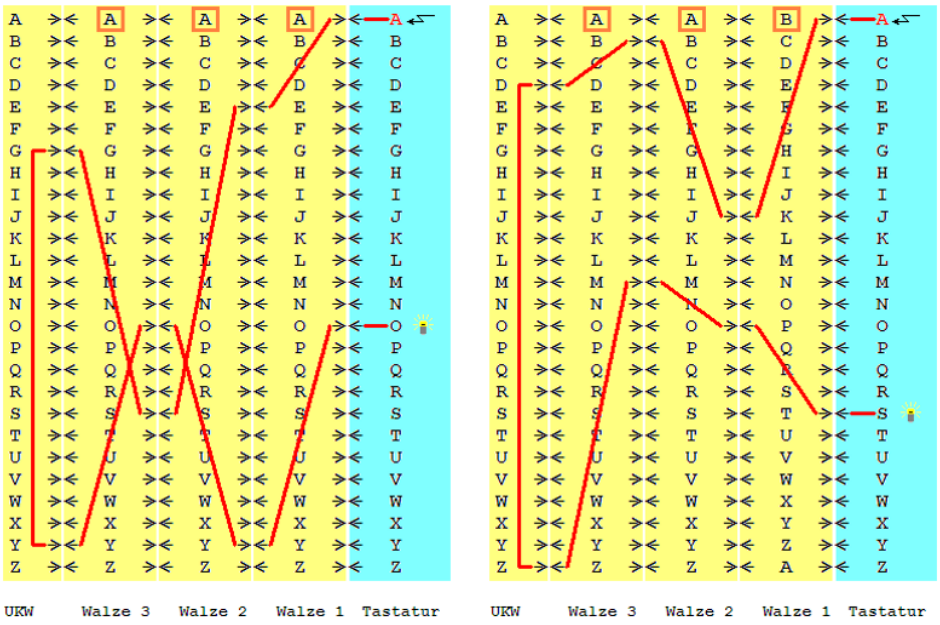

Abbildung 5. Schematische Darstellung zwei aufeinanderfolgender Verschlüsselungen des Buchstabens „A“ mit Hilfe einer Enigma mit drei Walzen. Die Abkürzung UKW steht für Umkehrwalze.

so dass nie ein Kontakt durch sich selbst verschlüsselt wird. Drückt man eine Buchstabentaste, so fließt elektrischer Strom von einer in der Enigma befindlichen 4,5 Volt Batterie über die gedrückte Taste durch den Walzensatz und lässt eine Anzeigelampe aufleuchten. Der aufleuchtende Buchstabe ist die Verschlüsselung des gedrückten Buchstabens. Jetzt wäre immer noch eine Häufigkeitsanalyse möglich, die im Zusammenhang mit der Caesar-Chiffre beschrieben wurde. Das wird aber verhindert. Bei jedem Tastendruck drehen sich nämlich die Walzen ähnlich wie bei einem mechanischen Kilometerzähler weiter. Dadurch werden die Buchstaben jedes Mal anders verschlüsselt (und nicht wie beim Caesar-Chiffre immer auf die gleiche Art). In Abb. 5 wird bei der Grundeinstellung der gewählten Walzen der Buchstabe A zunächst zum Buchstaben O verschlüsselt. Dann dreht sich die erste Walze um eine Position weiter. Jetzt wird A zu S verschlüsselt. Der geheime Schlüssel der Enigma ist die Ausgangsposition der Walzen. Zuerst wurde versucht, auch die Verdrahtungen im Inneren der Walzen geheim zu halten. Sie wurde aber bekannt, weil verschiedene Enigma-Varianten gestohlen wurden.

Im Laufe der Zeit wurde die Enigma noch komplexer. Die Enigma-Walzen konnten aus einem Satz von bis zu fünf Walzen ausgewählt werden, die unterschiedlich verdrahtet waren. Die Anzahl der möglichen Grundeinstellungen und damit die Anzahl der verfügbaren Schlüssel war in der kompliziertesten Enigma etwa 10^{26}. Die alle durchzuprobieren würde auf dem heutzutage schnellsten Superrechner der Welt etwa 10 000 Jahre dauern. Trotzdem wurde eine einfache Version von polnischen Mathematikern entschlüsselt. Für die Entschlüsselung der komplizier-

K	R	A	N	I	C	H
3	13	15	3	21	20	22
N	E	P	Q	D	W	D

Verschlüsselung des Klartextes „KRANICH“

N	E	P	Q	D	W	D
3	13	15	3	21	20	22
K	R	A	N	I	C	H

Entschlüsselung des Chiffretextes „NEPQDWD“

Abbildung 6. Ver- und Entschlüsselung mit Hilfe einer erweiterten Ceasar-Chiffre

teren Varianten enstand im englischen Bletchley Park, dem damaligen britischen Zentrum für Kryptoanalyse, die *Turing-Bombe*. Diese Entschlüsselungsmaschine beruhte auf Ideen der polnischen Kollegen. Sie ist nach dem berühmten englischen Mathematiker Alan Turing (1912–1954) benannt, der an ihrer Entwicklung maßgeblich beteiligt war. Die Turing-Bombe nutzte zum Beispiel Schwächen bei der Verwendung der Enigma aus. So wurden damals alle Funksprüche an deutsche U-Boote verschlüsselt, zum Beispiel auch Wetterberichte. Aber die Wetterberichte waren öffentlich bekannt. So kannten die Alliierten den Klartext, also den Wetterbericht, und den Schlüsseltext, den sie abgehört hatten. Die Kenntnis solcher Kombinationen erleichterte die Entschlüsselung erheblich. Die Möglichkeit, die Chiffretexte der Enigma zu entschlüsseln, trug wesentlich zum Ende des Zweiten Weltkriegs und zur Niederlage der Deutschen bei.

So kompliziert die Enigma auch konstruiert war, so wenig konnte sie Sicherheit garantieren. Die Verschlüsselungsmethode der Enigma war Ingenieurskunst. Es gab aber kein wissenschaftliches Indiz dafür, dass die Enigma tatsächlich sicher war. Und schließlich war sie es ja auch nicht.

Wünschenswert wäre also eine beweisbar sichere Verschlüsselung. Dass diese möglich ist, bewies der amerikanische Mathematiker und Elektrotechniker Claude Shannon (1916–2001) im Jahr 1948. Ein nach Shannon beweisbar sicheres Verschlüsselungsverfahren funktioniert wie folgt: Angenommen das Wort KRANICH soll verschlüsselt werden. Zur Verschlüsselung wird die Caesar-Chiffre verwendet, allerdings wird für jeden Buchstaben ein neuer Schlüssel zufällig gewählt.

In Abb. 6 ist das dargestellt. Für die sieben Buchstaben werden nacheinander die Schlüssel 3, 13, 15, 3, 21, 20, 22 gewählt. Der erste Buchstabe K wird zum Beispiel durch den drei Stellen weiter im Alphabet stehenden Buchstaben N verschlüsselt. Der zweite Buchstabe R wird jedoch durch den 13 Stellen weiter im Alphabet stehenden Buchstaben E ersetzt. So ergibt sich der Schlüsseltext NEPQDWD. Die gewählten Schlüssel erlauben auch die Entschlüsselung. Dann wird aus NEPQDWD wieder KRANICH. Wie können Angreifer ohne Kenntnis der geheimen Schlüssel aus dem Chiffretext NEPQDQD den Klartext ermitteln? Sie wissen, dass die Schlüssel zufällig gewählt wurden. Es bleibt ihnen also nichts anderes übrig, als zu raten. Wenn sie zum Beispiel die Schlüssel 12, 10, 23, 24, 3, 5, 0 raten, so erhalten sie den Klartext BUSSARD. Werden dagegen 24, 0, 4, 8, 19, 22, 16 als Schlüssel geraten, so lautet der entsprechende Klartext PELIKAN.

Auf diese Weise kann sich jeder Vogelname mit sieben Buchstaben ergeben, ja sogar jedes Wort mit sieben Buchstaben. Keiner der möglichen Klartexte ist wahrscheinlicher als ein anderer, weil die Schlüssel zufällig gewählt wurden. Mit anderen Worten: der Chiffretext enthält keinerlei Informationen über den Klartext. Ein solches Verschlüsselungsverfahren nennt man *informationstheoretisch sicher*.

N	E	P	Q	D	W	D
12	10	23	24	3	5	0
B	U	S	S	A	R	D
24	0	4	8	19	22	16
P	E	L	I	K	A	N
3	16	4	8	2	5	21
K	O	L	I	B	R	I

Abbildung 7. Mögliche Klartexte zum Chiffretext „NEPQDWD“

Mathematisch gesprochen: Auf den Klartexten gibt es eine Wahrscheinlichkeitsverteilung Pr, die jedem Klartext P eine Wahrscheinlichkeit $\Pr(P)$ zuordnet. Sie reflektiert den Kommunikationskontext. Wenn zum Beispiel zwei Ornithologen kommunizieren, ist es wahrscheinlicher, dass Namen von Vögeln vorkommen als bei zwei Fußballtrainerinnen. Bei informationstheoretisch sicheren Verschlüsselungsverfahren ändert sich diese Wahrscheinlichkeit nicht, wenn ein Schlüsseltext C bekannt wird. Die bedingte Wahrscheinlichkeit $\Pr(P|C)$ und die unbedingte Wahrscheinlichkeit $\Pr(P)$ sind gleich.

Informationstheoretisch sichere Verschlüsselung klingt vielversprechend. Die entsprechenden Verfahren sind aber nicht besonders praktisch. Die Schlüssel müssen genauso lang sein wie die verschlüsselten Texte. Wenn also ein Text von 2000 Zeichen verschlüsselt werden soll, muss vorher ein Schlüssel ausgetauscht werden, der aus 2000 Zahlen besteht. Außerdem muss bei jeder Verschlüsselung ein neuer Schlüssel gewählt werden. Darum nennt man das beschriebene Verfahren auch *One-Time-Pad*.

Das One-Time-Pad wird verwendet, um sehr sicherheitskritische Kommunikation zu verschlüsseln. Dabei kann heutzutage der *Quantenschlüsselaustausch* zum Einsatz kommen. Dabei sind die beiden Kommunikationspartner mit einem Glasfaserkabel verbunden. Durch das Glasfaserkabel werden polarisierte Photonen geschickt. Richtig implementiert ist dieses Verfahren sicher, solange die Gesetze der Quantenmechanik gelten. Für diejenigen, die daran glauben, dass diese Gesetze ewig gültig sind, bedeutet das: informationstheoretische Sicherheit. Die Entwicklung dieser Technologie steht noch vor etlichen Herausforderungen. Sie wird aber an vielen Orten der Welt erforscht und sogar schon praktisch eingesetzt. Zum Beispiel konnte in Japan eine stabile, mit Quantenschlüsseln gesicherte, Videokonferenz durchgeführt werden. Die Gesprächsteilnehmenden waren immerhin 45 km voneinander entfernt. Die Quanten-Technologie kann also einen wichtigen Beitrag dazu leisten, Kommunikation langfristig vertraulich zu halten.

In der Praxis spielt informationstheoretisch sichere Verschlüsselung eine sehr untergeordnete Rolle. Stattdessen werden heute moderne symmetrische Verschlüsselungsverfahren eingesetzt, an der Spitze der *Advanced Encryption Standard* AES. AES verwendet Schlüssel, die aus 128 bis 256 Bits bestehen. Diese Schlüssel können mehrfach verwendet werden. Einen Sicherheitsbeweis für AES oder ähnliche Verfahren gibt es bis jetzt nicht. Warum gelten diese Verfahren also als sicher? Es gibt mathematische Untersuchungen zur Sicherheit und viele Kryptographen aus der ganzen Welt haben diese Sicherheit untersucht. Gäbe es Schwächen, so wären sie bereits entdeckt und in der globalisierten Welt öffentlich bekannt, weil so viele intelligente Forscher sich damit beschäftigt haben. Aber das ist kein mathematischer Beweis, sondern reine Spekulation.

2 *Verschlüsselung im Internetzeitalter: Die Bedeutung der Zahlentheorie*

Im Internet ist der Schutz der Kommunikation durch Verschlüsselung wichtiger denn je. Wer zum Beispiel im Internet einkauft oder seine Bankgeschäfte über das Internet macht, meldet sich normalerweise mit einem Passwort an. Wer das Passwort kennt, gelangt an viele Informationen. Er erfährt zum Beispiel die Banktransaktionen des Passwortinhabers. Um zu verhindern, dass Passwörter entwendet und unerlaubt genutzt werden können, werden sie verschlüsselt übertragen. Allerdings genügt symmetrische Verschlüsselung für diesen Zweck nicht. Das Problem ist die Schlüsselvereinbarung zwischen Kunden und Anbietern. Banken oder Internethändler müssten bei Verwendung symmetrischer Verschlüsslung mit jedem Kunden einen geheimen Schlüssel austauschen. Das ist bei den Milliarden von Internetnutzern viel zu aufwändig.

Ende der 1970er Jahre hatten Whitfield Diffie (*1944) und Martin Hellman (*1945) eine bahnbrechende Idee: die *asymmetrische Kryptographie*, auch *Public-Key-Kryptographie* genannt. Anstatt denselben Schlüssel für Ver- und Entschlüsselung zu benutzen, verwendet die asymmetrische Kryptographie ein Schlüsselpaar. Es besteht aus einem öffentlichen Schlüssel zum Verschlüsseln und einem geheimen Schlüssel zum Entschlüsseln.

Der entscheidende Punkt: der geheime Schlüssel zum Entschlüsseln lässt sich nicht aus dem öffentlichen Schlüssel zum Verschlüsseln berechnen. Also braucht man den Verschlüsselungsschlüssel nicht mehr geheim zu halten. Er kann veröffentlicht werden. Der Entschlüsselungsschlüssel bleibt dagegen geheim. In Abb. 8 ist Bob der Empfänger geheimer Nachrichten. Er erstellt einen privaten Schlüssel (rot) und einen öffentlichen Schlüssel (grün). Anschließend speichert er den öffentlichen Schlüssel zusammen mit seinem Namen in einer öffentlichen Datenbank. Von dort kann Alice Bobs öffentlichen Schlüssel herunterladen. Vertrauliche Nachrichten an Bob verschlüsselt Alice mit diesem öffentlichen Schlüssel. Bob kann den Chiffretext mit seinem geheimen Schlüssel entschlüsseln.

Ein Onlineshop kann also seinen Verschlüsselungsschlüssel in ein öffentliches Verzeichnis schreiben. Jeder, der sein Passwort an den Onlineshop übermitteln möchte, kann es mit diesem

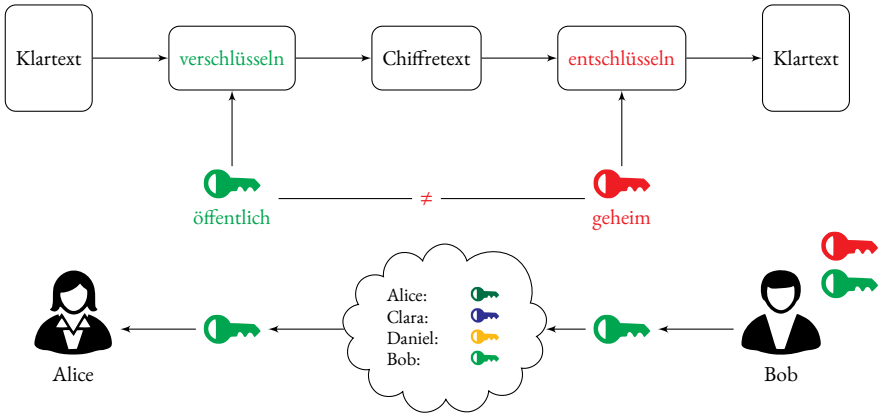

Abbildung 8. Asymmetrische Verschlüsselung

Schlüssel verschlüsseln. Nur der Onlineshop kann die Kundenpasswörter entschlüsseln, weil sonst niemand den Entschlüsselungsschlüssel kennt.

Asymmetrische Kryptographie ist eine tolle Idee. Nur ist sie nicht so leicht zu realisieren. Jedenfalls kann sie nicht mit traditionellen symmetrischen Verschlüsselungsverfahren umgesetzt werden. Im Jahr 1978 hatten Ron Rivest (*1947), Adi Shamir (*1952) und Leonard Adleman (*1945) einen genialen Einfall. Sie erfanden das erste asymmetrische Verschlüsselungsverfahren, das sogenannte *RSA-Verfahren*. Seine Grundlagen stammen aus der Zahlentheorie, einer der ältesten Disziplinen der Mathematik.

Erste Zeugnisse der Zahlentheorie finden sich schon bei den Babyloniern im zweiten Jahrtausend vor Christus. Auch im antiken Griechenland spielte die Zahlentheorie eine wichtige Rolle. Sie beschäftigt sich zum Beispiel mit Primzahlen, also natürlichen Zahlen, die außer 1 und sich selbst keine Teiler haben. Die ersten Primzahlen sind 2, 3, 5, 7, 11, 13, 17. Aber auch

> 10715086071862673209484250490600018105614048117055336074437503883703510511249361224931983788156958581275946729175531468251871452856923140435984577574698574803934567774824230985421074605062371141877954182153046474983581941267398767559165543946077062914571196477686542167660429831652624386837205668069673837205668069673

ist eine Primzahl.

Gibt es noch größere Primzahlen? Tatsächlich konnte schon Euklid im dritten Jahrhundert vor Christus beweisen, dass es beliebig große Primzahlen gibt. Die Idee von Rivest, Shamir und Adleman beruht auf dem Folgenden: Es ist leicht mit modernen Computern zwei große Primzahlen miteinander zu multiplizieren (im RSA-Verfahren werden heute etwa 300-stellige Primzahlen verwendet). Aus dem Produkt die Primfaktoren zu rekonstruieren, würde aber auf den modernsten Supercomputern Millionen von Jahren dauern. Im RSA-Verfahren wird ein solches Produkt, auch *RSA-Modul* genannt, zum Verschlüsseln benutzt. Die beiden Primfaktoren werden zum Entschlüsseln verwendet.

Der öffentliche Schlüssel des Onlinehändlers Amazon.de ist zum Beispiel folgender 617-stelliger RSA-Modul

> 20372136009514320379018203391639318811220566051969104884700049908893930619622221278309073969768558208552984889997026871726462737120720629394310859123838152925734502553161947274592643759076365948511180734778332874951398561113850605129748240218912477156688813560011315780387757288885435519378825822466205560151974479629057988903632127044280549823058512994237496457390308110599384640971401018467769194459832508758293527539611418638863244723545254497981103896230553373471067736553965821835722159375941802751728954636948150972531017422172776434469898141751349619024119145124081095962028011533653005198110084245661835023051.

Er ist das Produkt von zwei über 300-stelligen Primzahlen, die aber nur Amazon kennt. Jeder kann den RSA-Modul von Amazon verwenden, um seine Amazon-Passwörter zu verschlüsseln. Aber nur Amazon kann sie entschlüsseln.

Wie funktioniert das RSA-Verschlüsselungsverfahren nun im Einzelnen? Die Erklärung erfordert ein bisschen Mathematik.

Zuerst muss man verstehen, wie Modulo-Rechnen funktioniert. Wir beginnen mit einem einfachen Beispiel: Wir verwenden die Zahl $n = 391$. Es ist

$$393 \equiv 2 \bmod 391. \tag{13.1}$$

Zahlen dürfen beim Rechnen modulo 391 nämlich durch die Reste bei der Division durch 391 ersetzt werden. Daher ist auch

$$19^3 \equiv 212 \bmod 391. \tag{13.2}$$

Das kann man leicht nachprüfen. Man berechnet $19^3 = 6859$. Anschließend teilt man das Ergebnis 6859 mit Rest durch 391. Es zeigt sich, dass $6859 = 17 \cdot 391 + 212$ ist. Also ist 212 der Rest bei der Division von 6859 durch 391.

Aus dieser Rechnung wird deutlich, dass es nicht schwer ist, dritte Potenzen modulo 391 auszurechnen. Und wie steht es damit, dritte Wurzeln modulo 391 zu ziehen? Also zum Beispiel aus 75? Das ist komplizierter. Was ist zum Beispiel $\sqrt[3]{75}$ modulo 391?

Zuerst stellt man fest, das 391 das Produkt von zwei Primzahlen ist, nämlich $p = 17$ und $q = 23$. Als nächstes berechnet man

$$(p-1)(q-1) = (17-1)(23-1) = 352 \tag{13.3}$$

und findet eine Zahl d mit der Eigenschaft

$$3 \cdot d \equiv 1 \bmod 352. \tag{13.4}$$

Diese Zahl ist

$$d = 235. \tag{13.5}$$

Das lässt sich wieder leicht nachprüfen. Es ist nämlich $3 \cdot 235 = 705$ und $705 \equiv 1 \bmod 352$. Jetzt kann die dritte Wurzel aus 75 modulo 391 berechnet werden, indem man 75^{235}

$$\sqrt[3]{75} \equiv 75^{235} \equiv 31 \bmod 391 \tag{13.6}$$

bestimmt. Wie soll man das nachprüfen? 75^{235} ist eine riesige Zahl. Der Trick ist, dass man schon zwischendurch modulo 391 rechnen darf, also

$$\begin{aligned} 75^{235} &\equiv 75^{234+1} \equiv (75^2)^{117} \cdot 75 \equiv 151^{117} \cdot 75 \\ &\equiv 151^{116+1} \cdot 75 \equiv 151^{116} \cdot 151 \cdot 75 \equiv (151^2)^{58} \cdot 11325 \\ &\equiv 123^{58} \cdot 377 \equiv (123^2)^{29} \cdot 377 \equiv (271^2)^{14} \cdot 116 \\ &\equiv \ldots \equiv 31 \bmod 391. \end{aligned}$$

Tatsächlich ist

$$\begin{aligned} 31^3 &\equiv 961 \cdot 31 \equiv (2 \cdot 391 + 179) \cdot 31 \equiv 179 \cdot 31 \\ &\equiv 5549 \equiv 14 \cdot 391 + 75 \\ &\equiv 75 \bmod 391. \end{aligned}$$

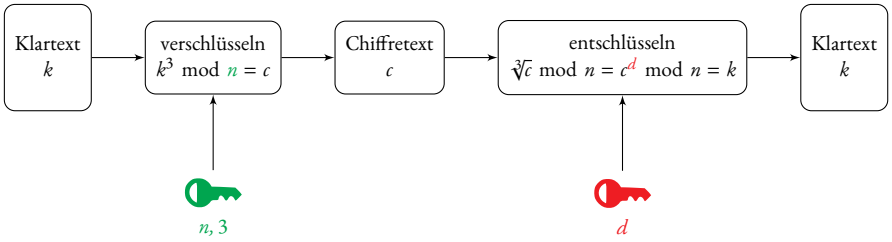

Abbildung 9. Das RSA-Verschlüsselungsverfahren

Dieses Verfahren funktioniert auch für den RSA-Modul von Amazon. Die Primzahlen p und q sind dann die Primfaktoren dieses RSA-Moduls. Oder noch allgemeiner: Es lassen sich auf diese Weise auch andere Wurzeln berechnen. Die Zahl 3 wird dabei durch den entsprechenden Exponenten ersetzt. Das funktioniert, solange der Exponent zu $(p-1)\cdot(q-1)$ teilerfremd ist. Dass das Verfahren stimmt, liegt an einem berühmten Ergebnis des Juristen und Mathematikers Pierre de Fermat (1607–1665). Dies genau darzustellen, ist hier aber leider zu kompliziert.

Entscheidend ist: Potenzieren kann jeder, der den RSA-Modul und den Exponenten kennt. Die entsprechende Wurzel zu berechnen, erfordert aber die Kenntnis der Primfaktoren des RSA-Moduls. Jetzt ist es leicht, das RSA-Verfahren zu beschreiben. Der öffentliche Schlüssel ist der RSA-Modul n und der Exponent e, mit dem potenziert wird, zum Beispiel 3. Verschlüsselt wird durch potenzieren mit e modulo n. Der geheime Schlüssel ist der Exponent d, den man nur mit Hilfe der beiden Primfaktoren p und q des RSA-Moduls berechnen kann. Entschlüsselt wird durch Ziehen der e-ten Wurzel. Dies entspricht dem Potenzieren mit d modulo n.

Ist das RSA-Verfahren praktisch? Jedenfalls nicht, wenn man es naiv anwendet und versucht, damit sehr lange Nachrichten zu verschlüsseln. Dazu ist es zu langsam. In der Praxis kommt eine *Hybrid-Methode* zum Einsatz: Nachrichten werden mit einem symmetrischen Verfahren verschlüsselt. Die Absenderin wählt einen Schlüssel für ein symmetrisches Verschlüsselungsverfahren. Damit verschlüsselt sie ihre Nachricht. Den symmetrischen Schlüssel verschlüsselt sie mit dem öffentlichen RSA-Schlüssel des Empfängers, dem sie beide Chiffretexte schickt. Der Empfänger verwendet seinen geheimen Schlüssel und erhält den symmetrischen Schlüssel. Damit kann er die Nachricht entschlüsseln. Das RSA-Verfahren wird hier also für den Schlüsseltransport benutzt. Die beschriebene Hybrid-Methode ist schematisch in Abb. 10 dargestellt.

Und wie steht es mit der Sicherheit des RSA-Verfahrens? Heute geht man davon aus, dass RSA so lange sicher ist, wie man die RSA-Moduli nicht faktorisieren kann. Bewiesen ist das aber

Tabelle 1. Größe von sicheren RSA-Moduli

Sicher bis zum Jahr	1980	1990	2000	2010	2016	2020	2030	2040	2050
Anzahl Dezimalstellen des RSA-Moduls	105	162	244	335	383	417	511	616	735

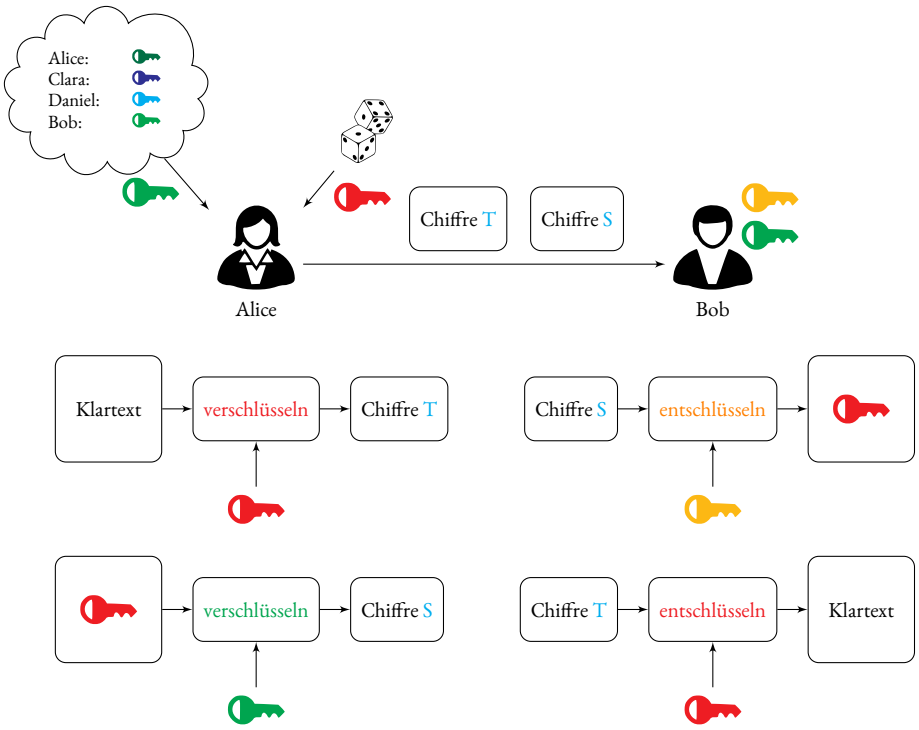

Abbildung 10. Hybrid-Methode aus asymmetrischer und symmetrischer Verschlüsselung

nicht. Aber gehen wir einfach mal davon aus. Dann müssen RSA-Moduli verwendet werden, die groß genug sind.

In ihrer Veröffentlichung des RSA-Verfahrens schrieben die Autoren 1978: "[U]sing 200 digits provides a margin of safety against future developments". Diese Aussage hat sich als viel zu optimistisch erwiesen. Seitdem hat es bei der Lösung von Faktorisierungsproblemen viele Fortschritte gegeben. Nach aktuellem Forschungsstand erfordert bis zum Jahr 2040 sichere RSA-Verschlüsselung über 600-stellige RSA-Moduli. Tabelle 1 gibt eine Übersicht über die erwartete zukünftige Größe von sicheren RSA-Moduli.

Ist das RSA-Verfahren also ein sicheres Verschlüsselungsverfahren?

3 *Quantencomputer und die Folgen*

Anfang der 1980er Jahre schlug der Physiknobelpreisträger Richard Feynman (1918–1988) Quantencomputer für die Simulation quantenphysikalischer Experimente vor. Im Jahr 1994 wurden

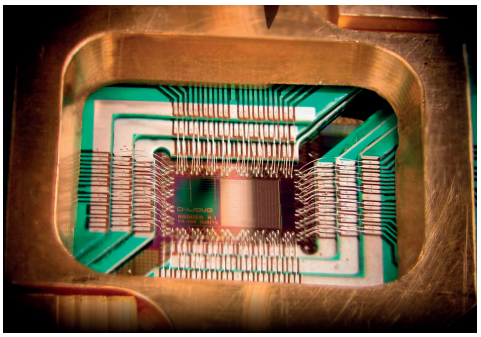

Abbildung 11. Photographie eines Prozessor-Chips produziert von D-Wave Systems, Inc.

Quantencomputer plötzlich bedeutsam für die Kryptographie. Der Mathematiker Peter Wiliston Shor (*1959) stellte nämlich einen Quantencomputer-Algorithmus vor, der sehr effizient Teiler von ganzen Zahlen berechnen kann. Dieser Algorithmus kann auch die geheimen Faktoren von RSA-Moduli finden. Berechnungen eines Quantencomputers nutzen die Prinzipien der Quantenphysik. Informationen werden dabei in quantenphysikalischen Zuständen, sogenannten *Qubits*, gespeichert, verarbeitet und übertragen. Für die Kryptographie bedeutet die Erfindung des Shor-Algorithmus, dass das RSA-Verfahren unsicher ist, sobald genügend große Quantencomputer gebaut werden können.

Es stellt sich also die Frage, ob jemals Quantencomputer konstruiert werden können, die groß genug sind, um komplizierte Berechnungen durchzuführen. Kleine Quantencomputer für sehr spezielle Aufgaben existieren bereits. Die größte Zahl, die mit dem Shor-Algorithmus auf einem Quanten-Computer bis jetzt faktorisiert wurde, ist 21. Das Forschungslabor IBM Research Lab Yorktown Heights im US-Bundesstaat New York hat bereits einen Quantencomputer mit fünf logischen Qubits entwickelt. Um die Rechenleistung heutiger Superrechner zu übertreffen, ist laut IBM ein Quantencomputer mit lediglich 50 logischen Qubits ausreichend. Ein anderes Beispiel ist *D-Wave Two*: eine von der kanadischen Firma D-Wave entwickelte und später von Google und NASA gekaufte Maschine, die für die Lösung mathematischer Optimierungsprobleme konstruiert wurde. Wissenschaftler sehen diese Maschine jedoch noch kritisch.

John Martinis, Forscher an der Universität von Santa Barbara und bei Google, plant, bis 2019 den ersten universellen Quantencomputer zu entwickeln. Manche Wissenschaftler schätzen die Wahrscheinlichkeit, dass das RSA-Verfahren bis zum Jahr 2031 gebrochen wurde, auf 50 %. Experten der Europäischen Union schätzen, dass universale Quantencomputer im Jahr 2035 existieren werden. Genaue Voraussagen kann niemand machen. Aber Forschungsinstitute, Geheimdienste und Unternehmen treiben mit großem Aufwand die Entwicklung von Quantencomputern voran. Die rasante Entwicklung im Bereich der Quantencomputer fördert auch die Forschung an Alternativen zum RSA-Verfahren. Wissenschaftler auf der ganzen Welt forschen im Bereich der sogenannten *Post-Quantum-Kryptographie* an Verfahren, die auch gegen Quantencomputer sicher sind. Eine Umstellung auf Post-Quantum-Verfahren wird heute schon vorbereitet.

4 *Verschlüsselung – Schutz und Risiko*

Früher war Verschlüsselung eine Kunst: Ingenieure erfanden komplizierte Verfahren, die Sicherheit bieten sollten. Mathematische Beweise der Sicherheit gab es noch nicht. Erst in den 1940er Jahren und besonders rasant seit den späten 1970er Jahren entwickelte sich die Kryptographie zu der Wissenschaft, die sie heute ist. Ihr Ideal ist es, die Sicherheit von Verschlüsselung durch mathematische Beweise zu begründen. So ist mathematisch perfekt sichere Verschlüsselung möglich. Sie ist aber sehr aufwändig und zum Beispiel im Internet nicht einsetzbar. Für das Internet geeignet ist die Public-Key-Verschlüsselung. Sie macht einen komplexen Schlüsselaustausch überflüssig und erlaubt die vertrauliche Kommunikation von vielen Millionen Teilnehmern. RSA, das wichtigste Public-Key-Verfahren, bezieht seine Sicherheit aus der praktischen Unmöglichkeit, die Primfaktoren der RSA-Moduli zu berechnen. Allerdings ist heute bekannt, dass große Quantencomputer das RSA-Verfahren brechen werden und solche Computer sind in der Entwicklung. Alternativen zu RSA sind in Vorbereitung.

Bleibt Verschlüsselung also doch ein ewiges Katz-und-Maus-Spiel? Die Erfahrung zeigt: heute verwendete Verschlüsselung wird in 20 Jahren unsicher sein. Ist 20 Jahre Vertraulichkeitsschutz genug? Zum Beispiel bei medizinischen Daten? Angesichts der fortschreitenden Digitalisierung müssen wir Methoden finden, die eine sichere Verschlüsselung langfristig gewährleisten.

Abbildungsnachweise

Tab. 1: keylength.com
Abb. 1: Wikimedia commons/CC BY-SA 3.0
Abb. 3: Crypto Museum (www.cryptomuseum.com)
Abb. 4: Gemeinfrei
Abb. 5: www.lotus7.de/programs/enigma2/enigma.htm
Abb. 11: Wikimedia Commons, D-Wave Systems, Inc./CC BY 3.0