Kryptografie

nach Simon Singhs Buch Geheime Botschaften, 2000, Hanser Verlag
von Dieter Holzhäuser

Schon im Altertum hat man Verfahren angewandt, um Botschaften während der Übermittlung geheim zu halten. So hat auch Cäsar seine Mitteilungen verschlüsselt und darüber in seinem Werk "Der gallische Krieg" berichtet.

Das Geheimhalten von Botschaften durch Verstecken nennt man Steganografie. Zum Beispiel sieht man dem harmlosen Text auf einem Blatt Papier nicht an, dass zwischen den Zeilen die eigentliche Nachricht mit unsichtbarer Tinte geschrieben ist.

Mit dem Begriff "Code" bezeichnet Simon Singh einen Satz oder einen Teil davon, der an Stelle eines Klartextes übermittelt wird. Nur der Empfänger kennt die wirkliche Bedeutung. Zum Beispiel könnte man dem Empfänger mitteilen: "Der Mond ist aufgegangen", wenn gemeint ist: "Die Beleuchtung wurde eingeschaltet".

Die Kryptografie dagegen ersetzt zur Geheimhaltung von Nachrichten die Buchstaben des Klartextes durch andere (Substitution) oder ordnet sie anders an (Transposition) oder beides zusammen.

Die Kryptografen (Verschlüsseler) haben immer schon die Kryptoanalytiker auf den Plan gerufen, deren Bestreben es ist, die Verschlüsselung zu brechen. Obwohl von Codes in der Kryptografie nicht die Rede sein kann, benutzt Singh oft den griffigen Ausdruck "Codebrecher" für Kryptoanalytiker.

1 Handwerkliches

Das allgemeine Verfahren einer Verschlüsselung ist der Verschlüsselungs-Algorithmus. Das genaue Verfahren ergibt sich aber erst durch den Schlüssel, der die Einzelheiten des Vorgangs festlegt. Zum Beispiel könnte der Verschlüsselungs-Algorithmus lauten, dass jeder Buchstabe eines Klartextes durch einen Buchstaben aus einem Geheimalphabet zu ersetzen ist. Und der Schlüssel gibt nun an, welches.

```
                    Klartext:    HALLO
                    Geheimtext:  VHDDT

          Klartextalphabet:  ABCDEFGHIJKLMNOPQRSTUVWXYZ
          Geheimalphabet:    HIFKEBCVGZMDUPTYNLXARJOQWS
```

In der Kryptografie ist jede beliebige Anordnung unserer 26 Buchstaben ein Alphabet. Das Ergebnis der Substitution ist der Geheimtext oder auch Chiffre. Der Empfänger muss den Algorithmus kennen, hier also Substitution, und er muss den Schlüssel, also das Geheimalphabet, kennen, um den Geheimtext zu dechiffrieren.

Die Anzahl der Möglichkeiten, die 26 Buchstaben anzuordnen, ist eine Zahl mit 26 Nullen. Entsprechend viele Geheimalphabete gibt es. Diese gewaltige Zahl von Schlüsseln durchzuprobieren, ist eine unlösbare Aufgabe für die Codebrecher. Aber für Sender und Empfänger einer Nachricht ist es auch nicht einfach, 26 zufällig angeordnete Buchstaben als Schlüssel zu vereinbaren und geheim zu halten. Schlüssel, die man nicht aufschreiben muss, sind da schon besser.

Schlüssel auszuprobieren, ist nur eine Möglichkeit, in den Besitz des Klartextes zu kommen. Es ist ein Leichtes für Codebrecher, eine Botschaft zu entschlüsseln, die nur mit *einem* Geheimalphabet, also monoalphabetisch, verschlüsselt ist. Sie setzen bei den Spuren an, die die Sprache oder die Verschlüsselung selbst im Geheimtext hinterlassen. Zum Beispiel findet sich die Häufigkeit der Buchstaben einer Sprache im Geheimtext wieder. Das heißt, wenn x der häufigste Buchstabe des Geheimtextes ist, wird x dem Buchstaben e des Klartextes entsprechen, sofern es sich um die deutsche Sprache handelt. (Häufigkeitsanalyse). Oder man weiß, dass ein bestimmtes Wort im Klartext vorkommen muss. Auch das ist manchmal schon eine Spur.

Eine wichtige Methode der Kryptografen ist, das Geheimalphabet nach jedem verschlüsselten Buchstaben zu wechseln (polyalphabetische Verschlüsselung). Jetzt müssen Sender und Empfänger nicht nur mehrere Geheimalphabete vereinbaren, sondern auch noch die Art und Weise wie sie zu wechseln sind.

Bei der historischen Vigenère-Verschlüsselung, werden die 25 Geheimalphabete benutzt, die sich durch Verschieben der Buchstaben des Klartextalphabets ergeben. Die Geheimalphabete beginnen also mit B, C, D usw. und man kann sie mit ihrem ersten Buchstaben benennen. In dieser Systematik ist das Klartextalphabet gleichzeitig das Geheimalphabet A.

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ

BCDEFGHIJKLMNOPQRSTUVWXYZA
CDEFGHIJKLMNOPQRSTUVWXYZAB
DEFGHIJKLMNOPQRSTUVWXYZABC
EFGHIJKLMNOPQRSTUVWXYZABCD
FGHIJKLMNOPQRSTUVWXYZABCDE
GHIJKLMNOPQRSTUVWXYZABCDEF
HIJKLMNOPQRSTUVWXYZABCDEFG
IJKLMNOPQRSTUVWXYZABCDEFGH
JKLMNOPQRSTUVWXYZABCDEFGHI
KLMNOPQRSTUVWXYZABCDEFGHIJ
LMNOPQRSTUVWXYZABCDEFGHIJK
MNOPQRSTUVWXYZABCDEFGHIJKL
NOPQRSTUVWXYZABCDEFGHIJKLM
OPQRSTUVWXYZABCDEFGHIJKLMN
PQRSTUVWXYZABCDEFGHIJKLMNO
QRSTUVWXYZABCDEFGHIJKLMNOP
RSTUVWXYZABCDEFGHIJKLMNOPQ
STUVWXYZABCDEFGHIJKLMNOPQR
TUVWXYZABCDEFGHIJKLMNOPQRS
UVWXYZABCDEFGHIJKLMNOPQRST
VWXYZABCDEFGHIJKLMNOPQRSTU
WXYZABCDEFGHIJKLMNOPQRSTUV
XYZABCDEFGHIJKLMNOPQRSTUVW
YZABCDEFGHIJKLMNOPQRSTUVWX
ZABCDEFGHIJKLMNOPQRSTUVWXY
```

Klartextalphabet und 25 Geheimalphabete der Vigenère-Verschlüsselung

Für den ständigen Wechsel wird ein Wort vereinbart, dessen Buchstaben, das jeweils anzuwendende Geheimalphabet bezeichnen, z. B. wird das Wort WETTER mit dem Schlüssel GELB verschlüsselt, indem nacheinander die Geheimalphabete G, E, L ,B, G, E verwendet werden. Der Geheimtext für WETTER ist also: CIEUKV

Aber auch die Vigenère-Verschlüsselung wurde geknackt und zwar von Charles Babbage, vermutlich 1854. Seine Ansatzpunkte waren der Zyklus im Wechsel der Geheimalphabete und die Tatsache, dass *sinnvolle* Schlüsselworte vereinbart wurden. Die Geheimtextalphabete wiederholen sich, z. B. beim Schlüssel GELB, bei jedem 5. Buchstaben des Klartextes.

Es gab und gibt einen unablässigen Kampf zwischen Kryptografen und Kryptoanalytikern. Bisher haben die jeweils Besiegten aber immer wieder aufgeholt und die Oberhand gewonnen.

Gibt es denn überhaupt eine wirklich sichere Verschlüsselung? Ja. Es ist eine starke Erweiterung der Vigenère-Verschlüsselung: Die 25 Geheimalphabete werden beibehalten. Das Schlüsselwort wird so lang gewählt wie der Klartext, besteht aus einer wirklich zufälligen Buchstabenfolge und wird nur einmal verwendet.

Die praktische Umsetzung ist aber so aufwendig, dass diese Verschlüsselung nur für ultrageheime Kommunikation in Frage kommt. Allein schon die Herstellung echter Zufallsreihen ist sehr schwierig. Das wahllose Herumhacken auf einer Tastatur ergibt noch lange keine wirklich zufälligen Buchstabenfolgen und würde sofort zum Angriffspunkt für die Codebrecher.

Sender und Empfänger erhalten eine Anzahl identischer Zufallsschlüssel in identischer Reihenfolge auf Vorrat. Für den ersten Nachrichtenaustausch wird der erste Schlüssel verwendet, für den zweiten der zweite usw. Die Methode wird als "one time pad" bezeichnet. Tatsächlich ist (oder war?) der "heiße Draht", über den der amerikanische und der russische Präsident kommunizieren können, mit one time pad gesichert.

2 Die Mechanisierung der Verschlüsselung

Bei der militärischen Nachrichtenübermittlung der Deutschen im Zweiten Weltkrieg wurde ein elektromechanisches Chiffrier- und Dechiffriergerät benutzt, die Enigma. Ein Buchstabe des Klartextes wurde eingetippt und an einem Lampenfeld leuchtete der verschlüsselte Buchstabe auf.

Die elektrischen Verbindungen der Tasten zu den Lampen waren in 3 Walzen enthalten, die sich, ähnlich wie bei einem mechanischen Kilometerzähler, nach jedem eingetippten Buchstaben weiterdrehten, wodurch sich die Verbindungen ständig änderten. Die 3 Walzen konnten gegen solche mit anderen elektrischen Verbindungen ausgewechselt und in je 26 möglichen Stellungen in das Gerät eingesetzt werden. Dazu kam noch, dass die Verdrahtung von 6 Tasten umgesteckt werden konnte.

Der Geheimtext wurde entschlüsselt, indem zu Beginn die gleichen Walzen in der gleichen Stellung in die Maschine eingesetzt wurden wie bei der Verschlüsselung, das heißt: Die Ersteinstellung ist der eigentliche Schlüssel der Enigma.

Der Schlüssel wurde täglich gewechselt. Dazu gab es Schlüsselbücher, in denen die Schlüssel, meistens für einen Monat, verzeichnet waren. Aber das war nicht sicher genug. Es ist für Kryptoanalytiker im allgemeinen leichter, eine Chiffre zu knacken, wenn es viel Text gibt, der mit demselben Schlüssel verschlüsselt ist. Der Chiffreur hat daher bei jeder Nachricht die Grundstellung der Walzen und damit den Schlüssel neu festgelegt. Den Tagesschlüssel verwendete er nur noch, um dem Dechiffreur den eigentlichen Schlüssel der Nachricht mitzuteilen.

Man war vollkommen davon überzeugt, dass eine solche Chiffre nicht zu knacken sei. Und doch ist den Engländern durch die Vorarbeit der Polen das scheinbar Unmögliche gelungen. An dieser Leistung hatte Alan Turing den wesentlichen Anteil. Das war, als sich beim U-Boot-Krieg im Atlantik das Blatt zu Gunsten der Alliierten wendete. Die intellektuelle Leistung der englischen Kryptoanalytiker war gewaltig, denn sie knackten nicht nur die Enigma, sondern auch noch andere weit stärkere kryptografische Verfahren. Man ist sich heute sicher, dass ihre Arbeit den Zweiten Weltkrieg wesentlich verkürzt hat.

3 Kryptografie und Computer

Die ersten Computer brachten noch keine große Veränderung in der Kryptografie. Man hatte nun, dank der Programmierbarkeit, ein beliebig komplexes und sehr schnelles Chiffrier- bzw. Dechiffriergerät zur Verfügung, bei dem die Buchstaben der Texte wie auch die Schlüssel intern als Zahlen verarbeitet wurden. Zahlenverarbeitung ist die eigentliche Stärke eines Computers.

Dringend erforderlich war es, Chiffrierverfahren zu standardisieren, um einen allgemeinen Nachrichtenaustausch zwischen Computern zu ermöglichen. Das geschah 1976, als DES (Data Encryption Standard) zum offiziellen amerikanischen Verschlüsselungsstandard wurde. Die National Security Agency (NSA), die für die Sicherung des Nachrichtenverkehrs von Regierung und Militär und auch für das Abhören fremder Nachrichten verantwortlich ist, hat die Zahl der Schlüssel begrenzt, um mit ihren eigenen leistungsstarken Computern gerade noch in DES-verschlüsselte Nachrichten einbrechen zu können.

Jede Verschlüsselung, so komplex sie auch sein mag, setzt sich aus den beiden einfachen Vorgängen der Transposition und Substitution zusammen. So auch bei DES, das eine unglaubliche Verwirbelung des Klartextes vornimmt. Simon Singh vergleicht es mit Teigkneten, nur dass bei DES die ursprünglichen Zutaten (Klartext) wiedergewonnen werden können, wenn man den Schlüssel kennt.

Die Voraussetzung dafür, dass Computer verschlüsselt kommunizieren konnten, war natürlich die geheime Schlüsselverteilung. Wie wurde sie praktisch umgesetzt? Da standen Computer, z.B. von Banken und großen Wirtschaftsunternehmen bereit, Nachrichten untereinander oder mit Kunden auszutauschen und mussten warten bis ein durchs Land reisender, vertrauenswürdiger Bote kam und den Schlüssel brachte. Die Kosten explodierten.

Überhaupt hat die geheime Übermittlung der Schlüssel den Kryptografen schon immer Kopfzerbrechen bereitet. Die Schlüsselverteilung des deutschen Oberkommandos im Zweiten Weltkrieg an die Enigma-Operateure war ein gewaltiges logistisches Problem.

Um was geht es eigentlich, wenn man in Betracht zieht, auch den Schlüssel über Computer auszutauschen? Um gesichert kommunizieren zu können, muss der Chiffrierschlüssel dem anderen Partner bekannt sein, damit er dechiffrieren kann. Um den Chiffrierschlüssel sicher dem Partner mitzuteilen, muss man aber gesichert kommunizieren können. Die Katze beißt sich in den Schwanz. Hat man es mit einem unlösbaren Problem zu tun?

4 Der größte kryptografische Fortschritt seit 2000 Jahren

Martin Hellman, Professor an der kalifornischen Stanford-Universität und seine Mitarbeiter Diffie und Merkle hatten 1976 den entscheidenden Gedanken: Ein Partner muss dem anderen nicht einen *ganz bestimmten* geheimen Schlüssel in öffentlicher Kommunikation mitteilen, sondern es genügt, wenn am Ende dieses Vorgangs beide Partner den *gleichen* geheimen Schlüssel besitzen.

Kryptografen stellen sich für ihre Diskussionen die drei Personen Bob, Alice und Eve vor. Bob und Alice wollen geheime Nachrichten austauschen, und Eve ist die Codebrecherin, die versucht, in den Besitz des Klartextes zu kommen.

Bob und Alice wollen irgendeinen Schlüssel (Zahl) erzeugen. Sie einigen sich zunächst auf eine Zahl, z.B. 4, die Eve natürlich abhört. Dann wählt Bob 2 und Alice 3 als persönliche Geheimzahl. Damit potenzieren beide die Zahl 4. Bob schickt sein Ergebnis 16 an Alice und Alice schickt ihr Ergebnis 64 an Bob. Wenn nun Alice Bobs Ergebnis mir ihrer Geheimzahl 3 potenziert, erhält sie 4096 und wenn Bob Alices Ergebnis mit seiner Geheimzahl 2

potenziert, erhält er auch 4096. Die Ergebnisse stimmen überein, weil neben der gleichen Ausgangszahl die gleichen Exponenten in die jeweilige Rechnung eingingen und die Reihenfolge keine Rolle spielt.

Bob und Alice besitzen die gleiche Zahl, den Schlüssel, der nicht von vornherein feststand, sondern in zwei Rechenschritten entstanden ist.

Bob : $4^2 = 16$ Weiter bei Alice: $16^3 = 4096$

Alice: $4^3 = 64$ Weiter bei Bob: $64^2 = 4096$

Natürlich geht es so nicht! Eve hat die Zwischenergebnisse mitbekommen und kann sich z.B. Bobs Geheimzahl 2 errechnen, indem sie die Aufgabe löst, den Exponent zu finden, mit dem Bob die Zahl 4 potenziert hat, um das Zwischenergebnis 16 zu erhalten. Dieser Rechenvorgang ist das Logarithmieren. Mit Bobs Geheimzahl 2 und Alices Zwischenergebnis 64, errechnet auch Eve den Schlüssel 4096.

Es wird deutlich, worauf es ankommt: Bob und Eve bauen jeder für sich den Schlüssel auf, indem sie ihre Geheimzahl einbringen und ihre Zwischenergebnisse austauschen, nur dürfte Eve daraus nicht auf die Geheimzahlen schließen können. Die Potenz, die zum Aufbau des Schlüssels verwendet wurde, ist wohl schuld daran, denn Eve kann das Potenzieren durch Logarithmieren einfach umkehren.

Potenzieren ist eine mathematische Funktion, und zwar eine umkehrbare. Hellman löste das Problem, indem er eine Funktion wählte, die sich praktisch nicht umkehren lässt (Einweg-Funktion), und zwar nahm er die Modular-Potenz.

Modular-Arithmetik gibt es auch im Alltag. Wenn man z.B. zu 18 Uhr 10 Stunden hinzu zählt, dann erhält man nicht 28 Uhr, sondern 4 Uhr. Das liegt daran, dass bei Uhrzeiten nur die Zahlen 0 bis 23 erlaubt sind.

Der Mathematiker sagt: (18 + 10) modulo 24 = 4.
Praktisch rechnet man: 18 + 10 = 28 : 24 = 1 Rest 4.
Der Divisionsrest ist also das Modular-Ergebnis.

Bob und Alice potenzieren auch jetzt, aber zusätzlich wird mit dem jeweiligen Potenzergebnis eine Modulo-Rechnung durchgeführt. Bob wählt die Geheimzahl 5 und Alice nimmt die Zahl 7. Beide einigen sich dann noch auf die Basis 15, mit der die Rechnung startet, und den Modul 213.

Bob rechnet mit seiner Geheimzahl 5: $15^5 = 759375 \quad \textit{und dann} \quad :213 = 3565 \; \textit{Rest} \; 30$
Alice rechnet mit 7: $15^7 = 170859375 \quad \textit{und dann} \quad :213 = 802156 \; \textit{Rest} \; 147$

Bob schickt sein Ergebnis 30 an Alice, und Alice sendet ihr Ergebnis 147 an Bob.

Alice rechnet nun: $30^7 = 21870000000 \quad \textit{und dann} \quad :213 = 102676056 \; \textit{Rest} \; 72$
Bei Bob ergibt sich: $147^5 = 68641485507 \quad \textit{und dann} \quad :213 = 322260495 \; \textit{Rest} \; 72$

Als Modular-Ergebnis (Rest) entsteht bei Bob und Alice die Zahl 72. Diese Zahl verwenden sie als Schlüssel für ihre Kommunikation.

Eve hat alle Zahlen, die Bob und Alice vereinbart und ausgetauscht haben, abgehört. Sie hat aber keine Möglichkeit, die Geheimzahlen und damit den Schlüssel zu errechnen, weil sich die Modular-Potenz nicht umkehren lässt.

Die Entdeckung Hellmanns und seiner Mitarbeiter verblüffte die Experten. Ab jetzt konnten „Bob und Alice im öffentlichen Gespräch miteinander ein Geheimnis erzeugen“, „die herrschende Lehre der Kryptografie musste umgeschrieben werden“ schreibt Simon Singh.

5 Öffentlicher und privater Schlüssel

Der Diffie-Hellmann-Merkle-Schlüsselaustausch stellt zwar einen gewaltigen Fortschritt dar, ist aber auch ein kleiner Rückschritt. Alice muss immer zu Hause sein, wenn Bob ihr eine geheime Nachricht schicken will, und Bob kann erst mit der Verschlüsselung beginnen, wenn die Schlüsselerzeugung mit Alice erledigt ist. Ohne ein "Vorgespräch" ist kein Nachrichtenaustausch möglich. Es sollte eine Möglichkeit geben, eine geheime Nachricht in Alices Briefkasten zu legen.

Whitfield Diffie kam 1975 auf folgende Idee: Bob chiffriert seine Nachricht für Alice mit einer speziellen Einweg-Funktion, die nicht von ihm und auch nicht von Eve umgekehrt werden kann. Das heißt, die Einweg-Funktion dient nicht zur Vereinbarung eines Schlüssels, sondern zur Verschlüsselung der Nachricht selbst. Nur Alice kann diese Einweg-Funktion anhand einer geheimen Information, nämlich ihrem privaten Schlüssel, umkehren und die Nachricht dechiffrieren.

Den Schlüssel, den Bob bei der speziellen Einweg-Funktion verwendet, hat Alice öffentlich verbreitet. Jeder kann ihr also jederzeit eine geheime Nachricht - auch für ihren Briefkasten - schicken.

So gut Diffies Idee war, die spezielle Einweg-Funktion musste erst noch gefunden werden, und es war keineswegs sicher, ob das gelingen würde. Doch 1977 hatten die drei amerikanischen Wissenschaftler Rivest, Shamir und Adleman Erfolg. Ihr Verfahren wird mit RSA bezeichnet, den Anfangsbuchstaben ihrer Namen.

Es ist bei RSA nicht erforderlich, immer wieder neue Schlüssel zu vereinbaren, um Codebrechern zuvor zukommen, denn das eigentliche Geheimnis hat der Empfänger erzeugt und dort bleibt es auch.

Neu ist ebenfalls, dass der Verschlüsselungs-Algorithmus nicht mehr aus einer mehr oder weniger verbalen Vorschrift für Substitution und Transposition von Buchstaben besteht, sondern dass eine mathematische Funktion angewandt wird, um die verschlüsselte Botschaft zu errechnen.

Bei RSA geht die Initiative vom Empfänger aus, das heißt Alice muss alle Vorbereitungen treffen.

Sie wählt zwei große Primzahlen p und q, die ihr Geheimnis bleiben, multipliziert sie und erhält den öffentlichen Schlüssel: $O = p \cdot q$

Alice teilt den Schlüssel O, neben einer frei gewählten Zahl Z, ihren möglichen Kommunikationspartnern mit, also auch Bob.

Alice muss die Zahl Z so wählen, dass Z und $(p-1)\cdot(q-1)$ keinen gemeinsamen Teiler haben.

Dann errechnet Alice die Zahl P, ihren privaten Schlüssel, mit folgender Formel:
$(Z \cdot P) \, mod [(p-1)\cdot(q-1)] = 1$ Alice hält P ebenso geheim wie ihre beiden Primzahlen.

Damit hat Alice ihre Vorbereitungen abgeschlossen.

Bob muss seinen Klartext zunächst in eine Folge von Zahlen verwandeln, die er dann einzeln mit $G = K^Z \, mod \, O$ verschlüsselt. O und Z sind die Zahlen, die er von Alice erhalten hat, K ist eine Zahl seines Klartextes und G ist die verschlüsselte Zahl.

Die Bedingung $K < O$ muss Bob bei der Umsetzung seines Klartextes in Zahlen einhalten. Die Methode stellt kein Geheimnis dar. Sie ist beliebig und muss auch dem Empfänger bekannt sein. Keinesfalls darf jeder Buchstabe einzeln umgewandelt werden. Wenn doch, wäre RSA so unsicher wie eine monoalphabetische Verschlüsselung.

Wenn Alice die Zahl G empfangen hat, entschlüsselt sie mit ihrem privaten Schlüssel P und erhält die Zahl K , die Bob verschlüsselt hat: $K = G^P \bmod O$ Alice gewinnt daraus die Buchstabenfolge des Klartextes, indem sie Bobs Umsetzungsmethode umkehrt.

Zum Nachvollziehen von RSA benutzt das folgende Beispiel kleine Zahlen:

Alice wählt $Z = 7$ sowie die Primzahlen $p = 5$ und $q = 11$. Sie gibt $Z = 7$ und $O = p \cdot q = 55$ öffentlich bekannt.

Die Zahl $(p-1) \cdot (q-1) = 40$ und $Z = 7$ sind wie gefordert teilerfremd.

Dann löst sie die Gleichung $(7 \cdot P) \bmod 40 = 1$, die dann erfüllt ist, wenn $(7 \cdot P)$ die Werte 1, 41, 81, 121, 161, 201 usw. annimmt.

Nur die Zahl 161 ergibt mit $(7 \cdot P) = 161$ den ganzzahligen Wert $P = 23$. Diese Zahl ist Alices privater Schlüssel.

Weil die Zahlen so klein sind, konnte der private Schlüssel durch Probieren gefunden werden. Das praktisch verwendete Verfahren für diesen Rechenschritt ist der erweiterte Euklidische Algorithmus. Im einfachsten Fall wird damit der größte gemeinsame Teiler errechnet.

Nun kann Alice die Nachricht von Bob erwarten.

Bobs Klartextzahl ist zum Beispiel $K = 9$ (Die Bedingung $K < O$ ist eingehalten.)

Er verschlüsselt sie mit $G = K^Z \bmod O$ und erhält $G = 9^7 \bmod 55 = 4$

Alice empfängt diese Zahl und entschlüsselt sie mit $K = G^P \bmod O$ Das ergibt $K = 4^{23} \bmod 55 = 9$, also die Zahl, die Bob verschlüsselt hat.

Man kann große Zwischenergebnisse, mit denen Taschenrechner nicht mehr umgehen können, vermeiden, indem man den Exponenten zerlegt. Mit $23 = 4 \cdot 5 + 3$ sieht die vorstehende Rechnung $K = 4^{23} \bmod 55 = 9$ dann so aus: $K = [(4^3 \bmod 55) \cdot (4^5 \bmod 55)^4] \bmod 55$

Was kann nun Eve ausrichten, um in den Besitz des Klartextes zu gelangen? Die Einweg-Funktion, die Bob benutzt hat, kann sie nicht umkehren, auch wenn sie die Zahlen Z und O kennt.

Eve kann nur den Klartext gewinnen, wenn sie genauso entschlüsselt wie Alice. Aber dazu braucht sie deren privaten Schlüssel P. Den kann Eve nur errechnen, wenn sie die geheimen Primzahlen p und q kennt, aus denen Alice ihren öffentlichen Schlüssel O gebildet hat. Wegen $O = p \cdot q$ muss Eve eine Primfaktorenzerlegung vornehmen.

Wenn es auch eine leichte Aufgabe ist, z.B. die Zahl 55 in ihre Primfaktoren 11 und 5 zu zerlegen, so ist das Problem praktisch unlösbar, wenn die Zahl in der Größenordnung von 10^{300} liegt. 100 Millionen PCs, die zusammenarbeiten, würden mehr als tausend Jahre brauchen, um die Primfaktoren solcher Zahlen zu finden.

Durch die Stärke des RSA-Verfahrens haben zur Zeit die Kryptografen einen klaren Vorteil gegenüber den Kryptoanalytikern.

RSA und den Hellman-Diffie-Merkle-Schlüsselaustausch haben *auch* die Engländer James Ellis, Clifford Cooks und Malcolm Williamson erfunden, und zwar schon 1973, was aber erst 1997 bekannt wurde, da die drei zur Geheimhaltung verpflichtet waren.

6 Pretty Good Privacy

Chiffre, bei denen die Partner den gleichen Schlüssel verwenden, werden als symmetrisch bezeichnet. RSA dagegen ist ein asymmetrisches Verfahren, denn Alice entschlüsselt anders als Bob verschlüsselt, insbesondere verwenden sie verschiedene Schlüssel.

Das asymmetrische RSA benötigt eine weitaus höhere Rechnerleistung als die symmetrischen Verfahren. Software zur RSA-Verschlüsselung wurde deshalb nur für Organisationen mit entsprechend leistungsstarken Rechnern entwickelt.

Phil Zimmermann jedoch war der Meinung, jeder sollte das Recht auf Privatsphäre haben und seine persönlichen Nachrichten schützen können. Je einfacher der Nachrichtenaustausch besonders durch das Internet wurde, umso einfacher war es auch, diese Nachrichten elektronisch zu belauschen. Deshalb stellte sich Phil Zimmermann die Aufgabe, eine Verschlüsselungs-Software zu entwickeln, die mit den Vorteilen von RSA einen durchschnittlichen PC nicht überforderte. Es entstand Pretty Good Privacy (PGP).

Seine Idee war, die eigentliche Nachricht mit einem starken symmetrischen Verfahren zu verschlüsseln, und nur dessen Schlüssel mit RSA zu chiffrieren, um den oben dargestellten Nachteil des Diffie-Hellmann-Merkle-Schlüsselaustauschs zu vermeiden. Auf diese Weise stellt RSA für einen PC kein Problem dar.

Und damit schließt sich der Kreis: Mit PGP wird das erreicht, was 1970 noch unmöglich schien: Einen bestimmten Schlüssel zusammen mit einer symmetrisch verschlüsselten Nachricht sicher zu übertragen.

Nicht nur die Sicherheit einer Nachricht, auch ihre Echtheit ist von größter Bedeutung. Einer einfachen E-Mail kann man nicht ansehen, ob sie tatsächlich von dem stammt, dessen Name darauf steht. PGP nutzt RSA auch für eine elektronische Unterschrift, da RSA umkehrbar ist:

Alice will mit Bob ausprobieren, ob ihr RSA auch dann funktioniert, wenn sie eine Nachricht mit ihrem privaten Schlüssel verschlüsselt und Bob die Nachricht mit Alice öffentlichem Schlüssel entschlüsselt. Von Geheimhaltung kann natürlich nicht die Rede sein, weil alle Welt Alices öffentlichen Schlüssel kennt.

Alice verschlüsselt ihre Nachricht 17 mit: $17^{23} \, mod \, 55 = [(17^3 \, mod \, 55) \cdot (17^5 \, mod \, 55)^4] \, mod \, 55 = 18$
und Bob entschlüsselt: $18^7 \, mod \, 55 = 17$ Bob erhält tatsächlich Alices Nachricht.

Mittlerweile hat sich Bob einen öffentlichen und privaten RSA-Schlüssel zugelegt, damit auch Alice ihm Nachrichten schicken kann. Alice will nun die Umkehrbarkeit von RSA nutzen, um eine mit RSA verschlüsselte Nachricht an Bob elektronisch zu unterschreiben.

Sie verschlüsselt ihre Nachricht zuerst mit ihrem privaten Schlüssel, was ihre elektronische Unterschrift ist, und dann mit Bobs öffentlichem Schlüssel, der die Geheimhaltung garantiert. Den Geheimtext sendet sie an Bob, der umgekehrt handelt: Er entschlüsselt zuerst mit seinem privaten Schlüssel und anschließend, da Alice als Absender auf der Nachricht steht, mit Alices öffentlichem Schlüssel. Da ein sinnvoller Text entstanden ist, kann Bob sicher sein, dass es wirklich Alice war, die ihm geschrieben hat.

Pretty Good Privacy hat seinem Schöpfer Phil Zimmermann eine Menge Ärger eingebracht, denn er stellte PGP im Internet zur Verfügung (http://www.pgpi.com/). Die amerikanische Regierung stufte PGP wegen der starken Verschlüsselung als Kriegswaffe ein, und man warf Phil Zimmermann u. a. unerlaubten Kriegswaffenexport vor. Amerikanische Softwareprodukte, z.B. Browser, dürfen nur mit einer schwachen Verschlüsselung exportiert

werden. Mittlerweile ist Phil Zimmermann rehabilitiert.

Die Diskussion über starke kryptografische Verfahren für jedermann ist noch im Gange. Denn wo Licht ist, ist auch Schatten. Der Terrorismus und das internationale Verbrechen wissen Programme wie PGP ebenfalls zu schätzen, weil die Verbrechensbekämpfung in den stark verschlüsselten illegalen Nachrichtenaustausch kaum noch eindringen kann.

7 Zum Schluss

Der Beitrag ist ein Versuch, die Methoden der Kryptografie, die Simon Singh in seinem Buch behandelt, in ihrem Kern geschlossen darzustellen und auch mathematisch nachvollziehbar zu machen.

Simon Singh beschreibt neben kryptografischen auch kryptoanalytische Verfahren, umrahmt von vielen Anekdoten und Geschichten. Einer seiner Schwerpunkte ist natürlich die Historie der Kryptografie.

Wer sich weitergehend für Kryptografie interessiert, sollte nicht versäumen, dieses Buch zu lesen. Ein angenehmerer und leichterer Einstieg in das Wissensgebiet ist kaum denkbar.