

Eine kurze Geschichte der Schlüssel

Johannes Buchmann und Alex Wiesmaier

Vertraulichkeit und Verschlüsselung

Emails enthalten oft Informationen, die nicht für jeden bestimmt sind. Beim Homebanking werden PINs und TANs versendet. Unternehmen können ihre Steuererklärungen elektronisch abgeben.

Rechtsanwälte und Notare tauschen mit Gerichten und Behörden elektronisch Informationen aus. Wie kann Vertraulichkeit in einer digitalen Welt erreicht werden?

Daten bleiben vertraulich, wenn sie sicher *verschlüsselt* werden. Eine Verschlüsselungsmethode, die schon Caesar benutzte, besteht darin, jeden Buchstaben in einem Text durch einen anderen zu ersetzen. Man kann zum Beispiel Buchstaben immer durch die übernächsten Buchstaben im Alphabet ersetzen. Dann würde aus dem *Klartext* „gut“ der *Schlüsseltext* „iuv“. Das sieht zwar ziemlich unleserlich aus, ist aber leicht zu knacken. Man muss nur wissen, dass „e“ der häufigste Buchstabe der deutschen Sprache ist. Dann sucht man den häufigsten Buchstaben im Schlüsseltext und weiß: das war vorher „e“. Genauso findet man die Bedeutung der anderen Buchstaben. Einen solchen Angriff nennt man *Frequenzanalyse*. Das hört sich einfach an, war aber Caesar offenbar nicht bekannt. Damit ist ein Prinzip der Verschlüsselungslehre schon beschrieben. Ein *Kryptologe* erfindet ein Verschlüsselungsverfahren. Ein *Kryptanalytiker* bricht das Verfahren. Ein neues Verschlüsselungsverfahren wird entwickelt, das den Angriff berücksichtigt. Ein Katz-und-Maus-Spiel. Kryptologen und Kryptanalytiker werden immer raffinierter. 1976 wurde der Data Encryption Standard DES als sicheres Verschlüsselungsverfahren in den USA standardisiert. 14 Jahre später erfanden Biham und Shamir eine neue Angriffstechnik: die *differentielle Kryptoanalyse*. Wirklich unsicher wurde DES aber 1998, als der Spezialcomputer *Deep-Crack* einen geheimen DES-Schlüssel durch Ausprobieren in 56 Stunden finden konnte. Der 56-Bitschlüssel war einfach zu kurz. Das war das Aus für DES. Der Nachfolger, der Advanced Encryption Standard AES, wurde im Jahr 2000 standardisiert. Er gilt als sicher gegen differentielle Kryptoanalyse. Andere Beispiele moderner Verschlüsselungsverfahren sind *Twofish* und *Serpent*. Am besten wäre es natürlich, wenn man Verschlüsselungsverfahren hätte, deren Sicherheit garantiert ist, zum Beispiel durch einen mathematischen Beweis. Heute weiß aber niemand, wie man das machen soll.

Public-Key-Verschlüsselung

Wenn eine Email mit AES verschlüsselt werden soll, müssen Sender und Empfänger vorher einen geheimen Schlüssel austauschen. Da sie sich aber vielleicht vorher noch nie getroffen haben und das Internet unsicher ist, geht das nicht so einfach. Würden nämlich alle gut 1,7 Milliarden Internet-Teilnehmer prophylaktisch einen geheimen Schlüssel austauschen, wären das c.a. 1,5 Trillionen Schlüssel. Das ist nicht zu organisieren.

Das Schlüsselverteilungsproblem wurde in den 70er Jahren durch Erfindung der *Public-Key-Verschlüsselung* gelöst. Wie das funktioniert, wird an einem Beispiel erklärt. Herr Schmitz und Frau Müller möchten mit den anderen Internetnutzern verschlüsselt kommunizieren können. Dazu benutzen beide ihr eigenes *Schlüsselpaar*. Es besteht aus einem *öffentlichen Schlüssel*, der zusammen mit den

öffentlichen Schlüsseln vieler anderer auf einer Webseite steht, und einem *privaten Schlüssel*. Seinen privaten Schlüssel kann Herr Schmitz benutzen, um Nachrichten, die mit seinem öffentlichen Schlüssel verschlüsselt worden sind, wieder lesbar zu machen. Das Analoge kann Frau Müller mit ihrem privaten Schlüssel machen. Beide halten ihre privaten Schlüssel geheim, zum Beispiel auf einer Chipkarte. Eines Tages lernt Herr Schmitz Frau Müller über eine Dating-Agentur kennen. Er möchte ihr per Email viel von sich schreiben. Er will aber nicht, dass andere seine Emails lesen könne. Also besorgt er sich den öffentlichen Schlüssel von Frau Müller von der Webseite und verschlüsselt seine Liebesmail damit. Frau Müller kann sie mit ihrem privaten Schlüssel lesen. Ihre Antwort verschlüsselt sie mit dem öffentlichen Schlüssel von Herrn Schmitz. Das wichtige ist: beide kannten sich vorher nicht und als sie miteinander vertraulich kommunizieren wollten, brauchten sie keine Schlüssel auszutauschen.

Das älteste, bekannteste und bis heute meist verwendete Public-Key-Verfahren stammt aus dem Jahr 1977 und heißt *RSA* nach seinen Erfindern Rivest, Shamir und Adleman, die dafür 2002 den Turing-Award, den „Nobelpreis der Informatik“, erhielten. Es wird heute bei fast jeder elektronischen Banktransaktion verwendet. Modernere Verfahren beruhen auf sogenannten *elliptischen Kurven*.

Elektronische Signaturen

Vertraulichkeit ist nicht das einzige und wahrscheinlich nicht einmal das wichtigste Schutzziel in der elektronischen Kommunikation. Wenn die Milliarden Benutzer von Microsoft Betriebssystemen ein Update bekommen, möchten sie sicher sein, dass es *authentisch* ist, also wirklich von Microsoft kommt und nicht in Wirklichkeit eine böartige Software ist, die die Festplatte löscht. Microsoft garantiert das mit einer *elektronische Signatur*. Die berechnet Microsoft mit Hilfe eines privaten Schlüssels. Jeder Microsoft-Rechner kennt den dazu passenden öffentlichen Schlüssel und verifiziert die Signatur damit. Ohne elektronische Signaturen wäre es viel zu gefährlich, Computer mit dem Internet zu verbinden. Hacker finden nämlich immer wieder Angriffsmöglichkeiten. Die müssen durch Updates repariert werden und die Updates müssen authentisch sein. Das gilt nicht nur für Betriebssysteme sondern für die ganze Palette der Anwendungssoftware.

Elektronische Signaturen haben noch viel weitreichendere Anwendungen. Gibt ein Unternehmen eine elektronische Steuererklärung ab und stellt sich Jahre später heraus, dass diese Erklärung betrügerisch war, muss das gerichtlich beweisbar sein. Darum muss das Unternehmen elektronische Steuererklärungen elektronisch signieren. Mit dem öffentlichen Schlüssel kann eine Richterin jederzeit die elektronische Unterschrift verifizieren und sich davon überzeugen, dass das Unternehmen tatsächlich diese Erklärung abgegeben hat. Das Unternehmen kann die Erklärung später nicht mehr abstreiten. Ohne Signatur könnte das Unternehmen behaupten, das Finanzamt habe die Erklärung nachträglich manipuliert. Die Nichtabstreitbarkeit spielt auch in vielen anderen Bereichen des öffentlichen Lebens eine wichtige Rolle. Darum existiert in Deutschland wie in vielen anderen Ländern ein Signaturgesetz, das die Verwendung von elektronischen Signaturen regelt.

Das bekannteste und weit verbreiteteste elektronische Signaturverfahren stammt auch von Rivest, Shamir und Adleman aus dem Jahr 1977 und heißt *RSA-Signaturverfahren*. Aber auch in diesem Bereich sind elliptische Kurven auf dem Vormarsch. Sie erlauben die Verwendung von viel kleineren Schlüsseln,

und werden zum Beispiel auf dem deutschen elektronischen Reisepass und auf dem zukünftigen elektronischen Personalausweis verwendet.

Die Zukunft der Kryptographie

Die RSA-Verfahren beziehen ihre Sicherheit aus der Schwierigkeit eines alten mathematischen Problems: der Zerlegung von Zahlen in ihre Primfaktoren. Es ist zwar leicht, die Zerlegung $6 = 2 \cdot 3$ zu bestimmen. Aber herauszufinden, dass $54991 = 127 \cdot 433$ ist und dass die beiden Faktoren Primzahlen sind, ist schon deutlich schwieriger. Der Leser kann es ja einmal mit der Zerlegung von 75151 versuchen. Heute ist die Faktorisierung von Zahlen mit 300 oder mehr Dezimalstellen völlig unmöglich. Ist RSA darum sicher? Jetzt ja, aber später? Es ist bis jetzt nicht bewiesen, dass Primfaktorzerlegung immer schwierig bleibt. Die Kryptographen am Center for Advanced Security Research Darmstadt (www.cased.de) und überall auf der Welt suchen daher nach neuen Verfahren mit wirklichen Sicherheitsgarantien. Sie tun das in Kooperation mit Quantenphysikern, die RSA unsicher machen würden, wenn sie große Quantencomputer bauen könnten. Quantenphysiker haben aber auch Ideen für kryptographische Verfahren, die sicher bleiben solange die Gesetze der Quantenmechanik gelten. Und daran glauben die meisten. Aber ob das jemals praktisch wird?

Kryptographie Timeline

- 2000 Ägyptische Geheimschrift
- 100 Caesar-Verschlüsselung
- 600 Frequenzanalyse wird bekannt
- 1928 Deutsche Reichswehr nutzt Enigma
- 1940 Die Briten brechen Enigma
- 1976 Data Encryption Standard DES
- 1977 RSA
- 1990 Differentielle Kryptoanalyse schwächt DES
- 1998 Deep-Crack bricht DES
- 1994 Quantenalgorithmus zur Primfaktorzerlegung
- 1997 Deutsches Signaturgesetz
- 2000 Advanced Encryption Standard AES
- 2001 Experimenteller Quantencomputer faktorisiert 15
- 2009 Faktorisierung einer Zahl mit 232 Dezimalstellen