2020/04 Networld

https://shop.jungle.world/artikel/2020/04/alice-bob-und-die-verschluesselung

Verschlüsselte Kommunikation und ein Pärchen namens Alice und Bob

Alice, Bob und die Verschlüsselung

Von **Barbara Eder**

Kryptographie gilt vielen als sperriges Wissensgebiet, das aufwendige Berechnungen und exklusives Wissen voraussetzt. Doch Programme wie PGP und GPG ermöglichen gesicherte Standards der verschlüsselten Kommunikation für alle.

Von außen sieht sie aus wie eine einfache Kofferschreibmaschine, in ihrem Inneren verbirgt sich eine komplexe elektronische Architektur: Die 1918 von Arthur Scherbius patentierte Chiffriermaschine Enigma zählte zu den ersten elektrisch betriebenen Verschlüsselungsapparaten in Europa. Sie basiert auf drei bis vier Rotorscheiben mit je 26 Kontakten auf beiden Seiten, die lose miteinander verdrahtet sind. Sobald man auf der Tastatur einen Buchstaben drückt, wird ein Signal an den ersten Rotor gesendet, es durchläuft dann alle weiteren Verbindungen und tritt als chiffrierter Buchstabe an einem der Kontakte des letzten Rotors wieder aus. Wegen einer Vielzahl an möglichen Verbindungen ist das Ergebnis stets ein anderes – und doch kalkulierbar. Im Dezember 1939 knackte der britische Kryptoanalytiker Alan Turing, fußend auf polnischen Vorarbeiten, den Code der deutschen Enigma. Das Geheimnis von Scherbius’ Erfindung war gelöst und die Funksprüche aus Nazideutschland konnten in Klartext übertragen werden.

Seit Beginn des Informationszeitalters ist Kryptographie nicht mehr nur eine kriegswichtige Wissenschaft, für die sich lediglich die NSA, der BND und andere Geheimdienste interessieren. Kryptographie ist zu einer weit verbreiteten Technik zur Bewahrung der Integrität von Nachrichten geworden, die ihre Empfängerinnen und Empfänger auf elektronischem Weg erreichen. Bei den dazugehörigen Verfahren handelt es sich auch um Mittel im Kampf um die Privatheit digitaler Daten in Zeiten ihres wachsenden Marktwerts. Generiert und ausgetauscht werden diese vornehmlich im Internet und häufig werden sie an die Werbekunden großer Plattformen weiterverkauft. Gelegenheit dazu geben auch viele auf iPhones und Android-Mobiltelefonen vorinstallierte Messenger, die über eine mangelhafte oder gar keine Ende-zu-Ende-Verschlüsselung, also Verschlüsselung über alle Übertragungsstationen hinweg, verfügen. Idealtypisch ist in dieser Hinsicht der proprietäre Messenger-Dienst Whatsapp, der Metadaten -

unaufgefordert mitschickt und sie mit seinem Eigentümer Facebook teilt. Auch die Kommunikation über SMS und MMS erfolgt seit jeher unverschlüsselt.

Kaum jemand versendet heutzutage noch Nachrichten im handversiegelten Umschlag, die Marken auf den Briefen des 21. Jahrhunderts heißen timestamps. Offen zugängliche Nachrichten sollten jedoch insbesondere während des Transportwegs geschützt werden. Um ein Mitlesen durch Dritte zu verhindern und zu garantieren, dass an der elektronischen Botschaft nichts verändert wurde, sollte diese vom Sender ver- und vom Empfänger entschlüsselt werden. Dafür gibt es digitale Schlüssel, generiert mit Hilfe von Verschlüsselungsalgorithmen, die auf mathematischen Berechnungsverfahren basieren, beispielsweise diskrete Logarithmen großer Primzahlen mit Restgrößen oder elliptischen Kurven und endlichen Gruppen. Ein Schlüssel besteht aus einem privaten und einem öffentlich Teil, wobei der sogenannte public key allgemein zugänglich ist. Jeder kann damit Nachrichten verschicken, sie dechiffrieren können hingegen nur jene, die über den privaten Teil desselben Schlüssels verfügen. Seine Anwendung macht es auch möglich, Daten zu signieren, entschlüsseln kann sie nur der Schlüsselbesitzer selbst.

Die erste Software, die das Recht auf Verschlüsselung demokratisiert hat, heißt PGP – »Pretty Good Privacy« – und wurde 1991 vom US-amerikanischen Softwareentwickler Philip Zimmermann unter einer Creative-Commons-Lizenz veröffentlicht. Dafür handelte Zimmermann sich prompt eine Klage der US-amerikanischen Regierung wegen angeblicher Verletzung von Exportbeschränkungen kryptographischer Software ein, die erst fünf Jahre später fallengelassen wurde. Sein Programm verbreitete sich rasant und wurde unter dem Namen GPG oder GnuPG – eine Abkürzung für »Gnu Privacy Guard« – für Linux-Userinnen und -User adaptiert. Wenn die in sämtlichen informationstheoretischen Modellen als Synonym für Sender und Empfänger gebrauchten fiktiven Personen Alice und Bob heutzutage eine E-Mail austauschen, dann greifen sie idealerweise auf eines dieser beiden Verschlüsselungsverfahren zurück.

Seit Alice und Bob in einem wissenschaftlichen Artikel von 1978 erstmals erwähnt wurden, wird die Nachricht M nicht länger zwischen A und B ausgetauscht, sondern zwischen diesen beiden fiktiven Entitäten. Erste Überlegungen zur theoretischen Rekonstruierbarkeit von Nachrichten zwischen Sender und Empfänger beginnt hingegen schon mit den Postulaten der Shannon’schen Informationstheorie (1950). Dieser zufolge verfügt jede Nachricht über eine sogenannte Entropie, das Maß für den Informationsgehalt einer Nachricht, mit dem bestimmt werden kann, wie viele Bits bekannt sein müssen, um die Nachricht im Fall einer Störung vollständig rekonstruieren zu können. Noch immer ist das der Gradmesser für viele Verschlüsselungsalgorithmen, die meisten davon arbeiten mit blockweiser Chiffrierung.

Neben den klassischen Verfahren für den Austausch zwischen zwei Personen gibt es auch die gruppenorientierte Kryptographie. Dabei kennt jeder Teilnehmer nur einen Ausschnitt einer Nachricht, ihr Ganzes ergibt sich erst aus den dechiffrierten Teilnachrichten. Infolge der schnellen Fortschritte auf dem Gebiet der Verschlüsselung blicken auch Alice und Bob auf eine wechselvolle Geschichte zurück. Der Kryptograph John Gordon machte 1984 aus Bob einen Börsenmakler und aus Alice eine Spekulantin. Seit 1988 wird das Duo um eine Figur ergänzt, die vor allem durch ihre Unsichtbarkeit auffällt. Mit »Eve, the eavesdropper«

(Eva, die Lauscherin) kam eine dritte fiktive Person hinzu, die im Geheimen lauscht, gefolgt von Chuck, dem stillen Beobachter, und Craig, dem heimlichen Passwortknacker. Mit Faythe (lies: faith, Vertrauen) wurde eine Person kreiert, die den vertrauenswürdigen Aufbewahrungsort von elektronischen Schlüsseln im Betriebssystem symbolisieren soll.

Wer heutzutage verschlüsselt, hat nur selten etwas Illegales zu verbergen. Unter kritischen Computer-Usern ist Kryptographie längst ein Standard der elektronischen Alltagskommunikation. Anders als in vielen Darstellungen seitens staatlicher Behörden sind Alice und Bob nicht kriminelle Subjekte, sondern mündige Bürger einer digitalen Welt.

Das dazugehörige Informationsübertragungsmodell ist unter Insidern hingegen zur Parodie geworden: Mesalliancen zwischen Bob, Alice und Eve sind darin ebenso häufig wie der Austausch des gesamten Personals. Vor acht Jahren etwa schickte der indische Informatiker Srini Parthasarathy sämtliche Mitglieder der kryptographischen Familie in den Urlaub und nannte die Zwischenmieter Sita und Rama. Auch im von einem Sprecher mit dem Pseudonym »oots« beim 36. Chaos Communication Congress des Chaos Computer Clubs (36C3) im Dezember gehaltenen Vortrag »Cryptography Demystified. An Introduction without Maths« waren Alice und Bob ganz andere: Erstere wurde zu Carola Rackete und ihr Kommunikationspartner zu jemandem, der die Arbeit der Flüchtlingsrettungsorganisation Sea-Watch finanziell unterstützen will. Auch dafür braucht es Verschlüsselung. Nicht, um undeklarierte Summen heimlich im Online-Ozean verschwinden zu lassen, sondern weil das Recht auf private Kommunikation ein Menschenrecht ist.