Spektrum
DER WISSENSCHAFT

KOMPAKT

Vertrauliches verschlüsseln – Kodes knacken

KRYPTOGRAFIE

Moderne Kryptotechnik
Vertraulichkeit ist machbar

Geldsysteme
Die Zukunft der Kryptowährung

Quantenkryptografie
Alice und Bob im Geheimraum

EDITORIAL

Folgen Sie uns:

Janosch Deeg

Liebe Leserin, lieber Leser,

immer mehr Menschen achten darauf, dass ihre Daten im digitalen Raum geschützt sind. Dabei nutzen sie Verschlüsselungsverfahren – sei es bei Emails, Online-Banking oder Apps für das Smarthphone. Während man früher Textnachrichten kodierte, indem man auf eine bestimmte Art und Weise Buchstaben per Hand durch andere ersetzte, übernehmen das heutzutage ausgeklügelte Algorithmen. Den Schlüssel kennt dabei meist nur noch der Empfänger. Fängt jemand die vertraulichen Daten ab, hat er kaum eine Chance, sie zu dechiffrieren. Das könnte sich aber in Zukunft ändern – dann, wenn Quantencomputer tatsächlich Realität werden. Mit ihren enormen Rechenleistungen könnten sie auch »sichere« Kodes knacken; gleichzeitig wären mit ihnen aber auch neuartige, noch sicherere Kryptografieverfahren möglich.

Eine aufschlussreiche Lektüre wünscht Ihnen

Erscheinungsdatum dieser Ausgabe: 13.06.2016

IMPRESSUM

Chefredakteure: Prof. Dr. Carsten Könneker (v.i.S.d.P.), Dr. Uwe Reichert
Redaktionsleiter: Christiane Gelitz, Dr. Hartwig Hanser, Dr. Daniel Lingenhöhl
Art Director Digital: Marc Grove
Layout: Oliver Gabriel
Schlussredaktion: Christina Meyberg (Ltg.), Sigrid Spies, Katharina Werle
Bildredaktion: Alice Krüßmann (Ltg.), Anke Lingg, Gabriela Rabe
Produktmanagerin Digital: Antje Findeklee
Verlag: Spektrum der Wissenschaft Verlagsgesellschaft mbH, Tiergartenstr. 15-17, 69121 Heidelberg, Tel. 06221 9126-600, Fax 06221 9126-751; Amtsgericht Mannheim, HRB 338114, USt-Id-Nr. DE147514638
Geschäftsleitung: Markus Bossle, Thomas Bleck
Marketing und Vertrieb: Annette Baumbusch (Ltg.)
Leser- und Bestellservice: Helga Emmerich, Sabine Häusser, Ute Park, Tel. 06221 9126-743, E-Mail: service@spektrum.de

Die Spektrum der Wissenschaft Verlagsgesellschaft mbH ist Kooperationspartner der Nationales Institut für Wissenschaftskommunikation gGmbH (NaWik).

Bezugspreis: Einzelausgabe € 4,99 inkl. Umsatzsteuer
Anzeigen: Wenn Sie an Anzeigen in unseren Digitalpublikationen interessiert sind, schreiben Sie bitte eine E-Mail an anzeigen@spektrum.de.

INHALT

FOTOLIA / DEEPAGOPI2011

ISTOCK / DIETER MEYRL

ISTOCK / ANETLANDA

ISTOCK / PETAR CHERNAEV

ÜBERBLICK

Zehn Schlüsselfragen der Kryptografie

von Eva Wolfangel

FOTOLIA / DEEPAGOPI2011

Seit dem iPhone-Hack durch das FBI und der Einführung der Ende-zu-Ende-Verschlüsselung von WhatsApp fragen sich viele, wie sicher Verschlüsselung ist und wie sie überhaupt funktioniert. Hier die zehn wichtigsten Fakten zum Thema – und ein kleines Rätsel, das viel verdeutlicht.

Wie funktioniert Verschlüsselung?

Einfache Verschlüsselungsverfahren gab es bereits vor Tausenden von Jahren. So entwickelte schon Kaiser Julius Cäsar 50 v. Chr. eine Methode, bei der man jeden Buchstaben durch denjenigen ersetzt, der 13 Stellen später im Alphabet kommt. Ein derart umgewandelter Text ist unlesbar für jeden, der die Verschlüsselungsmethode oder kurz den Schlüssel nicht kennt.

Dieses später »Cäsar-Verschlüsselung« genannte Verfahren basiert auf einer symmetrischen Verschlüsselung. Der Text wird auf die gleiche Weise ver- wie entschlüsselt. Der Haken solcher Methoden: Alle Beteiligten müssen den Schlüssel kennen. Dazu muss man diesen möglichst sicher weitergegeben. Denn sobald ein Spion ihn bekommt, ist die Verschlüsselung wertlos. Dann muss man den alten Schlüssel ändern – und auch darüber wieder alle auf sicherem Weg informieren.

Um diese Probleme zu umgehen, verwendet man heute asymmetrische Verfahren: Die Daten werden mit einem Schlüssel chiffriert, der öffentlich zugänglich ist, und mit einem privaten Schlüssel dechriffiert, den nur der Empfänger der Nachricht hat. Man kann sich das vorstellen wie eine Kiste, die mit einem geöffneten Vorhängeschloss versehen ist: Jeder kann etwas in diese Kiste hineinlegen und das Schloss ohne Schlüssel zudrücken. Nur der Empfänger aber kann es mit seinem Schlüssel öffnen.

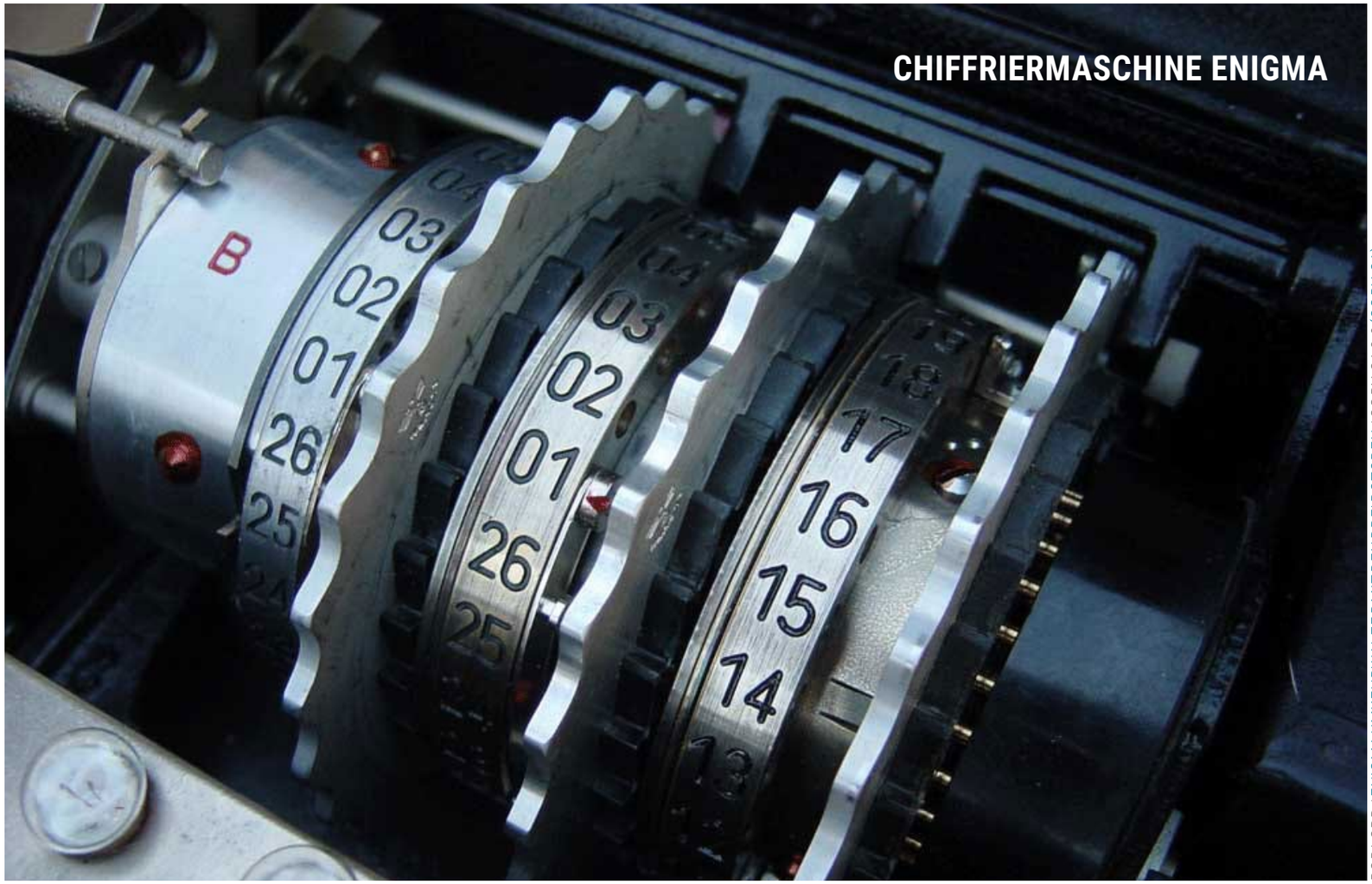
Mathematisch funktioniert das vereinfacht gesagt über Berechnungen, die in eine Richtung sehr leicht, in die andere hingegen schwierig zu lösen sind, wie beispielsweise die Multiplikation von Primzahlen. Der öffentliche Schlüssel ist das Ergebnis der Multiplikation. Um die Daten zu entschlüsseln, braucht man aber die beiden Ausgangsprimzahlen. Diese sind der private Schlüssel. Schon bei kleinen Zahlen wird der Effekt deutlich. Testen Sie selbst: Welche beiden Primzahlen muss man multiplizieren, um auf das Ergebnis 879 zu kommen? Ein Taschenrechner ist natürlich erlaubt. Das Ergebnis finden Sie am Ende dieses Artikels.

Was bedeutet Ende-zu-Ende-Verschlüsselung?

Bei der Ende-zu-Ende-Verschlüsselung werden die Daten beim Sender verschlüsselt und erst beim Empfänger wieder entschlüsselt. Sollten sie unterwegs abgefangen werden, sind sie ohne Schlüssel unlesbar. Und auch der Anbieter selbst, auf dessen Servern die Daten liegen, hat sie nur in

verschlüsselter Form vorliegen. Wenn also Behörden beim Anbieter die Daten anfordern, kann dieser nur wertlose verschlüsselte Informationen herausgeben – ob er will oder nicht.

Das Gegenstück dazu ist die Transportverschlüsselung, auch Punkt-zu-Punkt-Verschlüsselung genannt. Diese nutzt beispielsweise die Initiative »E-Mail made in Germany«, was immer wieder für Protest sorgt. Schließlich verkauften die Anbieter ihre Verschlüsselung in Folge der NSA-Affäre als besonders sicher und innovativ, obwohl nur der Weg zwischen den einzelnen Punkten – beispielsweise zwischen zwei Geräten in einem Rechnernetz – gesichert ist. Auf den Servern der Anbieter hingegen liegen die Mails unverschlüsselt vor.



CHIFFRIERMASCHINE ENIGMA

BOB LORD / ENIGMA UMKEHRWALZE B MIT DEN DREI ROTOREN / CC BY-SA 3.0 (CC BY-SA)

Welche Faktoren machen eine Verschlüsselung sicher?

Die Länge des Schlüssels spielt eine Rolle dabei, wie kompliziert es ist, ihn zu erraten, und folglich auch wie rechenintensiv. Mit größeren Primzahlen steigt im Allgemeinen der Aufwand, den Kode zu knacken. Doch heutzutage ist weniger die Verschlüsselung an sich das Problem, sondern die richtige Anwendung und eine gute Implementierung. Ein Verschlüsselungsalgorithmus kann noch so gut sein: Wenn er schlecht in »Maschinensprache« übersetzt ist, die Computerprozessoren verstehen, hat er Lücken. Die nächste Hürde sind Fehler in der Nutzung. Verschlüsselung funktioniert nur, wenn man auch den richtigen Schlüssel nutzt (siehe auch den Abschnitt »Was ist eine Man-in-the-middle attack?«), was man eigentlich nachprüfen müsste, indem man den Kontakt persönlich trifft oder auf einem anderen Wege verifiziert, dass der Schlüssel auch zu der Person gehört, von der man es vermutet.

Objektive Faktoren, die eine gute Verschlüsselung ausmachen, sind außerdem: eine Ende-zu-Ende- und nicht nur eine Transportverschlüsselung, die der Anbieter selbst nicht durchbrechen kann, die Möglichkeit, Kontakte zu verifizieren, und

ein Verfahren, das verhindert, dass ein Angreifer mit gestohlenen Schlüsseln Kommunikation aus der Vergangenheit entschlüsseln kann. Außerdem ist jede Maßnahme, den Kode überprüfbar zu machen, ein gutes Zeichen, beispielsweise die Veröffentlichung des Quellcodes.

Wie sicher ist die neue WhatsApp-Verschlüsselung?

WhatsApp verschlüsselt nun auf der Grundlage des Signal Protocol, eines Messengers, den auch Edward Snowden empfiehlt. Anders als Signal ist WhatsApp aber keine Open-Source-Software, weshalb die Qualität der Verschlüsselung von außen schwerer zu überprüfen ist. Doch der Druck auf WhatsApp und Facebook, das den Messenger aufgekauft hat, ist groß, sagt Kryptografieexperte Michael Backes von der Universität des Saarlandes: »Irgendjemand wird die App reverse engineeren, also wieder in lesbaren Quellcode umwandeln. Tauchen dann grobe Fehler auf, gibt das ein Reputationsproblem für die Firmen.«

Grund zum Misstrauen gibt allerdings der bisherige Umgang von WhatsApp mit Verschlüsselung: Als Experten des Heise-Verlags vor etwa einem Jahr die damals schon angekündigte Ende-zu-Ende-Verschlüsselung untersuchten, wies sie massive Lücken auf. Zu der Zeit wurden nur Nachrichten zwischen Android-Geräten chiffriert verschickt. Zudem konnten Nutzer nicht überprüfen, welche Nachrichten verschlüsselt wurden und welche nicht. Das scheint nun ausgemerzt. Die Experten testeten nämlich auch die aktuelle WhatsApp-Verschlüsselung: »Unsere Beobachtungen zeigen, dass verschiedene Clients tatsächlich wie versprochen ver- und entschlüsseln. Die von uns unternommenen Versuche, dies zu umgehen oder auszutricksen, schlugen fehl.«

WhatsApp betont zudem in einem Whitepaper (PDF), dass selbst wenn der private Schlüssel vom Smartphone eines Nutzers gestohlen würde, der Täter damit nicht im Nachhinein früher übertragene Nachrichten entschlüsseln könne.

Auch die US-Datenschutz-NGO Electronic Frontier Foundation hat die WhatsApp-Verschlüsselung getestet und WhatsApp in ihrem »Secure Messaging Scorecard« fast die Bestpunktzahl gegeben. Einen Punkt Abzug gab es für den fehlenden offenen Quellcode. Ein Blick auf die Karte lohnt sich: Der Facebook-Chat bekommt nur zwei von sieben Punkten, ebenso wie Google Hangout; Skype rangiert mit nur einem Punkt unter den unsichersten Messengern. Signal gehört mit der vollen Punktzahl zu den sichersten.

Wovor schützt Verschlüsselung nicht?

Ein großer Schwachpunkt für die Sicherheit, der sich nicht einfach durch die Verschlüsselung von Nachrichten ausmerzen lässt, sind die so genannten Metadaten. Diese Daten begleiten jede digitale Kommunikation und beschreiben beispielsweise, zwischen wem, wann und gegebenenfalls von wo aus die Teilnehmer sich unterhalten. Das kann für Geheimdienste interessanter sein als der Inhalt der vielen Nachrichten, der aufwändig auszuwerten ist. Wie viel diese Metadaten über unser Leben verraten, zeigt ein mittlerweile berühmt gewordenes Experiment des Grünenpolitikers Malte Spitz in Zusammenarbeit mit dem Datenjournalismusbüro Open Data City und »Zeit Online«: Spitz ließ sich freiwillig aushorchen, er stellte die Metadaten seines Mobiltelefons den Datenjournalisten zur Verfügung. Heraus kam ein ziemlich perfektes Persönlichkeits- und Bewegungsprofil – ohne dass die

Datenspione den Inhalt von SMS, E-Mails oder Messengerchats überhaupt anschauen mussten. Im Fall von Spitz wussten alle Beteiligten über die Abhöraktion Bescheid. Unangenehm wird es, wenn jemand die übertragenen Informationen mitschneidet, ohne dass es die Ausspionierten überhaupt mitbekommen. So einen Angriff nennt man eine Man-in-the-middle attack.

Was ist eine Man-in-the-middle attack?

Dieser Angriff nutzt die zentrale Schwachstelle moderner Verschlüsselung aus: Die Nutzer, die miteinander kommunizieren, müssen sicher sein, dass der ihnen übertragene Schlüssel auch zur entsprechenden Kontaktperson gehört. Im Internetzeitalter trifft man sich aber meist nicht persönlich. Der Schlüssel wird mit der Nachricht mitgeschickt. Unterwegs ist er dabei angreifbar. Hacker fangen für so einen Angriff Schlüssel und Nachricht ab und tauschen den öffentlichen Schlüssel gegen ihren eigenen aus, um das Paket dann weiter an den Empfänger zu schicken. Äußerlich sieht man der Nachricht nicht an, dass sie manipuliert wurde, schließlich kommt sie vom richtigen Absender. Der Empfänger antwortet und verschlüsselt die Daten mit dem Schlüssel, der ihm geschickt wurde. Der »Mann in der Mitte« fängt wiederum beides ab, entschlüsselt mit seinem privaten Schlüssel und verschlüsselt mit dem öffentlichen Schlüssel des ursprünglichen Absenders (den er ja abgefangen hatte). Bei dem kommt eine korrekt verschlüsselte Nachricht an. Auf diese Art merken die beiden Kontaktparteien nicht einmal, dass sie ausgespäht werden.

Wer diese Gefahr umgehen will, muss sich auf anderem Weg treffen und die Schlüssel austauschen. Manche Messenger lösen das mittels eines QR-Codes, den man vom Smartphone des anderen einscannt und dann abgleicht. Darin ist der öffentliche Schlüssel kodiert. Oder es gibt eine elektronische Prüfsumme der Schlüssel in wenigen Zeichen, die man beispielsweise telefonisch vergleichen kann.

Wie hat das FBI das Terroristen-iPhone geknackt? Und sind iPhones nun sicher oder nicht?

Merkmal einer guten Verschlüsselung ist, dass der Anbieter selbst diese nicht knacken kann; und das kann Apple auch nicht. Was der Konzern allerdings nach dem Willen des FBI hätte tun sollen, ist, eine Sicherung außer Kraft zu setzen: Das iPhone des Attentäters war in diesem Fall verschlüsselt mit einem PIN-Kode. Durch so genannte »Brutforce-Attacken«, also das Ausprobieren verschiedener Passwörter, hätte die-

APPLE

TIM COOK, CEO VON APPLE

»Ist die Verschlüsselung auf dem neuesten Stand der Technik, ist sie nicht knackbar«

[Michael Backes]

ser möglicherweise geknackt werden können. iPhones besitzen dagegen zweierlei Sicherheitsmaßnahmen: Die Software verzögert einerseits die Zeit, mit der neue Passwörter getestet werden können, mit der zunehmenden Anzahl an Fehlversuchen. Andererseits können Nutzer einstellen, dass der Speicher nach zehn Fehlversuchen automatisch gelöscht wird. Ob der Attentäter diese Funktion aktiviert hatte, ist unbekannt. Die Gefahr, den Speicher zu löschen, hielt das FBI jedenfalls vom wilden Rumprobieren ab.

Apple weigerte sich nun, ein Programm für das FBI zu schreiben, das diese Maßnahme umgeht – aus gutem Grund: Apple-CEO Tim Cook schreibt in einem offenen Brief, das FBI habe »nach etwas gefragt, was wir schlicht nicht haben, und nach etwas, was wir zu gefährlich finden, um es zu entwickeln«. Die Sicherheit hätte sich dadurch für alle iPhone-Nutzer verschlechtert. Ein anderer Weg wäre gewesen, die Daten über das Backup in der iCloud zu bekommen. Dort sind sie zwar auch verschlüsselt, aber mit einem Schlüssel von Apple. Der Konzern hätte dem FBI also relativ einfach helfen können – wenn er gewollt hätte. Dieser Zustand betrifft übrigens auch alle anderen Apple-Kunden: Wer seine Daten in der iCloud speichert, hat weniger Sicherheit. Diese Option fiel im vorliegenden Fall aber weg, weil die Backup-Funktion des Attentäter-iPhones seit einigen Monaten nicht mehr benutzt worden war.

Nach aktuellen Informationen hat das FBI die Lösung nun für mehr als 1,3 Millionen Dollar von Hackern gekauft, die eine Sicherheitslücke im System des betreffenden iPhones 5c entdeckt hatten. Für neuere iPhones soll der Hack laut FBI hingegen nicht taugen. Man kann nur hoffen, dass sich Apple diese Informationen auch beschafft oder selbst gefunden hat, um die Lücke in zukünftigen Geräten geschlossen zu halten.

Wozu ist ein offener Quellcode gut?

Vielen Messengern fehlt im Test der Electronic Frontier Foundation der Punkt »Is the code open to independent review?«: Den Quellcode offenzulegen, gilt als zentrale Sicherheitsmaßnahme, da nur so Experten und gutwillige Hacker die Qualität der Verschlüsselung überprüfen können. Sie können nicht nur testen, ob wirklich keine Hintertür für Geheimdienste eingebaut ist, sondern auch nach anderen