

Was ist eigentlich...

... ein 128-Bit-Schlüssel?

Sensible Daten werden im Internet verschlüsselt übermittelt. Als Standard hat sich die 128-Bit-Verschlüsselung durchgesetzt, die ursprünglich für die Übermittlung von Kreditkarten-Informationen angewandt wurde. Dabei werden die zwischen Ihrem Computer und einem Server ausgetauschten Daten mit einem Schlüssel codiert (verschlüsselt) und decodiert (entschlüsselt): Die Zeichen werden vor dem Senden so vermischt, dass man sie nicht mehr lesen kann. Nur wer den richtigen Schlüssel besitzt, kann sie wieder in die richtige Reihenfolge bringen.

Grundsätzlich unterscheidet man zwischen symmetrischer und asymmetrischer Verschlüsselung. Bei der symmetrischen Verschlüsselung benutzt Ihr Computer denselben Schlüssel wie der Server. Damit beide Rechner die Daten verschlüsseln und entschlüsseln können, muss bei dieser Methode der Schlüssel übermittelt werden. Das ist ein Sicherheitsrisiko, weil der Schlüssel beim Verschicken in falsche Hände geraten könnte: Jede Person, die den Schlüssel hat, kann die Nachricht lesen. Deshalb wird im Internet für die sichere Datenübertragung eine asymmetrische Verschlüsselung verwendet.

Asymmetrisch werden Verschlüsselungssysteme genannt, bei denen für die Codierung ein anderer Schlüssel verwendet wird als für die Decodierung. Der erste Schlüssel wird öffentlicher Schlüssel genannt, da er für alle zugänglich ist, die an einen Server verschlüsselte Daten übermitteln wollen. Diese Daten können vom Empfänger der Daten (dem Server) nur dann gelesen werden, wenn er sie mit dem zweiten, privaten Schlüssel entschlüsselt.

Dies tönt alles ziemlich kompliziert, braucht Sie aber nicht zu kümmern. Ihr Internetprogramm (Browser) ist so eingerichtet, dass es bei Bedarf automatisch eine sichere (verschlüsselte) Verbindung aufbaut. Sie erkennen das an einem Symbol in Form eines Schlosses in der Statusleiste Ihres Browsers am unteren Bildschirmrand.



In der Praxis spielt sich die Übermittlung von Daten wie folgt ab: Ihr Computer meldet dem Server, dass er eine verschlüsselte Verbindung aufbauen möchte. Dies geschieht automatisch, wenn Sie eine gesicherte Webseite aufrufen. Der Server schickt als Antwort quasi ein Schnappschloss (den «öffentlichen Schlüssel») zurück. Nur der Server hat einen Schlüssel für dieses Schloss. Es ist durch ein Zertifikat geschützt, das seine Echtheit bestätigt. Nun generiert Ihr Browser ebenfalls ein eigenes Schnappschloss, für das wiederum nur er selbst einen Schlüssel hat, und übermittelt es an den Server. Jetzt kann der Datentransfer beginnen. Die Dokumente werden mit dem Schnappschloss gesichert verschickt, und nur der Empfänger besitzt den passenden Schlüssel. Im Internet werden nur die Schlösser verschickt, nie aber die passenden Schlüssel. Daher ist die asymmetrische Verschlüsselung so sicher.

Die Zahl 128 bezeichnet die Länge des Schlüssels. Bei einer 128-Bit-Verschlüsselung ist der Schlüssel also 128 Zeichen lang. Grundsätzlich gilt: Je länger ein Schlüssel ist, desto schwieriger ist es, ihn zu knacken. 128-Bit-Schlüssel gelten zwar heute nicht mehr als unknackbar, aber der Zeitaufwand dafür ist zu gross, als dass man sich fürchten müsste. **(rue)**

Impressum



Die Schweizer PC-Zeitschrift

Verlag IDG Communications AG
Witikonstr. 15, PF 253, 8030 Zürich, Tel. 01 387 44 44
Gesamtleitung IDG Gebhard Osterwalder
Redaktion Tel. 01 387 44 44, Fax 01 387 45 84, Postadresse wie Verlag
E-Mail redaktion@pctip.ch, Internet <http://www.pctip.ch/>
E-Mail für Pressemitteilungen: pr@pctip.ch
E-Mail für Free-/Shareware-Vorschläge: downloads@pctip.ch
Pctip-Kummerkasten: <http://www.pctip.ch/helpdesk/kummerkasten/anfrage.asp> (Telefonische Anfragen können nicht bearbeitet werden.)
Sonja Wunsch (sw), Chefredaktion
Hansjörg Honegger (hh), Produktion • Christian Bütikofer (chb),
Beat Rüdt (rue), Gaby Salvisberg (sal), Sascha Zäch (sz), Redaktion •
Anne Kittel (ki), Assistenz/Abschluss • Balbina Hossmann (bh), Assistenz
Ständige freie Mitarbeit Bruno Habegger (bha), Markus Zitt (z),
Nelly Bach (abschluss), Heinz Zollinger (abschluss)
Beiträge aus IDG-Schwesterpublikationen sind mit (idg) gezeichnet.
Pctip-Kummerkasten Bruno Amsler (ba), Marci Castro (mc),
Ruth Gogoll (rgl), Monica Hubacher (mo), Martin Huber (mhu),
Antje Küchler (ak), Martin Schwieder (mas), Simon Wepfer (swe)
Layout/Gestaltung Daniel Brühlmann, Hans-Jakob Rickli
Druck St. Galler Tagblatt AG, 9001 St. Gallen
Druckauflage: 74 800 Exemplare
Auf chlorfrei gebleichtem Papier gedruckt.
Leserschaft 271 000 Leser (MACH Basic 2002)
Verkaufte Auflage 56 074 (Jahr 2001 gemäss WEMF 2002)
Vertrieb & Marketing Jacqueline Ort, E-Mail jacqueline.ort@idg.ch
Bestellung Abo/bis zu 2 Jahre alte Ausgaben, Adressänderung
Pctip-Aboservice, PF 9001 St. Gallen, Tel. 071 272 71 90, Fax 071 272 73 84
E-Mail abo@pctip.ch, Internet <http://www.pctip.ch/abo/>
Bezugspreise Pctip erscheint monatlich (plus ein Sonderheft zur
Orbit/Comdex), die nächste Ausgabe am 28.1.2003.
Einzelausgabe Kiosk Fr. 3.80, Jahresabo Fr. 38.-
Anzeigen Schweiz Tel. 01 387 44 44, Fax 01 387 45 83
E-Mail anzeigen@pctip.ch und banner@pctip.ch
Kurt Strebel, Gesamtleitung Anzeigen IDG • Rolf Fischer, Lokaler Verkauf
Urs Flückiger, Internationaler Verkauf/Online • Esther Majolet, Marktplatz
Natalie Rickli, Disposition • Nina Osterwalder, Assistenz
Anzeigen Deutschland Tina Ölschläger, IMS München
Tel. 0049 89 360 86 116, Fax 0049 89 360 86 263
Es gilt der Anzeigentarif 2003.

© 2002 IDG Communications AG, Zürich. ISSN 1422-4704

Alle Rechte vorbehalten. Die Urheberrechte für angenommene und veröffentlichte Manuskripte und Abbildungen liegen bei der IDG Communications AG. Nachdruck, Verbreitung und elektr. Wiedergabe, auch auszugsweise, nur mit schriftlicher Genehmigung des Verlages. Dies gilt auch für in elektronischer Form vertriebene Beiträge sowie für Beiträge auf <http://www.pctip.ch/>. Die ganze oder teilweise Verwertung von Inseraten (inkl. Einpreisung in Online-Dienste) durch unberechtigte Dritte ist untersagt. Alle Beiträge werden mit grösster Sorgfalt erstellt. Trotzdem können wir keine Haftung für deren Richtigkeit übernehmen. Insbesondere übernehmen wir keine Haftung für Kaufempfehlungen oder für Schäden, die beim Ausprobieren der Bauanleitungen oder Tipps u. a. passieren. Ebenfalls keine Haftung wird übernommen für unverlangt eingesandte Manuskripte, Soft-/Hardware, CD-ROMs, Floppys, Fotos, Dias etc. Eine Rücksendegarantie geben wir nicht. Wir behalten uns das Recht vor, eingesandte Beiträge auf anderen Medien etwa auf CD-ROMs, in Sonderheften oder im Online-Verfahren herauszugeben.

ILLUSTRATION: CHRISTOPH NIEMAN

Privatsphäre: So verschlüsseln Sie Ihre E-Mails
Alleskönner: Multifunktions-Geräte im Test
Datensicherheit: Backup Schritt für Schritt erklärt
Dialer: Die fiesesten Tricks der Einwählprogramme
Online-Auktionen: Schnäppchenjagd – aber richtig

Nachzulesen im nächsten PCtip vom Februar 2003. Themen können aus aktuellem Anlass ändern.



Der nächste PCtip 2/2003 erscheint am Dienstag, 28. Januar 2003.