Verschlüsselungsverfahren

Verschlüsselungen sind kryptographische Verfahren, die dafür sorgen sollen, dass nur die vorgesehenen Empfänger einer Nachricht diese verstehen können.

Symmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung, auch konventionelle Verschlüsselung genannt, wird die Nachricht durch ein bestimmtes Verfahren so verändert, dass sie nur durch erneute Anwendung des gleichen Verfahrens lesbar gemacht werden kann. Sender und Empfänger müssen im Besitz des gleichen Schlüssels sein. Das Verfahren ist so sicher, wie dieser Schlüssel vor Unbefugten geheim gehalten werden kann. Zudem erhöht sich die Sicherheit mit steigender Schlüssellänge (in Bit), da der Aufwand einer Brute -Force-Attacke (alle Kombinationen durchprobieren) von der Schlüssellänge abhängt. Ein Sicherheitsrisiko ist jedoch bereits, dass der Schlüssel zunächst zwischen den Kommunikationspartnern ausgetauscht werden muss. Ein weiterer Nachteil symmetrischer Verschlüsselungsverfahren besteht darin, dass sehr viele Schlüssel benötigt werden, wenn in einer größeren Gruppe Nachrichten ausgetauscht werden, jedoch nicht jede Nachricht von jedem Teilnehmer lesbar sein soll. (Animation zur symmetrischen Verschlüsselung)

Asymmetrische Verschlüsselung

Bei der asymmetrischen Verschlüsselung wird grundsätzlich mit einem Schlüsselpaar gearbeitet, einem privaten Schlüssel (Private Key) und einem öffentlichem Schlüssel (Public Key). Daher wird diese Form der Verschlüsselung auch oft als Public-Key-Verschlüsselung bezeichnet. Beide Schlüssel ergänzen sich: der öffentliche verschlüsselt, der private entschlüsselt die Nachricht. Entscheidend bei diesem Verfahren ist, dass aus Kenntnis des öffentlichen Schlüssels der jeweilige private Schlüssel nicht ableitbar ist. Aus diesem Grund kann ein Schlüssel öffentlich zugänglich gemacht werden, mit dem jeder eine Nachricht verschlüsseln kann. Zum Entschlüsseln ist dann ein geheimer, der private Schlüssel, notwendig. Nur der Besitzer dieses geheimen Schlüssels ist in der Lage, die mit dem öffentlichen Schlüssel verschlüsselte Nachricht wieder zu entschlüsseln. (Animation zur asymmetrischen Verschlüsselung)

Hybride Verschlüsselung

Da asymmetrische Verschlüsselungsverfahren aufgrund des hohen Rechenaufwands sehr langsam sind, werden sie häufig dazu benutzt, die Sicherheit der symmetrischen Verfahren zu erhöhen, indem der Austausch der Schlüssel über ein asymmetrisches Verfahren abgewickelt wird. Der Austausch der eigentlichen Nachricht erfolgt dann über die symmetrische, schnellere Verschlüsselung.

Zertifizierung und Digitale Signatur

Zentral für die Anwendung asymmetrischer Verschlüsselungsverfahren ist, dass die jeweils einmaligen Schlüsselpaare (privater und öffentlicher Schlüssel) natürlichen Personen fest zugeordnet werden. Dies geschieht durch öffentliche Dienstleister, sogenannte Zertifizierungsstellen. Diese stellen Zertifikate aus, in denen einer Person ein öffentlicher Schlüssel eindeutig zugeordnet wird. Das Zertifikat erhält seine Vertrauenswürdigkeit durch die Signatur der Zertifizierungsstelle: Diese verschlüsselt das Zertifikat dazu mit ihrem privaten Schlüssel. Indem das Zertifikat nur durch den öffentlichen Schlüssel der Zertifizierungsstelle lesbar wird, kann der Empfänger überprüfen, dass das Zertifikat tatsächlich von dieser Stelle stammt und damit ist die Zuordnung vertrauenswürdig – vorausgesetzt, die Zertifizierungsstelle genießt entsprechendes Vertrauen. Eine Alternative zu einer solchen so genannten Public Key Infrastructure (PKI) stellt ein Web of Trust dar, in dem die Teilnehmenden die Funktion der Zertifizierung übernehmen. Bei beiden Zertifizierungsformen kann durch bestimmte mathematische Verfahren überprüft werden, ob die

Nachricht unbemerkt manipuliert wurde. Das Gesamtverfahren wird auch als Digitale Signatur bezeichnet.

SSL (Secure Socket Layer)

Bei der Übertragung personengebundener Daten im Internet, z. B. beim Online-Banking oder –Shopping, wird häufig das von der Firma Netscape entwickelte Verschlüsselungsverfahren SSL angewendet. Dabei wird nicht die eigentliche Nachricht, sondern das Übertragungsprotokoll (z. B. http, ftp) verschlüsselt. Eine SSL-Verbindung kann am ersten Teil der URL erkannt werden, die sich von http:// in https:// ändert.

PGP (Pretty Good Privacy)

Das Programm PGP arbeitet mit einem als sehr sicher geltenden hybriden Verschlüsselungsverfahren. Es ist insbesondere für die Verschlüsselung von E-Mails weit verbreitet und für alle gängigen Betriebssysteme erhältlich. PGP gibt es in einer kommerziellen, für Privatanwender jedoch kostenlosen Variante (www.pgp.com) sowie als Open Source -Angebot (www.gnupg.org). Eine Anleitung zur Installation von PGP finden Sie auf den Seiten des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein.

Letzte Änderung: 13.07.2015

Zitation

e-teaching.org (2015). Verschlüsselungsverfahren. Zuletzt geändert am 13.07.2015. Leibniz-Institut für Wissensmedien: https://www.e-teaching.org/technik/datenhaltung/datenschutz/verschluesselung/index_html. Zugriff am 18.01.2019