Wie funktioniert die Datenverschlüsselung?

Die Verschlüsselung von Daten, auch als Kryptografie bezeichnet, spielt im Zeitalter der Informationstechnologie eine wichtige Rolle. Gerade in vielen Internetanwendungen werden kryptografische Verfahren für die Sicherheit der Daten eingesetzt. Unser Autor und IT-Experte Thomas Burgard gibt einen fundierten Einstieg.

Einführung

Die Verschlüsselung von Daten wird in der Geschichte der Menschheit schon lange angewendet. Geheime und nicht lesbare Texte waren oft entscheidend z.B. für einen Sieg über den Feind. Bis heute hat sich da nicht viel geändert. Was bedeutet nun Verschlüsselung von Daten genau?
Die Verschlüsselung von Daten verändern lesbare Zeichen (Text), Ton oder Bilder in der Art, dass die Zeichen durch ein Verschlüsselungsverfahren, auch **„Kryptosystem“** genannt, in eine nicht lesbare (geheime) Zeichenfolge umgewandelt wird. Als Basis der Verschlüsselung wird ein sogenannter **„Schlüssel“** verwendet.
Definition: **Die Kryptografie ist die Wissenschaft der Informationsverschlüsselung** und ist eine **Teilmenge der Kryptologie**.
Das Ziel der Kryptografie ist nicht nur eine Verschlüsselung der Informationen, sondern auch die Informationen so zu bearbeiten, dass diese vor dem Zugriff von Unbefugten geschützt und nur vom Absender und dem befugten Empfänger zugänglich gemacht wird.
Bereits in der Antike (im 5. Jahrhundert v. Chr.) wendeten die Spartaner kryptografische Verfahren für den militärischen Einsatz erfolgreich an. **„Ein Stab aus Holz wurde mit einem Streifen Papyrus so umwickelt“**, dass ein Text auf den Stab geschrieben werden konnte. Zog man den Papyrusstreifen vom Holzstab wieder ab, war lediglich nur eine unlesbare Zeichenfolge sichtbar. Um die geheime Information wieder lesbar zu machen, also zu entschlüsseln, war ein Stab mit denselben Abmessungen und das Wissen um die Technik des Aufwickelns des Papyrusstreifens notwendig.
Ein anderes von Julius Caesar für die Militärkorrespondenz angewendetes und aus heutiger Sicht ein recht simples Verschlüsselungsverfahren hat jeden Buchstaben im Alphabet um eine bestimmte Anzahl linear verschoben, dass ein Buchstabe durch jeweils einen anderen Buchstaben im Alphabet ersetzt wurde. Diese simple Art von Verschlüsselung ist auch als **„Caesar-Code“** bekannt. Der Schlüssel ist hierbei die Anzahl der Stellen, um die die Buchstaben verschoben werden. Für die Entschlüsselung der geheimen Nachricht werden natürlich nur 26 Versuche benötigt.
Im Laufe der Zeit wurden viele verschiedene kryptografische Verfahren entwickelt, die allerdings früher oder später alle geknackt wurden. Erst durch die moderne Mathematik und die Computertechnologie ist es möglich, für die heutigen Anwendungen, leistungsfähige und sichere Verschlüsselungsverfahren zu entwickeln, die nur äußerst schwer (der Aufwand ist extrem hoch) oder gar nicht mehr zu entschlüsseln sind. Das Entscheidende bei den neuen Verfahren ist die **Länge des Schlüssels**. Es nutzt ja wenig, wenn die Gesamtheit der möglichen Schlüssel in relativ kurzer Zeit durch Ausprobieren geknackt wird. Der Schlüssel muss also eine ausreichende Länge besitzen.
Im Zeitalter des Internets, in dem die Menschen und Unternehmen im Internet immer mehr vertrauliche Nachrichten (z.B. E-Mails) versenden oder Geldtransaktionen tätigen, ist die Sicherheit und damit auch die Verschlüsselungsverfahren zu einem ganz zentralen Thema, wenn nicht sogar zum wichtigsten Thema im Umgang mit Computern und Netzwerken geworden.
Für eine vertrauensvolle Kommunikation zwischen Absender und Empfänger werden grundlegende Anforderungen gestellt:

- *Authentizität*: Es muss sichergestellt sein, dass eine Nachricht auch tatsächlich vom richtigen Absender stammt.
- *Autorisation:* Es muss sichergestellt sein, dass nur der richtige Empfänger die Berechtigung hat, die Nachricht zu lesen.
- *Vertraulichkeit:* Es muss sichergestellt sein, dass eine Nachricht nur von der Person gelesen werden kann, für die auch die Nachricht vom Absender bestimmt ist.
- *Datenintegrität:* Es muss sichergestellt sein, dass eine Nachricht während dem Nachrichtentransport auf dem Übertragungsweg nicht verändert wird und im Originalzustand beim Empfänger ankommt.

Verschlüsselungsverfahren

Die Verschlüsselungsverfahren werden in sogenannte symmetrische und asymmetrische Verschlüsselungsverfahren eingeteilt.

Symmetrische Schlüsselverfahren

Bei den symmetrischen Verschlüsselungsverfahren, die auch als **„Private-Key-Verfahren“** bezeichnet werden, wird für die Verschlüsselung der Daten der **gleiche Schlüssel** verwendet, der zwischen Absender und Empfänger auf einem sicheren Weg ausgetauscht werden muss. Die Sicherheit dieses Verschlüsselungsverfahren hängt ganz klar von der Geheimhaltung des gemeinsamen ab.
Das symmetrische Verschlüsselungsverfahren **„One-Time-Pad“** ist das einzige Verfahren, das nachweislich nicht zu knacken ist. Hierbei werden für jeden Buchstaben eines Textes eine zufällige erzeugte Anzahl von Buchstaben zur Verschlüsselung verwendet.
Die symmetrischen Verschlüsselungsverfahren lassen sich in zwei Klassen einteilen:

- *Blockalgorithmen:* Hierbei werden ganze Datenblöcke gleichzeitig verschlüsselt.
- *Bitstromverschlüsselungsverfahren:* Hierbei wird der Text Bit für Bit verschlüsselt.

Am häufigsten werden folgende symmetrische Verschlüsselungsverfahren eingesetzt:

- *DES (Data Encryption Standard):* DES wurde von ANSI (American National Standards Institute) 1981 standardisiert und findet nach wie vor in vielen Verschlüsselungssystemen Einsatz. DES verwendet den Blockalgorithmus, der 64 offenen Text in 64-Bit verschlüsselten Text umwandelt. Der Schlüssel hat eine Länge von 56 Bit.

Einstufung der Sicherheit:
Nicht sonderlich hoch, da die Schlüssellänge nicht ausreichend ist. Mit 56 Bit kann ein Schlüsselraum von max. 2^{56} Schlüsseln erzeugt werden.

- *Triple-DES:* Bei Triple-DES werden zwei Schlüssel mit jeweils 56 Bit verwendet. Es werden insgesamt drei DES Verschlüsselungen durchgeführt, bei denen dann nacheinander die zwei Schlüssel verwendet werden. Die Anzahl der max. möglichen Schlüssel liegt demnach bei 2^{112}.

Einstufung der Sicherheit:
Deutlich sicherer als beim DES. Dieses Verfahren wird sehr oft bei Finanztransaktionen verwendet.

- *IDEA (International Data Encryption Algorithmus):* IDEA basiert auf dem Blockalgorithmus und arbeitet mit einer Blocklänge von 64 Bit und einer Schlüssellänge von 128 Bit. Es können also 2^{128} Schlüssel erzeugt werden.

Einstufung der Sicherheit:
Durch seine große Schlüsselmenge ist dieses Verfahren relativ sicher.

Vorteil:
- Nur ein Schlüssel für beide Kommunikationspartner.

Nachteile:
- Der Austausch der Schlüssel ist unsicher, denn ein unbefugter Dritter könnte den Austausch ausspionieren.
- Die Verschlüsselung ist leicht zu brechen (siehe Abb. 1).

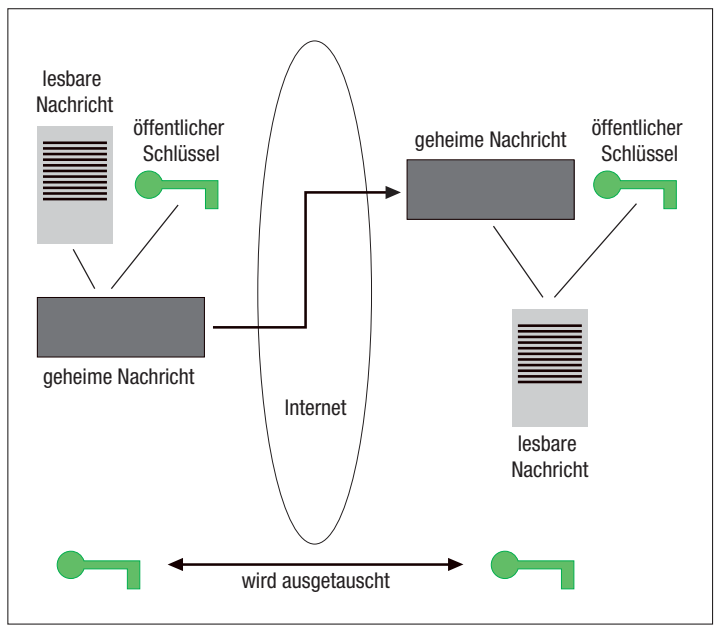

Abb. 1: Die symmetrische Verschlüsselung.

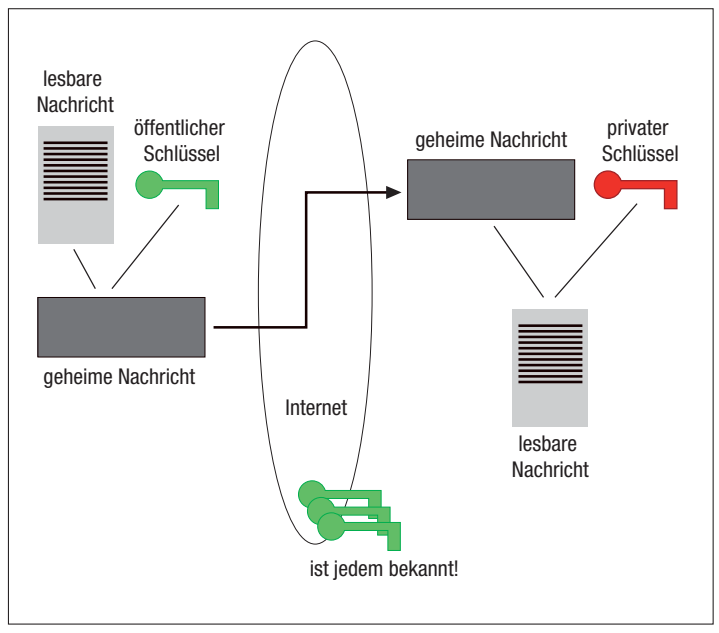

Abb. 2: Die asymmetrische Verschlüsselung.

Asymmetrische Schlüsselverfahren

Bei den asymmetrischen Verschlüsselungsverfahren, die auch als **„Public-Key-Verfahren“** bezeichnet werden, werden **zwei ungleiche Schlüssel** verwendet. Mathematisch gesehen, besteht zwischen beiden Schlüssel eine Abhängigkeit, jedoch kann ein Schlüssel vom anderen nicht hergeleitet werden, auch wenn man den anderen Schlüssel kennt. Sogenannte **„Einwegfunktionen“** machen dieses Verhalten möglich. Eine sogenannte „Umkehrfunktion“ kann demnach aus einer Einwegfunktion nicht berechnet werden.
Die Funktionsweise ist folgende: Anwender A möchte eine verschlüsselte Nachricht zu Anwender B senden. Zuerst generiert A zwei Schlüssel, von denen einer öffentlich und der andere geheim ist. Die geheime Nachricht von A wird dann mit dem öffentlichen Schlüssel (public key) verschlüsselt. Die Nachricht kommt absolut sicher bei B an, da ja für die Entschlüsselung der geheime Schlüssel (private key) benötigt wird. Nur B kann die Nachricht mit dem geheimen Schlüssel entschlüsseln, da nur er in Besitz des geheimen Schlüssels ist. Die asymmetrische Verschlüsselung wird zur Verschlüsselung, Authentifizierung und Sicherung der Integrität eingesetzt, z.B beim E-Mail-Verkehr.
Am häufigsten werden folgende asymmetrische Verschlüsselungsverfahren eingesetzt:

- *RSA (Rivest, Shamir und Adleman):* Die Namen der Entwickler Rivest, Shamir und Adleman gaben diesem Verfahren seinen Namen. Dieses Verschlüsselungsverfahren ist im Internet ein Quasistandard und basiert auf die Zerlegung einer großen Zahl in ihre Primzahlen. Entscheidend für die Sicherheit von RSA ist die Auswahl geeigneter Primzahlen.
- *DSS (Digital Signature Standard):* Dieses Verfahren wurde vom NIST (National Institute for Standards and Technology) bei der ISO () eingereicht und basiert auf dem „EIGamal-Verfahren“ (wie RSA nur Verwendung von diskreten Logarithmen statt der Primzahlenzerlegung). DSS wird für „Digitale Signaturen“ verwendet und die Schlüssel können eine Länge von 512 bis 1.024 Bit haben.

Vorteil:
- Die Verschlüsselung ist sehr sicher, da ein zweiter geheimer Schlüssel für die Entschlüsselung notwendig ist. Voraussetzung ist natürlich ein absolut sicherer Austausch (am besten persönlich) der öffentlichen Schlüssel unter den Kommunikationspartnern.

Nachteil:
- Durch die zwei Schlüssel ist das Verfahren sehr aufwendig (siehe Abb. 2).

Kryptografische Prüfsummen (Message Digest)

Durch die Verschlüsselung einer Nachricht wird ja die Vertraulichkeit einer Kommunikationsnachricht erreicht. Zusätzlich muss aber auch eine unverfälschte Übertragung der Nachricht gegeben sein. Dies wird durch sogenannte **„One-Way-Hashfunktionen“** erreicht, die zudem auch große Datenmengen beherrschen. Hashfunktionen sind mathematische Funktionen, die jeder beliebigen Nachricht eine „kryptografische Prüfsumme“ von 128 Bit oder 160 Bit Länge zuordnet.
Folgende Verfahren für die Erzeugung von kryptografischen Prüfsummen finden im Internet Verwendung:

- *MD2:* „Message Digest Nr. 2“ ist das älteste Verfahren und erzeugt eine kryptografische Prüfsumme von 128 Bit Länge.
- *MD4:* Ein weiterer Algorithmus mit ebenfalls 128 Bit Prüfsumme.
- *MD5:* Eine Weiterentwicklung des MD4-Algorithmus mit ebenfalls 128 Bit Prüfsumme.
- *SHA-1:* Der SHA-1 (Secure Hash Algorithmus) ist ein Algorithmus mit einer 160 Bit langen Prüfsumme und gilt als sehr sicher.

Digitales Zertifikat und digitale Signatur

Digitales Zertifikat
Um sicherzustellen, dass der öffentliche Schlüssel auch zum wahren Empfänger gehört und der öffentliche Schlüssel auch mit diesem Verschlüsselungsverfahren und dem entsprechenden Anwendungsbereich verwendet werden darf, muss ein Nachweis dies bestätigen. Genau diesen Nachweis nennt man „digitales Zertifikat“.

Digitale Signatur
Eine digitale Signatur basiert auf dem asymmetrischen Verschlüsselungsverfahren und stellt einen Zahlenwert dar, mit dem die Integrität der Daten ermittelt und eine eventuelle Veränderung der Daten aufgedeckt werden kann. Man kann auch sagen, dass die digitale Signatur eine digitale Unterschrift ist.

PKI
PKI steht für **„Public-Key-Infrastruktur“** und ist ein System, das digitale Zertifikate (digital signierte öffentliche Schlüssel) ausstellt, prüft und verteilen kann und darf. ZT

ZT Adresse

Thomas Burgard Softwareentwicklung & Webdesign
Dipl.-Ing. (FH) Thomas Burgard
Bavariastr. 18b
80336 München
Tel.: 0 89/54 07 07-10
E-Mail: info@burgardsoft.de
www.burgardsoft.de
burgardsoft.blogspot.com
twitter.com/burgardsoft