Verschlüsselung – heute notwendiger denn je

Die Kryptologie ist die Wissenschaft der Verschlüsselung und der Entschlüsselung von Informationen. Ein Überblick.

VON ANDREAS WISLER

Die Kryptologie lässt sich wie folgt in drei Grundvarianten unterteilen:

► Kryptografie: Verschlüsselung von Informationen

► Kryptoanalyse: Entschlüsselung von Informationen (ohne Kenntnis des Schlüssels)

► Steganografie: Verstecken von Informationen

Nachdem die Kryptologie früher fast ausschliesslich für das Militär eine Rolle spielte, findet sie heute immer mehr Zugang in zivilen Bereichen. Besonders im Internet ist die sichere Übertragung von Informationen (z.B. Passwörtern oder Kreditkartennummern) unerlässlich geworden.

Viele Regierungen wollen Verschlüsselung verbieten oder ineffektiv machen. Sie befürchten, Kriminelle oder Regierungskritiker könnten auf diese Weise kommunizieren, ohne dass dies von ihnen kontrolliert werden kann. Gegner dieser Massnahmen kritisieren jedoch die damit einhergehende Einschränkung des Grundrechts auf die Vertraulichkeit und die damit verbundene Überwachung des Bürgers.

Angriffsarten und Bedrohungen

Die Informationen präsentieren sich in der heutigen Zeit immer mehr in digitaler Form. Angreifer können unterschiedliche Attacken gegen digitale Informationen ausführen. Die Angriffsmethoden oder Bedrohungen werden in folgende Klassen unterteilt:

► **Abhören** von Nachrichten oder Einsicht in Nachrichten. Personen nehmen Einblick in Informationen oder Nachrichten, obwohl dies vom Verfasser der Nachricht oder der Information unerwünscht oder ungewollt ist.

► **Löschen** von Nachrichten oder Teilen davon. Informationen, welche aufbewahrt oder gesandt werden sollen, werden vom Verfasser der Nachricht ungewollt oder von einem unberechtigten Dritten vorsätzlich gelöscht.

► **Verändern** von Nachrichten. Hier wird eine Nachricht so weit verändert, dass der Sinn oder Zweck der ursprünglichen Nachricht nicht mehr mit der veränderten übereinstimmt.

► **Bestreiten des Versands** von Nachrichten (Non Repudiation of origin). Hier wird vom Absender einer Nachricht bestritten, die Nachricht versandt zu haben.

► **Bestreiten des Empfangs** von Nachrichten (Non Repudiation of receipt). Hier wird vom Empfänger einer Nach-

richt bestritten, die Nachricht erhalten zu haben.

► **Einspeisen** von Nachrichten. Hier werden von einer Person Nachrichten in die Kommunikation zweier oder mehrerer Teilnehmer eingefügt, was von diesen Teilnehmern nicht erwünscht oder gewollt ist.

► **Wiederholen** von Nachrichten. Bei diesem Angriff werden von einer Person bereits versandte Nachrichten noch einmal in die Kommunikation eingespiesen. Doch dies ist bei den Kommunikationsteilnehmern unerwünscht.

► **Vortäuschen** einer anderen Identität (Masquerade). Eine Person gibt sich als eine andere Person aus, um eine andere Person in die Irre zu führen.

Verschlüsselung: Einleitung und Begriffe

Ein lesbarer Text P wird mit dem Schlüssel K (Key) und der Funktion Ek(P) (E = Encryption) in einen verschlüsselten Text C (Ciphertext) umgewandelt. Die Umkehrfunktion entschlüsselt mit dem identischen Schlüssel K den Ciphertext mit der Funktion Dk(C) (D = Decryption) wieder in den lesbaren Text P.

Wesentliches Merkmal der symmetrischen Verschlüsselung ist also, dass sowohl für die Verschlüsselung wie die Entschlüsselung derselbe Schlüssel K verwendet wird.

Geschichte

Der früheste Einsatz von Kryptografie findet sich bei dem Einsetzen von unüblichen Hieroglyphen bei den Ägyptern um 1900 v. Chr. Hebräische Gelehrte verwendeten ungefähr 600 bis 500 a.D. einfache Zeichenaustauschalgorithmen (wie beispielsweise die Atbash-Verschlüsselung).

Die Spartaner wickelten einen Papierstreifen auf einen Stab und beschrifteten den Papierstreifen mit einer Nachricht. Die Empfänger des Papierstreifens konnten die Nachricht nur lesen, falls sie einen gleich dicken Stab verwendeten.

Cäsar verschlüsselte seine Nachrichten, indem er das Alphabet um ein paar Stellen verschob. So wurde z.B. ein A zu einem C, ein B zu einem D usw. (Cäsar-Chiffre). Im Mittelalter waren in ganz Europa vielfältige Geheimschriften zum Schutz des diplomatischen Briefverkehrs in Gebrauch, so etwa das Alphabetum Kaldeorum.

Im Zweiten Weltkrieg wurden mechanische und elektromechanische Kryptografiesysteme zahlreich eingesetzt. In dieser Zeit wurden grosse Fortschritte in der mathematischen Kryptografie gemacht. Notwendigerweise geschah dies jedoch nur im Geheimen. Die Deutschen machten regen Gebrauch von einem als Enigma bekannten System.

In den Jahren 1974 bis 1976 wurden der DES Algorithmus und die Public Key Kryptographie von W. Diffie und M. Hellman publiziert. Daraus resultierten 1976 das Diffie-Hellman-Verfahren, 1978 RSA und 1985 die Elliptischen Kurven. Es folgten danach 1990 IDEA (Xuejia Lai und James Massey an der ETHZ) und 2000 AES (Advanced Encryption Standard), der Nachfolger von DES.

XOR-Transformation

Eine der wichtigsten Transformationen ist die XOR-Funktion (von engl. eXclusive OR – exklusives Oder, entweder oder). Sie ergibt genau dann logisch «1», wenn an einer ungeraden Anzahl von Eingängen «1» anliegt und an den restlichen «0». Die folgende Wahrheitstabelle zeigt, wie die XOR-Transformation funktioniert:

Schlüssel	ASCII	Ergebnis aus XOR
1	1	0
1	0	1
0	1	1
0	0	0

Egal, welche Spalte fehlt, wenn zwei Spalten vorhanden sind, kann die Dritte immer errechnet werden. So sind beim Sender die Spalten «Schlüssel» und «ASCII» bekannt, beim Empfänger aber das «Ergebnis» und der zuvor definierte «Schlüssel».

Moderne Algorithmen wie AES, 3DES usw. arbeiten blockweise. Bei solchen Blockalgorithmen wird der Klartext zum Beispiel in Portionen zu 64 Bit aufgeteilt und aus jeder solchen Portion jeweils ein Geheimtext von 64 Bit Länge erzeugt.

Symmetrische Übertragung

Der grosse Nachteil symmetrischer Verfahren liegt in der Nutzung ein und desselben Schlüssels zur Ver- und Entschlüsselung. Ist der Schlüssel einem Angreifer bekannt, ist es für ihn leicht möglich, an Informationen zu gelangen und Fehlinformationen durch Veränderung der Originalnachricht zu verbreiten. Ein weiteres typisches Problem beim Einsatz von symmetrischen Verfahren ist, wie der Schlüssel erstmals über unsichere Kanäle zum Gegenüber übertragen werden kann.

Asymmetrische Übertragung

Bei der asymmetrischen Verschlüsselung wird für die Transformation der Information (Verschlüsselung) und die Rücktransformation je ein unterschiedlicher Schlüssel verwendet.

Authentisierwert-Methoden

Mit der Authentisierwert-Methode sollen die Integrität und die Authentizität von Daten geschützt werden. Die Authentisierwert-Methode basiert auf einer Prüfsumme. Es wird eine sogenannte Hashfunktion eingesetzt.

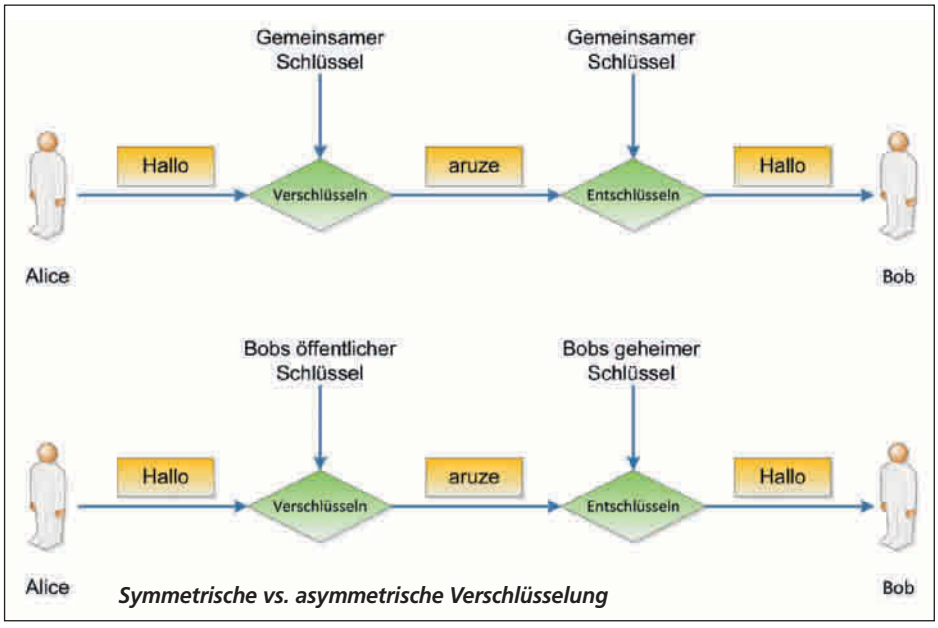
Ähnlich wie eine Komprimierungssoftware verkleinert eine Hashfunktion beliebig grosse Dokumente und Nachrichten. Eine Hashfunktion reduziert allerdings das Dokument auf eine so kleine Grösse, dass das Originaldokument nicht mehr aus dem durch die Hashfunktion resultierenden Informationswert hergestellt werden kann. Dieser Informationswert, d.h. das Ergebnis der Hashfunktion, wird Hashwert genannt.

Das Resultat der Hashfunktion, der Hashwert, ist also eine Art Prüfsumme. Wie bei einer Prüfsumme resultieren aus verschiedenen Texten unterschiedliche Werte. Die bekanntesten Verfahren sind MD5 und SHA1 (Hinweis: MD5 sollte heute nicht mehr verwendet werden).

Will man einen zu versendenden Text T vor Veränderung schützen, reicht es nicht aus, einen Hashwert H zu bilden und den an den Text T anzuhängen und dann T und H zu versenden. Denn ein aussenstehender Dritter vermag sowohl den Text T und H zu entfernen und durch einen Text T' und den dazu passenden Hashwert H' zu ersetzen. Daher wird der Hashwert zusätzlich verschlüsselt angehängt. Die Abbildung auf Seite 18 zeigt das Verfahren.

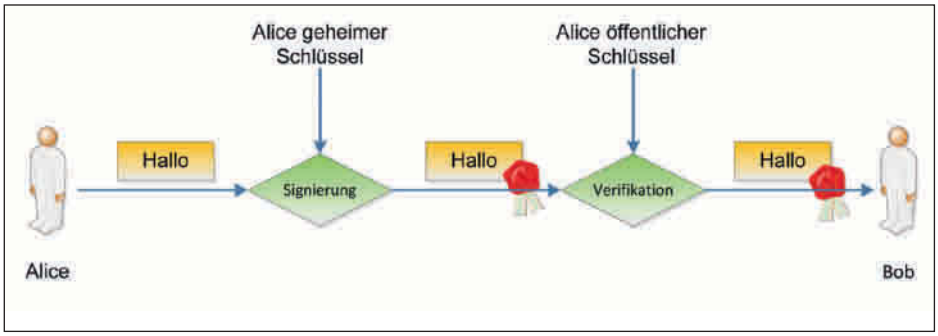
Kryptoanalyse

Grundsätzlich wird beim Design und vor allem beim Einsatz eines Chiffrierverfahrens davon ausgegangen, dass die Angrei-



Quelle: Andreas Wisler

Symmetrische vs. asymmetrische Verschlüsselung



Quelle: Andreas Wisler

Verschlüsselung mit Signatur

fer oder Hacker das eingesetzte Verfahren kennen. Man geht aber davon aus, dass sie den Schlüssel nicht kennen. Die Kryptoanalyse teilt die Angriffe auf den Schlüssel oder auf den Klartext.

► **Ciphertext Only** Manchmal wird diese Methode auch als Known Ciphertext bezeichnet. Der Angreifer kennt einen oder mehrere Geheimtexte und versucht mit deren Hilfe, auf den Klartext beziehungsweise den Schlüssel zu schliessen.

► **Known Plaintext** Der Angreifer besitzt Geheimtext(e) und den/die zugehörigen Klartext(e). Beide werden benutzt, um den Schlüssel zu ermitteln.

► **Adaptive Chosen Plaintext / Differential Cryptanalysis** Ähnlich dem vorhergehenden Angriff; der Angreifer hat längere Zeit Zugang zu einem Verschlüsselungssystem und kann sich immer wieder frei gewählte Klartexte verschlüsseln. Insbesondere kann er nach der Analyse des erhaltenen Kryptotextes je nach Ergebnis gezielt einen neuen Klartext zum Verschlüsseln wählen. –Differential Crypt -analysis.

► **Probable Plaintext** Der Angreifer besitzt Geheimtext und hat Grund zu der Annahme, dass dieser bestimmte Wortgruppen oder markante Wörter enthält, mit denen eine Analyse versucht werden kann.

Steganografie

Das Wort «Steganografie» kommt aus dem Griechischen und heisst übersetzt «verborgenes Schreiben». Sie wird oft definiert als «die Kunst und Wissenschaft der Kommunikation auf einem Weg, welcher die Existenz der Nachricht verbirgt». Somit ist Sinn und Zweck die «Vertuschung» von Informationen. Die Sicherheit einer geheimen steganografischen Botschaft liegt also darin, dass dem Angreifer die Existenz einer solchen nicht auffällt. Als Beispiel sei an dieser Stelle die computergestützte Steganografie (Quelle: Wikipedia) erwähnt: Mit der Entwicklung der Computer liessen sich diese Verfahren auch auf die elektronische Übermittlung von Daten anwenden. Neben den analogen Möglichkeiten einer linguistischen Steganografie entwickelten sich aber noch raffiniertere Verfahren, die für diejenigen, die keinen expliziten Verdacht auf eine versteckte Nachricht schöpfen, nahezu unbemerkbar sind.

Als Grundlage hierzu dient das sogenannte Datenrauschen. Hierbei handelt es sich um kein wirkliches Rauschen, sondern eher um eine unmerkliche Fehlertoleranz. Dementsprechend können gewisse Datenformen (Audiodateien und Bilder) leicht manipuliert und so Daten untergebracht werden, ohne dass das Gesamtbild bzw. der Ton sich verändert. Ideale Träger sind Musikdateien (z.B. WAV), wie auch Bilder (z.B. BMP).

Der Trick hierbei ist, dass bei jedem Byteblock das letzte Bit (auch LSB genannt => Least Significant Bit) nach Belieben manipuliert und die zu versteckende Datei so Bit für Bit in das Audioformat untergebracht werden kann. Das letzte Bit symbolisiert lediglich 2^0 – entscheidet also beispielsweise, ob eine Zahl 2^{30} oder 2^{31} lautet, und verändert so die originale Datei um maximal 1/256 (oder 0,39%). Das ist ein Unterschied, der in einer Audiodatei nicht hörbar ist.

Entsprechend der oben genannten Methode lassen sich bei reiner Nutzung des LSBs immer Dateien in der Trägerdatei unterbringen, die maximal 1/8 der Grösse haben, oder anders ausgedrückt, der Träger muss mindestens achtmal so gross sein.

Gesetzliche Vorschriften in der Schweiz

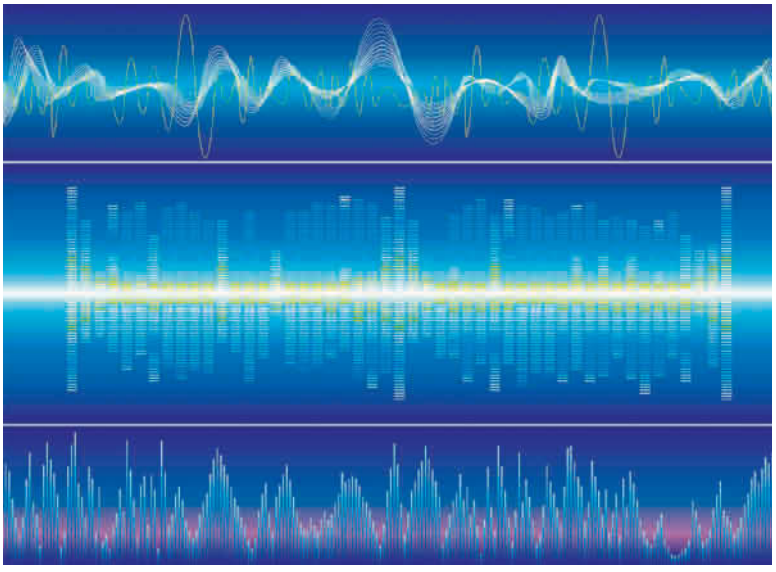
Seit 1. Januar 2005 werden elektronische Signaturen der handschriftlichen Unterschrift gleichgestellt. Der Bundesrat hat die ausführende Verordnung zum Bundesgesetz über die elektronische Signatur verabschiedet.

Das Parlament hat am 19. Dezember 2003 das Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (Bundesgesetz über die elektronische Signatur, ZertES) verabschiedet. Dieses definiert die Bedingungen, unter denen Anbieter von Zertifizierungsdiensten auf freiwilliger Basis anerkannt werden können, und regelt ihre Tätigkeiten im Bereich der elektronischen Zertifikate. Es legt zudem die Voraussetzungen fest, die eine elektronische Signatur erfüllen muss, um die gleichen Wirkungen wie eine handschriftliche Unterschrift erzielen zu können. Ausserdem regelt es die Frage der Verantwortung der Anbieterinnen von Zertifizierungsdiensten, der Anerkennungsstellen und der Inhaberinnen und Inhaber von Signaturschlüsseln.

Gleichzeitig hat der Bund die Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur (Verordnung über die elektronische Signatur, VZertES) verabschiedet. Sie konkretisiert insbesondere die Verpflichtungen, die anerkannten Anbieterinnen von Zertifizierungsdiensten auferlegt werden, und erteilt dem BAKOM den Auftrag, die nötigen technischen und administrativen Vorschriften zu erlassen. Die neuen gesetzlichen Bestimmungen sind mit der geltenden Regelung der Europäischen Union kompatibel.

Eine erste Anwendung ist die SuisseID, die den elektronischen Verkehr mit den Bundesstellen vereinfacht. Angeboten wird die SuisseID für Private von QuoVadis (in Zusammenarbeit mit der Trüb AG) und der Schweizerischen Post (SwissSign) und für Firmen zusätzlich von der Swisscom. ■

Der Autor: Andreas Wisler ist Dipl. Ing. FH, CISSP, ISO 27001 Lead Auditor und MCITP Enterprise Server Administrator. Er ist CEO der GO OUT Production GmbH.



Quelle: shutterstock

Audiodateien eignen sich hervorragend zum Verbergen von Informationen in Fremddateien ohne hörbaren Einfluss.