ZT IT-KOLUMNE

Kryptografie – Teil II

Im ersten Artikel ging es um den Einstieg in die Kryptografie. Im zweiten Teil geht es nun um die kryptografischen Verfahren, die überhaupt erst eine Verschlüsselung der Informationen und Daten ermöglichen.

Was ist ein Kryptosystem?

Bevor es dann richtig in die kryptografischen Verfahren geht, soll zuerst noch der Begriff „Kryptosystem" erklärt werden. Ein Kryptosystem ist ganz allgemein ein System, das eine Nachrichtenverschlüsselung mit einem beliebigen Verschlüsselungsverfahren ermöglicht.

Der Begriff der Verschlüsselung (Chiffrieren)

Die Verschlüsselung wandelt einen Klartext in Abhängigkeit von einer zusätzlichen Information, den sogenannten „Schlüssel", in einen zugehörigen Geheimtext, auch „Chiffrat" genannt, um. Derjenige, der den Schlüssel nicht kennt, kann die verschlüsselte Information nicht entziffern. Die Umkehrtransformation – die Zurückgewinnung des Klartexts aus dem Geheimtext – wird Entschlüsselung genannt. In den modernen Verschlüsselungsalgorithmen sind Klartexte, Geheimtexte und Schlüssel jeweils als Folgen von Bits gegeben. Um die Verschlüsselung in der Informationstechnologie auch anwendbar zu machen, müssen die Verschlüsselungsalgorithmen bestimmten Anforderungen genügen:

- Die mathematischen Verschlüsselungsalgorithmen müssen „entzifferungsresistent" sein, d. h. ohne Schlüssel darf die verschlüsselte Information nicht entschlüsselt werden können.
- Die Anzahl der möglichen Schlüssel muss so groß sein, dass ein simples Ausprobieren nicht möglich sein darf.
- Sie müssen einfach einsetzbar sein.
- Die Ver- und Entschlüsselung muss genügend schnell sein.

Wichtig zu wissen ist dabei, dass die „Entzifferungsresistenz" immer relativ zu den aktuellen technischen und mathematischen Möglichkeiten betrachtet werden muss.
Betrachten wir nun, dass eine Person A eine vertrauliche Nachricht an eine Person B versenden möchte. Hierfür wird dann folgendermaßen vorgegangen:

1. Beide Personen vereinbaren ein Chiffrierverfahren,

2. sie vereinbaren einen Schlüssel bzw. ein Schlüsselpaar,
3. A verschlüsselt eine Nachricht und sendet diese an B,
4. B entschlüsselt die von A gesendete verschlüsselte Information.

Aktuell werden zwei große Klassen von Chiffrierverfahren verwendet:

1. Symmetrische Verschlüsselungsverfahren
2. Asymmetrische Verschlüsselungsverfahren

Symmetrische Verschlüsselungsverfahren

Bei symmetrischen Verschlüsselungsverfahren gibt es nur einen einzigen Schlüssel. Dieser Schlüssel ist für die Verschlüsselung wie auch für die Entschlüsselung zuständig, d. h. zwei Kommunikationspartner (Sender und Empfänger) müssen denselben Schlüssel verwenden. Beim Sender ist das kein Problem, da er den Schlüssel schon zur Verschlüsselung hat, dem Empfänger fehlt aber natürlich der Schlüssel. Deswegen ist es bei der symmetrischen Verschlüsselung äußerst wichtig, dass der Schlüssel auf einem sicheren Übertragungsweg an den Empfänger übermittelt wird. Man kann sich nun leicht vorstellen, dass hier genau das Problem bei der symmetrischen Verschlüsselung liegt. Man musste deshalb früher den Schlüssel persönlich oder in Form eines Boten an den Kommunikationspartner übergeben. Wenn dann der Schlüssel in falsche Hände gelangt, kann die verschlüsselte Information von einem Fremden einfach entschlüsselt werden.

Da das persönliche Übergeben des Schlüssels sehr umständlich und bei weiten physikalischen Strecken undenkbar wäre, bedient man sich dem Prinzip der „asymmetrischen Verschlüsselung", dazu später mehr. Bei der symmetrischen Verschlüsselung werden wiederum zwei verschiedene Verfahren verwendet:

1. Verschlüsselungsverfahren mit Stromchiffren: Hierbei wird der Klartext Zeichen für Zeichen verschlüsselt, während bei der Entschlüsselung des Geheimtextes Zeichen für Zeichen entschlüsselt wird.
2. Verschlüsselungsverfahren mit Blockchiffren: Hierbei werden die Zeichen eines Textes in Blöcke fester Größe eingeteilt, sodass mehrere Zeichen in einem Schritt ver- bzw. entschlüsselt werden können.

Zu den einfachen symmetrischen Verschlüsselungsverfahren zählen die Varianten der „Monoalphabetischen Substitutionschiffren" wie z. B. die bekannte „Cäsar-Chiffre". Hierbei wird jeder Buchstabe um eine Zahl n verschoben. Die „Cäsar-Chiffre" kennt demnach nur 26 unterschiedliche Schlüssel und ist sehr einfach zu knacken. Anstatt einfach nur die Buchstaben zu verschieben, können diese auch durch andere Buchstaben ersetzt werden, also substituiert. Monoalphabetisch deshalb, weil immer nur ein bestimmter Buchstabe durch einen selben anderen ersetzt wird. Das Gegenteil ist die „Polyalphabetische Substitution". Hierbei wird ein Buchstabe durch mehrere andere Buchstaben ersetzt.
Eine weitere Verbesserung sind die sogenannten „Permutationschiffren". Hierbei werden die Buchstaben des Klartexts nicht durch andere ersetzt, sondern in ihrer Reihenfolge vertauscht.
Der „Data Encryption Standard" (DES) war lange Zeit der Algorithmus schlechthin für eine symmetrische Verschlüsselung. Er wurde in den Siebzigerjahren des vorigen Jahrhunderts von der Firma IBM entwickelt und gilt seitdem als Quasistandard für symmetrische Verschlüsselung. DES ist im Prinzip eine Mischung aus Substitutions-, Permutations- und anderen Chiffreverfahren.
Eine Verbesserung des DES ist der „Advanced Encryption Standard" (AES). Der Advanced Encryption Standard (AES) ist eine Blockchiffre, die als Nachfolger für DES im Oktober 2000 vom „National Institute of Standards and Technology" (NIST) als Standard bekanntgegeben wurde. Nach seinen Entwicklern Joan Daemen und Vincent Rijmen wird AES auch Rijndael-Algorithmus genannt (gesprochen wie dt. räindahl). Der Rijndael-Algorithmus besitzt variable, voneinander unabhängige, Block- und Schlüssellängen von 128, 160, 192, 224 oder 256 Bit. Rijndael bietet ein sehr hohes Maß an Sicherheit; erst mehr als zehn Jahre nach seiner Standardisierung wurde der erste theoretisch interessante, praktisch aber nicht relevante Angriff gefunden.
Die Blocklänge des AES ist auf 128 Bit beschränkt; bei der Schlüssellänge kann zwischen 128, 192 und 256 Bit gewählt werden. Entsprechend beziehen sich die jeweiligen Bezeichnungen der drei Varianten AES-128, AES-192 und AES-256 auf die Schlüssellänge. Der frei verfügbare Algorithmus kann ohne Lizenzgebühren eingesetzt oder in Soft- und Hardware eingebunden werden. In den USA werden die beiden Schlüssel AES-192 und AES-256 für staatliche Dokumente der höchsten Geheimhaltungsstufe zugelassen *(Quelle: Wikipedia)*.

Vorteile der symmetrischen Verschlüsselung
Da nur ein Schlüssel für beide Kommunikationspartner existiert, ist das Schlüsselmanagement sehr einfach. Ein weiterer Vorteil ist die hohe Geschwindigkeit für Ent- und Verschlüsselung.

Nachteile der symmetrischen Verschlüsselung
Die Nachteile überwiegen leider die Vorteile, sodass die symmetrische Verschlüsselung nur noch relativ selten zum Einsatz kommt.

- Dadurch, dass es nur einen Schlüssel gibt, darf der Schlüssel nicht in fremde Hände gelangen.
- Der Schlüssel muss über einen sicheren Weg übermittelt werden.
- Die Anzahl der Schlüssel bezogen auf die Anzahl der Kommunikationsteilnehmer wächst quadratisch.

Bekannte symmetrische Verschlüsselungsverfahren

- DES (Data Encryption Standard)
- Triple-DES
- AES (Advanced Encryption Standard)
- IDEA (International Data Encryption Algorithm)
- Blowfish
- Twofish
- CAST-128, CAST-256
- RC2, RC4, RC5, RC6
- Fox

Asymmetrische Verschlüsselungsverfahren (Public-Key-Verfahren)

Bei diesen Verfahren werden prinzipiell zwei verschiedene, jedoch mathematisch verwandte, Schlüssel verwendet. Es gibt einen „öffentlichen Schlüssel" (Public Key) für die Verschlüsselung und einen „privaten

Schlüssel“ (Private Key) für die Entschlüsselung. Das Schlüsselpaar muss folgende Eigenschaft aufweisen: Für alle, die lediglich den „Public Key“ kennen, muss es praktisch unmöglich sein, den zugehörigen „Private Key“ zu bestimmen oder eine mit dem „Public Key“ verschlüsselte Nachricht zu entschlüsseln. Asymmetrische Verschlüsselung hat eine „Einbahn“-Eigenschaft: eine Nachricht kann nicht wieder entschlüsselt werden, wenn der „Private Key“ nicht mehr verfügbar ist. Die Bezeichnung „Public-Key“-Verschlüsselung kommt daher, dass der „Public Key“ ohne Probleme öffentlich bekannt gemacht werden kann, ohne die Sicherheit des Verfahrens zu gefährden. Der „Private Key“ hingegen muss immer geheim gehalten werden.


© Maksim Kabakou

Will nun Person A eine Nachricht verschlüsselt an Person B senden, so holt sich Person A den öffentlichen Schlüssel von Person B aus einer frei zugänglichen Datei und verschlüsselt damit die Nachricht. Nach Erhalt der Nachricht benutzt Person B seinen geheimen Schlüssel, um die von Person A erhaltene Nachricht zu entschlüsseln. Wenn Person A und Person B ein asymmetrisches Verfahren zum Zweck der Vertraulichkeit verwenden, benötigen sie also keinen sicheren Kanal für den Schlüsselaustausch, aber Person A muss sicher sein, dass sie tatsächlich den öffentlichen Schlüssel von Person B benutzt und keinen Schlüssel, der ihr als Schlüssel von Person B untergeschoben wurde. Würde Person A eine Nachricht mit einem untergeschobenen Schlüssel verschlüsseln, so könnte der Täter, dem ja der passende geheime Schlüssel bekannt ist, die Nachricht entschlüsseln. Der Sender benötigt in der Regel die Bestätigung einer vertrauenswürdigen dritten Partei, dass der öffentliche Schlüssel des Empfängers wirklich zu diesem gehört. Diese Bestätigung, das „Zertifikat“, wird im Allgemeinen auch durch ein kryptografisches Verfahren erzeugt und dem öffentlichen Schlüssel beigefügt.

Zwei bekannte asymmetrische Verschlüsselungsverfahren sind das RSA-Verfahren (benannt nach den Erfindern Rivest, Shamir, Adleman) und die Klasse der Elgamal-Verfahren. Zu Letzteren gehören auch die auf elliptischen Kurven basierenden Verschlüsselungsverfahren.

Vorteile asymmetrischer Verfahren

- Jeder Teilnehmer einer vertraulichen Kommunikation muss nur seinen eigenen privaten Schlüssel geheim halten.
- Sie lassen sich einfach für digitale Signaturen benutzen.

- Sie bieten elegante Lösungen für die Schlüsselverteilung in Netzen, da die öffentlichen Schlüssel bzw. Schlüsselzertifikate frei zugänglich auf zentralen Servern gespeichert werden können, ohne die Sicherheit des Verfahrens zu beeinträchtigen.
- Sie sind gut geeignet für Nicht-Abstreitbarkeitszwecke.

Nachteile asymmetrischer Verfahren

- Sie sind langsam, d. h. sie haben im Allgemeinen einen geringen Datendurchsatz.
- Sicherheit: für alle bekannten Public-Key-Verfahren gilt:
  - Es gibt wesentlich bessere Attacken als das Durchprobieren aller Schlüssel, deshalb werden (im Vergleich zu symmetrischen Verfahren) relativ lange Schlüssel benötigt, um ein gleich hohes Maß an Sicherheit zu erreichen.
  - Die Sicherheit beruht „nur“ auf der vermuteten, aber von der Fachwelt anerkannten, algorithmischen Schwierigkeit eines mathematischen Problems (zum Beispiel die Zerlegung einer großen Zahl in die Primfaktoren).
- Die Schlüsselerzeugung ist im Allgemeinen komplex und aufwendig, da die Erzeugung „schwacher“ Schlüsselpaare vermieden werden muss.

(Quelle: BSI „Bundesamt für Sicherheit in der Informationstechnologie“)

Ausblick

Infos zum Autor

Im nächsten Teil der Kryptografie-Serie geht es um „Digitale Signaturen“. Es bleibt spannend, bleiben Sie also dran. ZT

ZT Adresse

Thomas Burgard Dipl.-Ing. (FH)
Softwareentwicklung
& Webdesign
Bavariastraße 18b
80336 München
Tel.: 089 540707-10
info@burgardsoft.de
www.burgardsoft.de
burgardsoft.blogspot.com
twitter.com/burgardsoft