Inhalt




Symmetrische Verschlüsselung

# Die symmetrische Verschlüsselung *

Symmetrisch wird ein Verfahren genannt, wenn man zum **Ver- und Entschlüsseln den gleichen Schlüssel einsetzt** (*die Aussage ist nicht ganz präzise, soll uns hier aber genügen. Erweitert würde man sagen, wenn beide Schlüssel entweder identisch oder sehr leicht auseinander berechnet werden können*). Das leuchtet jedem von uns ein. Den Schlüssel mit dem ich die Haustüre verriegle, brauche ich auch, um die Tür wieder zu entriegeln. Das Verfahren selbst wird auch als **Verschlüsselungsvorschrift** (*Algorithmus*) bezeichnet. In den vorangegangenen Artikeln [„Weißt Du wieviel Sternlein stehen„,

 

„Schlüssel,Salz und Regenbogen„] haben wir bereits festgehalten, dass die Güte eines Verschlüsselungsverfahrens von zwei Eckpfeilern bestimmt wird.

1. **Die Qualität des Algorithmus**. Wie wir gesehen haben, brauchen wir einen optimalen Algorithmus. Ein Verfahren also, bei dem die beste Möglichkeit, die Verschlüsselung zu „knacken“, die **Brute-Force** Methode (*stupides Durchprobieren aller möglichen Schlüssel*) ist.
2. Sofern wir einen optimalen Algorithmus haben, kommt die **Schlüssellänge** ins Spiel. Wir haben uns eine Formel erarbeitet, mit der wir den Aufwand einer Brute-Force Attacke bestimmen können. Für die optimalen symmetrischen Verfahren gilt: Anzahl möglicher Schlüssel = $2^{Schluessellaenge}$

   Bei AES (*Advanced Encryption Standard; 256 BIT*) erhalten wir einen Wert von $2^{256}$. Wenn Sie den Artikel „Weißt Du wieviel Sternlein stehen“ nicht gelesen haben, ist jetzt die Zeit für’s Lesen gekommen.

## Die Vorteile der symmetrischen Verfahren *

Ohne jetzt den mathematischen Hintergrund zu meinen, ist die symmetrische Verschlüsselung für jeden leicht „zu verstehen“. ***Der Schlüssel – Schloss Vergleich ist unmittelbar nachvollziehbar.*** Damit ist die Akzeptanz beim Anwender hoch. Was man versteht, nutzt man eher. Dieser Umstand ist nicht zu unterschätzen. Nicht ohne Grund haben wir eine recht große Nachfrage nach unserem ArchiCryptX Change. Das Verschlüsselungstool ersetzt in nicht seltenen Fällen asymmetrische Verfahren, die bei den Anwendern auf wenig Liebe bzw. auf besagtes Unverständnis stoßen.

Etablierte symmetrische Verfahren sind um ein **vielfaches schneller** als alle asymmetrischen Verfahren. Sie könnten ein reines asymmetrisches Verfahren zum Beispiel niemals einsetzen, um eine Echtzeitverschlüsselung wie ArchiCrypt Live zu realisieren.

## Die Nachteile symmetrischer Verfahren *

**Bei der Verschlüsselung geht es sehr oft darum, vertrauliche Informationen auf unsicherem Weg, von einem Sender zu einem Empfänger zu bringen.**

Da jedoch Sender und Empfänger den gleichen Schlüssel nutzen müssen (*symmetrische*

*Verschlüsselung*), besteht die **Schwachstelle** hier ganz klar bei der **Schlüsselübermittlung**/-übergabe. Der Schlüssel könnte abgefangen werden.

Wenn Sie viele Personen haben, mit denen Sie vertrauliche Informationen austauschen müssen, dann müssen Sie auch eine entsprechende Menge an Schlüsseln bereithalten. Das wird sehr schnell unübersichtlich! **Die Zahl der nötigen Schlüssel** für eine Gruppe von n Personen, die untereinander sicher Nachrichten austauschen wollen lautet: $\frac{n \times (n-1)}{2}$

Bei 100 Personen wären das bereits $\frac{100 \times (100-1)}{2} = \frac{100 \times 99}{2} = 4950$ Schlüssel.

# Caesar-Chiffre *

Gaius Julius Caesar, ein römischer Politiker und Feldherr ( 100v. Chr. – 44 v.Chr.), der bekanntlich kam, sah und siegte, nutzte ein einfaches symmetrisches Verschlüsselungsverfahren, um militärische Informationen zu verschlüsseln. Das Verfahren ist vollkommen unsicher, kann aber sehr gut eingesetzt werden, um das Prinzip der **symmetrischen Verschlüsselung** aufzuzeigen.
Das Verfahren besteht im Prinzip darin, das Alphabet einfach um ein paar Stellen zu verschieben und so aus dem Klartext den verschlüsselten Text zu erzeugen.

Besonders praktisch kann man das Prinzip mit einer Drehscheibe realisieren. Außen das normale Alphabet, im Innenring (die Geheimtextscheibe) dann das Alphabet durch Verschiebung. Die Anzahl der Stellen, um die man das Alphabet verschieben muss, stellt dabei den Schlüssel dar. Die Scheibe unten verschiebt das Original um 4 Stellen. Steht im unverschlüsselten Text ein A (*Aussenscheibe*), wird daraus ein W (*Innenscheibe*), steht im Originaltext ein H, wird daraus ein D. Zum Entschlüsseln geht man einfach umgekehrt vor. Aus W (*Innenscheibe*) wird ein A (*Aussenscheibe*), aus A wird ein E, aus D ein H usw.

So etwas lässt sich sehr schnell knacken. Man testet einfach alle 25 Verschiebungen aus und trifft irgendwann ins Schwarze.

Man kann über dieses Verfahren aus heutiger Sicht nur lächeln. Was bleibt, sind jedoch zwei wichtige Prinzipien.

 

1. Es gibt eine klar formulierte Anweisung (**Algorithmus**) mit der man ver- und entschlüsselt.
2. Es gibt einen **Schlüssel**, den man zum Ver- und Entschlüsseln benötigt. Der Schlüssel gibt hier die Anzahl an Stellen an, um die die innere Scheibe gegenüber der äußeren verschoben werden muss.

**Würden Sie mir glauben, dass es diese Form der Verschlüsselung in Windows heute noch gibt?**

Ja, selbst in Windows 7. Der passende Schlüssel (*Anzahl der Verschiebungen ist dabei ebenfalls fest und lautet 13*). Das Verfahren wird auch **ROT13** (*Rotation um 13 Stellen*) genannt.

Keine Angst, Microsoft nutzt das Verfahren nicht, um Ihre Windows Passwörter abzusichern. Vielmehr setzt man das Verfahren ein, um Ihr Nutzerverhalten statistisch zu erfassen. Sehen Sie sich einmal das User Assist Plugin in ArchiCrypt Shredder an. Sie werden große Augen machen, wenn Sie sehen, was da alles dauerhaft auf Ihrem Rechner gespeichert wird!

Im nächsten Teil beschäftigen wir uns dann etwas eingehender mit der asymmetrischen Verschlüsselung …

 