Inhalt

Gegenstand des dritten teils ist das asymmetrische Verschlüsselungsverfahren **RSA**!

RSA

Wer die Artikelserie im Blog aufmerksam verfolgt hat, kann sich vielleicht nicht als Kryptografie-Guru bezeichnen, den Status Laie hat er aber hinter sich gelassen! Sie sollten inzwischen wissen, was man unter **symmetrischen** und **asymmetrischen** Verschlüsselungsverfahren (Symmetrie vs. Asymmetrie Teil I und Teil II) versteht, verstanden haben, dass beide Verfahren ihre Vor- und Nachteile besitzen und man sie, hinsichtlich ihrer Sicherheit, nur schwer miteinander vergleichen kann. In „Weißt Du, wieviel Sternlein stehen„, wurde zudem anschaulich und eindrucksvoll gezeigt, was es mit Schlüssellängen auf sich hat und wie man sich die unglaublich großen Zahlen, die in diesem Zusammenhang immer wieder auftauchen, besser vorstellen kann.

Hier eine kurze Zusammenfassung:

- Symmetrische Verfahren nutzen zum Ver- und Entschlüsseln den gleichen Schlüssel.
- Symmetrische Verfahren sind extrem schnell und ideal geeignet, große

Datenmengen zu verschlüsseln
- Symmetrische Verfahren sind sehr sicher und ausschließlich (*ein optimales Verfahren vorausgesetzt*), durch Brute-Force zu knacken.
- Asymmetrische Methoden nutzen ein Schlüsselpaar. Mit Hilfe des NICHT geheimhaltungsbedürftigen **Öffentlichen Schlüssels** können wir dem Besitzer des zugehörigen **Privaten Schlüssels** auf sichere Weise eine vertrauliche Nachricht zukommen lassen. Der Private Schlüssel muss vom Besitzer unter allen Umständen geheim gehalten werden. Wer diesen privaten Schlüssel besitzt, kann alle Nachrichten entschlüsseln.
- Die Sicherheit der asymmetrischen Verfahren beruht auf bisher nicht bewiesenen mathematischen Vermutungen. Es besteht theoretisch die Möglichkeit, dass morgen eine Entdeckung gemacht wird, die die asymmetrischen Verfahren aushebelt.
- Asymmetrische Verfahren sind im Vergleich zu ihren symmetrischen Verwandten sehr langsam und eher für kleine Datenmengen geeignet.
- Da asymmetrische und symmetrische Verfahren unterschiedliche Mathematische Grundlagen haben, kann man ihre Sicherheit nur schwer miteinander vergleichen. Das Heranziehen der Schlüssellänge als alleiniges Kriterium ist nicht zulässig.

Als Vertreter der asymmetrischen Verfahren haben wir **RSA** unter die Lupe genommen, den historischen Hintergrund beleuchtet, hergeleitet, wie man das Schlüsselpaar erzeugt und schließlich gesehen, wie man ver- und entschlüsselt. Was aussteht sind zwei Themenkomplexe.

1. Wo setzt man asymmetrische Verfahren ein?
2. Wie greift man asymmetrische Verfahren an?

In diesem Artikel beschäftigen wir uns mit den Einsatzgebieten asymmetrischer Verfahren.

Warum überhaupt asymmetrische Verfahren nutzen? *

Sieht man sich die historische Entwicklung [siehe zum Beispiel Verschlüsselte Botschaften] der Kryptografie an, bemerkt man rasch, dass es zunächst darum ging,

Copyright by 1998-2017 ArchiCrypt Dipl.-Ing. Patric Remus

vertrauliche Informationen (*Bote, Kurier überbringt eine Botschaft; oft politischen oder militärischen Hintergrunds*) miteinander auszutauschen. In den Anfängen kamen sehr einfache Verfahren zum Einsatz und, da asymmetrische Verfahren erst sehr spät entdeckt wurden (siehe Geschichtlicher Hintergrund in RSA Verschlüsselung – Teil I), ausschließlich symmetrische Verfahren. Bei diesen verwenden Sender und Empfänger der Nachricht bekanntlich dasselbe Passwort (*genauer gesagt Schlüssel*).

Genau hier liegt der Knackpunkt.

> In der Sprache der Informationstechnik ausgedrückt, hat man es mit dem Problem zu tun, dass man eine vertrauliche Nachricht (*das zu verwendende Passwort*) über einen unsicheren Informationskanal übertragen muss.

Bevor man also jemandem die erste vertrauliche Nachricht zukommen lassen konnte, musste man diesem das entsprechende Passwort mitteilen. Per Kurier, Brieftaube, Brief oder was auch immer. Diese Mitteilungen konnten und können abgefangen werden, das Passwort wäre damit bekannt, die Verschlüsselung wäre unterlaufen. Siehe zum Beispiel http://de.wikipedia.org/wiki/Lauenburg_(1938)

Hier spielen asymmetrische Verfahren ihren Trumpf aus. Die beiden Parteien, die miteinander Informationen austauschen wollen, erzeugen einfach jeweils ein **Schlüsselpaar**. Den öffentlichen Schlüssel teilen sie dem anderen mit. Dabei spielt es keine Rolle, wie man die öffentlichen Schlüssel austauscht. Im Prinzip können sie sich einen Zeppelin mieten, der den öffentlichen Schlüssel auf einem Transparent hinter sich herzieht und für alle sichtbar über der Stadt kreist.

Den jeweiligen privaten Schlüssel müssen die beiden Parteien hingegen hüten, wie ihren Augapfel.

RSA ist zu lahm für diese Welt! *

Obwohl Rechenleistung und -kapazität immer größer werden, sind asymmetrische Verfahren den symmetrischen Methoden hinsichtlich der Geschwindigkeit hoffnungslos unterlegen. Geht es um große Datenmengen im Gigabyte- oder gar

Terabyte-Bereich, bringt kein Mensch die Geduld auf, die ein asymmetrisches Verfahren vom Anwender erfordern würde.

> Da symmetrische Verfahren in diesem Zusammenhang ausschließlich den Schwachpunkt beim Austausch des Schlüssels haben, kam man auf die naheliegende Idee, beide Verfahren zu kombinieren.

Mit dem asymmetrischen Verfahren tauscht man den Schlüssel aus, der dann anschließend in einem symmetrischen Verfahren zur Ver- und Entschlüsselung der eigentlichen Daten zum Einsatz kommt.

Diese Verfahren werden **HYBRIDE Verfahren** genannt.

> **Beispiel:**
>
> Kennen Sie ArchiCrypt Live?
>
> Kurz gesagt handelt es sich um eine Echtzeit-Verschlüsselung, die auf Ihrem Rechner virtuelle Laufwerke einrichten kann. Klar, dass das Programm ein symmetrisches Verfahren einsetzt, um tatsächlich alle Dateien in Echtzeit zu ver- und entschlüsseln. Zum Einsatz kommt der Industriestandard AES in der 256 BIT Version. Sie schützen damit Ihre lokalen sensiblen Daten gegen unberechtigten Zugriff. Hochsicher und extrem schnell. Was jedoch, wenn Sie ein solches ArchiCrypt Live Laufwerk einem anderen übersenden möchten. Natürlich können Sie das ohne jeden Aufwand, indem Sie dem Empfänger Ihr Passwort einfach per E-Mail (der Postkarte des Internetzeitalters) mitteilen. Doch jeder kann mitlesen, das Passwort abfangen und dann auf die geheimen Daten zugreifen. Das geht besser! ArchiCrypt Live kann selbst Schlüsselpaare für RSA erzeugen. Der Trick besteht auch hier darin, dass das eigentliche Passwort, mit dem die schnelle symmetrische Verschlüsselung gesteuert wird, „einfach“ mit dem öffentlichen Schlüssel des Empfängers verschlüsselt wird. Jetzt können Sie das entsprechend vorbereitete Live Laufwerk einfach per E-Mail oder auf DVD per Post versenden. Ohne den privaten Schlüssel des Empfängers sind die Daten wertlos. Nur der Besitzer des passenden privaten Schlüssels kann das ArchiCrypt Live Laufwerk öffnen. Sie können sich ein Video dazu

ansehen. In der Übersicht bitte das Kapitel X.509 Zertifikate (dazu weiter unten mehr) wählen.

Diese hybriden Verfahren sind (*neben der digitalen Signatur*) das Haupteinsatzgebiet in dem asymmetrische Verfahren zum Einsatz kommen. Man nutzt den Vorteil der asymmetrischen Verfahren um den vergleichsweise kleinen Schlüssel für die symmetrische Verschlüsselung zu übertragen. Entschlüsselt wird dann wieder mit dem so übertragenen symmetrischen Schlüssel. Sicher und rasant schnell!

Online-Shops und Online-Banking *

Sie kennen das kleine Schlosssymbol in Ihrem Browser, welches beim Besuch bestimmter WEB-Seiten angezeigt wird. Den Adressen dieser Seiten ist nicht das „http“ vorangestellt, sondern ein „**https**„.

Angenommen, sie nutzen unseren Dienst unter www.Passwort-Zentrale.de, um unterwegs auf Ihre Passwortdaten zugreifen zu können. Besuchen Sie einmal den Link. Sofort baut unser Server eine sichere Verbindung mit Ihrem Browser auf und lenkt den Datenaustausch auf *https://www.ssl-id.de/passwort-zentrale.de/index.php* um.

Was geschieht hierbei?
Ihr Rechner und unser Server tauschen öffentliche Schlüssel aus und verhandeln einen symmetrischen Schlüssel für die folgende Kommunikation. Dieser Schlüssel ist der so genannte **Sitzungsschlüssel** und wird nur für die aktuelle Verbindung verwendet. Die eigentlichen Daten (*Inhalt der Seite, alle Eingaben, die Passwortdatei*) werden ausschließlich symmetrisch verschlüsselt, mit dem einmaligen Sitzungsschlüssel, übertragen.

Eine Grafik zeigt die Vorgänge beim s.g. Handshake (*Ihr Browser und unser Server handeln das zu verwendende Verschlüsselungsverfahren, den symmetrischen Schlüssel und andere Details aus*). Genau dieselben Mechanismen und Verfahren werden verwendet, wenn Sie sich in einem vertrauenswürdigen Online-Shop befinden oder auf der Seite Ihrer Bank eine Transaktion durchführen. Immer wird zunächst mit einem asymmetrischen Verfahren (*sehr oft RSA*) ein Sitzungsschlüssel für ein

symmetrisches Verfahren ausgetauscht. Die eigentlichen Daten (*Ihre Angaben wie Kontonummer, PIN, Adresse, Name etc.*) werden damit verschlüsselt übertragen.

Der komplexe Vorgang beim Handshake und der Übertragung der Daten berücksichtigt bereits potentielle Angriffsmöglichkeiten um die wir uns in einem späteren Artikel kümmern.

Trau, schau, wem! *

Woher soll Ihr Browser wissen, ob er gerade Daten mit dem richtigen Server austauscht? In diesem Zusammenhang tauchen digitale Zertifikate auf. Dabei stellt X.509 den Standard für das Erstellen digitaler Zertifikate und den Aufbau einer so genannten Public-Key Infrastruktur dar. Wer das Beispiel mit ArchiCrypt Live oben nachvollzogen hat, kam bereits mit dem Begriff **X.509 Zertifikat** in Kontakt.

Ihr Browser kommt bereits nach der Installation mit einer ganzen Liste an s.g. Zertifizierungsstellen, denen man vertrauen kann. Die s.g. Zertifizierungsstellen geben gegen Entgelt Zertifikate an andere weiter. Dabei wird anhand von Dokumenten die Integrität und Vertrauenswürdigkeit der Antragsteller geprüft. Ihr Browser kann dann im Zertifikat der besuchten Seite nachsehen, wer für dieses Zertifikat einsteht (*Aussteller*) und ob es noch gültig ist. Treten Unstimmigkeiten auf, bricht Ihr Browser die Verbindung ab oder gibt eine Warnmeldung aus.

Digitale Signatur – Unterschreiben einmal anders *

Eine Fähigkeit von RSA wurde bisher komplett unterschlagen. Wenn Sie jemandem eine rechtsverbindliche Nachricht zukommen lassen wollen, muss sichergestellt sein, dass die Nachricht genauso von Ihnen auch verfasst wurde. In der „realen“ Welt bestätigen Sie das im Allgemeinen durch Stempel, Unterschrift etc. In der digitalen Welt hingegen wird wie folgt vorgegangen:

Die digitale Unteschrift (Signatur) *

Man Berechnet einen s.g. Hashwert für die Nachricht. Siehe „**Hash me if you can**“ in Schlüssel, Salz und Regenbogen. Diesen eindeutigen Wert verschlüsselt jetzt der Absender der Nachricht mit seinem **PRIVATEN Schlüssel** (*kein Schreibfehler*) und hängt das Resultat (*die s.g. Signatur*) an die Nachricht an. Der Empfänger der Nachricht kann die Signatur jetzt mit dem **öffentlichen Schlüssel** des Absenders entschlüsseln und erhält den Hashwert der Nachricht.

Der Empfänger berechnet jetzt ebenfalls den Hashwert der Nachricht und **vergleicht diesen Wert mit dem übermittelten Wert**. Stimmen beide Wert überein, wurde die Nachricht unverändert übermittelt, die Nachrict stammt vom angeblichen Absender. Integrität und Authentizität sind gewährleistet.

Auch diese Möglichkeit findet man in ArchiCrypt Live. Sie können ArchiCrypt Live Laufwerke auch digital signieren und dem Empfänger damit zeigen, dass der Inhalt in dieser Form von Ihnen stammt. Stimmen beim Empfänger die beiden Werte (*übermittelt und berechnet*) nicht überein, ist klar, dass an dem Laufwerk manipuliert wurde!

Reisen macht Spaß *

Wer hätte das gedacht? Auf unseren neuen **Reisepässen** kommt **RSA** zum Einsatz. RSA wird in diesem Zusammenhang eingesetzt, um eine Manipulation der Daten des RFID Chips zu verhindern. Natürlich muss man auf Reisen auch zahlen und dafür verwendet der moderne Mensch **Plastikgeld**.

Diese „Plastikgeld“-Karten haben nicht mehr den altbekannten Magnetstreifen, sondern einen kleinen Prozessor (*wie zum Beispiel auf der ArchiCrypt Card*). Auch hier werden Daten mit RSA gegen Manipulation geschützt.

Sie sehen, wie unglaublich verbreitet das RSA Verfahren ist. Es gibt noch unzählige weitere Anwendungen des Verfahrens, die jedoch vom Grundsatz her mit den genannten vergleichbar sind. Sie sehen, dass Sie täglich viele Male mit asymmetrischer Verschlüsselung in Berührung kommen, ohne es selbst zu bemerken.

Im letzten Teil der RSA Reihe werden wir uns ansehen, wie Angriffe gegen asymmetrische Verfahren aussehen.

Copyright by 1998-2017 ArchiCrypt Dipl.-Ing. Patric Remus