RSA-Kryptosystem

0. Einleitung

RSA ist ein asymmetrisches Verschlüsselungsverfahren, welches im Jahre 1977 von Ronald L. **R**ivest, Adi **S**hamir und Leonard **A**delman entwickelt wurde. Es ist sowohl zum Verschlüsseln als auch zum Signieren geeignet. Das Buch „New Directions in Cryptography“ von W. Diffie und M. Hellman legte 1976 den Grundstein zur Verwendung eines Public-Key-Verfahrens. Unter diesem Konzept wurde 1978 erstmals von Rivest, Shamir und Adelman einer der bis heute sichersten Public-Key-Algorithmen vorgestellt. Dazu führte die Erkenntnis, dass die Primfaktorenzerlegung um ein vielfaches aufwendiger ist als die Multiplikation zweier Primzahlen.

Vorteile

* Durch die Nutzung von öffentlichen und privaten Schlüsseln wird das Problem der Schlüsselübertragung behoben
* Es ist nicht möglich, durch Brute-Force-Methoden beide verwendeten Primfaktoren in annehmbarer Zeit zu ermitteln (dauert je nach Größe mehrere Mrd. Jahre)
* Um eine sichere Kommunikation aufzubauen, müssen den Teilnehmern nur die öffentlichen Schlüssel der Gegenstelle bekannt sein
* Durch Erweiterung der Primzahlen um ein paar Bit lässt sich der Algorithmus an die immer steigenden Prozessorleistungen anpassen, und bleibt somit auch zukünftig sicher

Nachteil

Die Sicherheit des RSA-Kryptosystems beruht auf der praktischen Annahme, dass die Faktorisierung immer größerer Primzahlen selbst mit den schnellsten Algorithmen eine ungeheuer lange Zeit braucht und damit praktisch nicht durchführbar ist. Wird jedoch ein Algorithmus gefunden, *p* und *q* schnell aus *n* (bez. als RSA-Modul, aus den zufälligen Primzahlen *p* \* *q*) zu folgern, ist der gesamte RSA-Algorithmus geknackt und damit unbrauchbar.

1. Schlüsselerzeugung

Die RSA-Verschlüsselung steht und fällt mit der Umkehrbarkeit der Funktionen. Deshalb setzt man auf Verfahren der Modul-Arithmetik (Division mit Rest). Darin lassen sich gewisse „Einwegfunktionen“ finden, die nur mit erheblichem Aufwand umgekehrt werden können.

Es werden zwei zufällig gewählte Primzahlen (bezeichnet als *p* und *q*) ausgewählt und miteinander multipliziert. Der daraus resultierende Wert *n* wird als RSA-Modul bezeichnet.

Es ist wichtig, für *p* und *q* sehr große Zahlen (mit 100 und mehr Dezimalstellen) auszuwählen, um eine Brute Force Attacke unmöglich zu machen.

Nun werden mit unterschiedlichen arithmetischen Funktionen, unter anderem der Euler‘sche Satz und später zur Erstellung des privaten Schlüssels der Euklid’sche Erweiterungsalgorithmus.

2. Verschlüsselung

Da nur Zahlen verschlüsselt werden können, muss der Klartext mit dem ASCII-Code zuvor in Zahlenreihen umgewandelt werden. Nun wird der Klartext in 512 Bit-Blöcke aufgeteilt, und mit der Funktion chiffriert. Der Geheimtext *g* ist der Rest der Ganzzahlendivision aus dem ursprünglichen Text *t* potenziert mit dem Codierschlüssel (öffentlichen Schlüssel) *c* des Adressaten und *n*.

3. Entschlüsselung

Die Entschlüsselung ist die dementsprechend einfache Umkehrung der Verschlüsselung:

wobei *d* den privaten Schlüssel des Empfängers darstellt.