Asymmetrische Verschlüsselung

Von Kefer Thomas und Laser Tobias

Geschichte[1]

Früher existierten nur symmetrische Verschlüsselungsverfahren, die voraussetzen, dass Sender und Empfänger den gleichen Schlüssel besitzen. Dadurch gestaltete sich der Austausch der Schlüssel als sehr komplex, ohne dass er für Mithörer unverständlich, bzw. ohne Nutzen ist. 1978 veröffentlichte Ralph Merkle das *Merkle Puzzle*, welches den ersten Schritt für die Entwicklung der asymmetrischen Verschlüsselung machte. Darin gab er nur eine verhältnismäßig grobe Idee an, welche dann aber von ihm und *Martin Hellman* noch im selben Jahr umgesetzt wurde.[2] Ein Jahr später festigten *Hellman* und *Whitfield Diffie* die Idee so abstrakt und doch konkret, dass sämtliche Verfahren mit ihren bestimmten Rahmenbedingungen möglich seien. Dadurch entwickelten diese beiden ebenso den nach ihnen benannten *Diffie-Hellman-Schlüsselaustausch*. Das 1978 entwickelte Verschlüsselungsverfahren von Markle und Hellman wurde jedoch bereits 1983 von *Adi Shamir* gebrochen und gilt seither als unsicher.

Das erste konkrete Verfahren wurde 1977 von *Ronald L. Rivest, Adi Shamir* und *Leonard M. Adleman*, benannt *RSA*, am MIT entwickelt und gilt auch bis heute noch als sicherer Standard. Anfang der 1970er-Jahre wurde von drei Mitarbeitern der britischen Regierungsbehörde für Nachrichtendienst und Sicherheitsdienst, im Speziellen Kryptographie, Verfahren für Datenübertragung und Fernmeldeaufklärung, ein ähnliches Verfahren zu dem von *Rivest, Shamir* und *Adleman* entwickelten Algorithmus, sowie dem Diffie-Hellman-Schlüsselaustausch ähnelndes Verfahren entwickelt. Diese wurden nie veröffentlicht aufgrund von Geheimhaltungsgründen und ebenso wenig wurde eine Anmeldung für ein Patent ausgesprochen.

Prinzip[3]

Die *Asymmetrische Verschlüsselung* wird mit zwei Schlüsseln durchgeführt. Der Text oder die Daten werden mit dem *Public Key* verschlüsselt und mit dem *Private Key* entschlüsselt. Dabei besitzt jeder Teilnehmer einen eigenen *Private Key* und jeder den gleichen *Public Key.* Den *Public Key* darf jeder ohne Einschränkungen einsehen, schließlich ist er auch öffentlich. Wichtig sei auch anzumerken, dass die Verschlüsselungsoperation selbst nicht umkehrbar sein darf, bzw. praktisch gesehen sie so schwer umzukehren sein muss, dass sie als unumkehrbar angesehen wird.

Wenn Bob eine Datei herunterladen und öffnen möchte von Alice, schickt Bob zuerst eine zufällige Zahl, die er mit seinem *Public Key* verschlüsselt hat, an Alice, die sie entschlüsselt dann wieder zurück sendet. Wenn dabei die ursprüngliche Zahl das Ergebnis ist, kann Bob sich sicher sein, dass er mit Alice kommuniziert, wenn nicht, dann ist es sehr wahrscheinlich, dass er zufällig mit jemand Fremden oder schlimmstenfalls mit Eve, dem MITM (=Man in the Middle), kommuniziert.

---

[1] https://de.wikipedia.org/wiki/Asymmetrisches_Kryptosystem (zuletzt abgerufen am 30.03.2022)
[2] https://de.wikipedia.org/wiki/Merkles_Puzzle (zuletzt abgerufen am 30.03.2022)
[3] https://www.kryptowissen.de/asymmetrische-verschluesselung.html (zuletzt aberufen am 30.03.2022)

Methoden[4]

- RSA – Rivest, Shamir und Adleman
- Diffie-Hellman-Merkle-Schlüsselaustausch
- MQV – Menezes, Qu und Vanstone (LMQSV)
- PGP – Pretty Good Privacy (OpenPGP)

Sicherheit

Die Sicherheit ist dadurch gegeben, dass niemand die Daten entschlüsseln kann, ohne selbst Teilnehmer zu sein. Der eigene *Private Key* bringt bei verschiedenen *Public Keys* auch immer wieder verschiedene Ergebnisse, in der Regel passt ein *Private Key* zu genau einem *Public Key*.

Anwendungsgebiete[5]

Allen voran wird asymmetrische Verschlüsselung zur Verschlüsselung benutzt. Weitere Einsatzgebiete sind aber auch Überprüfungen digitaler Signaturen, Kommunikationspartner zu verifizieren, dass sie es doch tatsächlich sind oder etwa Prüfsummenberechnung von Dateidownloads, um sicher zu stellen, dass es sich um die korrekte Datei handelt und nicht um eine modifizierte Version, die im schlimmsten Fall auch noch schädlich ist. Bereits bei der Verwendung von HTTPS oder SSH wird asymmetrische Verschlüsselung verwendet, um die Verbindung vor potenziell gefährlichen Mithörern zu verschlüsseln. In der Praxis wird oft nicht ausschließlich auf asymmetrischer Verfahren gesetzt, aufgrund ihrer Zeit, die sie in Anspruch nehmen bei ihrer Durchführung, sondern auf hybride Verfahren, die symmetrische und asymmetrische Verfahren kombiniert.

Vorteil

Der Vorteil der asymmetrischen Verfahren liegt darin, dass die Entschlüsselung nicht möglich ist ohne den korrekten privaten Schlüssel. Es wird auch keine hohe Anzahl an Schlüsseln benötigt, da genau 1 öffentlicher Schlüssel plus genauso viele private Schlüssel, wie Teilnehmer existieren müssen, im Gegensatz zu symmetrischen Verfahren.[6] Außerdem liegt auch kein Schlüsselverteilungsproblem vor, was bedeutet, dass kein geheimer Schlüssel jemanden mitgeteilt werden muss. Ebenso ein großer Vorteil ist, dass sich mit diesem Verfahren Prüfsummen erzeugen lassen, sowie Verifizierungen, etwa bei digitalen Unterschriften.

Nachteil

Asymmetrische Verschlüsselung beinhaltet komplexe und daher langwierige Schritte, wie etwa das Lösen einer Gleichung, was sich für Computer als sehr komplex erweist. Das bedeutet, dass viel Rechenleistung benötigt wird, um eine gebräuchliche Zeit zu erzielen.

---

[4] Autor: Asymetrische Krytografie, in: https://www.elektronik-kompendium.de (Veröffentlichungsdatum), https://www.elektronik-kompendium.de/sites/net/1910111.htm (abgerufen 27.02.2022)

[5] https://www.ionos.de/digitalguide/server/sicherheit/asymmetrische-verschluesselung/ (zuletzt abgerufen am 30.03.2022)

[6] https://www.kryptowissen.de/asymmetrische-verschluesselung.html (zuletzt abgerufen am 30.03.2022)