Symmetrische und Asymmetrische Verschlüsselungsarten

Symmetrische Verschlüsselung

Bei symmetrischen Verschlüsselungsverfahren wird ein Schlüssel verwendet zum ver- und entschlüsseln. Aus diesem Grund ist es ein symmetrisches Verfahren.
Symmetrische Verschlüsselungsverfahren:

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

[Kryptowissen 1]

Das Prinzip der symmetrischen Verschlüsselung ist ganz einfach. Es gibt nur einen Schlüssel, der sowohl für die Ver- wie auch für die Entschlüsselung benötigt wird. Die symmetrischen Verfahren können in zwei Gruppen aufgeteilt werden, Stromchiffren und Blockchiffren. Mit Stromchiffren wird der Klartext Zeichen für Zeichen ver- und auch entschlüsselt. Bei Blockchiffren werden Zeichen des Texts in feste Blockgrössen eingeteilt, so dass mehrere Zeichen in einem Schritt ver- oder auch entschlüsselt werden können.

Bei der symmetrischen Verschlüsselung muss ser Schlüssel gut geschützt werden da er direkten Zugriff auf die Daten gibt. Die grösste Gefahr für den Schlüssel ist in der Übermittlung. Aus diesem Grund gibt es spezielle Protokolle um dies zu machen. Das bekannteste Protokoll ist Diffie-Hellman.
Vorteile:

- Einfaches Schlüsselmanagement, da nur ein Schlüssel für Ent- und Verschlüsselung benötigt wird
- Hohe Geschwindigkeit für Ent- und Verschlüsselung, da Verfahren meist auf effizienten Operationen wie Bit-Shifts und XORs aufbauen

[Kryptowissen 1]

Nachteile:

- Nur ein Schlüssel für Ver- und Entschlüsselung, Schlüssel darf nicht in unbefugte Hände gelangen
- Schlüssel muss über einen sicheren Weg übermittelt werden
- Anzahl der Schlüssel bezogen auf die Anzahl der Teilnehmer wächst quadratisch

[Kryptowissen 1]

Asymmetrische Verschlüsselung

Bei einem Asymmetrischen Verschlüsselungsverfahren werden zwei Schlüssel verwendet zum ver- und entschlüsseln. Dieses sogenannte Schlüsselpaar setzt sich aus einem privaten Schlüssel und einem öffentlichen Schlüssel zusammen. Mit dem privaten Schlüssel, werden Daten Entschlüsselt oder eine digitale Signatur erzeugt. Mit dem öffentlichen Schlüssel kann man Daten verschlüsseln und erzeugte Signaturen auf ihre Authentizität überprüfen.

Weitere Asymmetrische Kryptosysteme:

- Elliptische-Kurven-Verfahren - Basis sind elliptische Kurven / Ähnelt Elgamal
- Merkle/Hellman - basierend auf dem Tornister-Problem
- LUC - ähnlich RSA, Bildung der Lucas-Folge
- MNLN - wie RSA, aber das Polynom xe durch ≫Dickson-Polynom≪ ersetzt
- Digital Signature Algorithm (DSA) - basiert auf dem Diskreten Logarithmus- Problem und benutzt die Kryptosysteme von Schnorr und ElGamal

[Kryptowissen 2]

Am Anfang wird der öffentliche Schlüssel veröffentlicht. Es gibt viele wege um einen Schlüssel zu veröffentlichen, es gibt sogar Server die auf darauf spezialisiert sind. Jeder der den öffentlichen Schlüssel hat kann jetzt Nachrichten verschlüsseln oder eine Signierte Nachricht verifizieren.

Der private Schlüssel muss um jeden Preis geheim halten werden, da die Daten nur damit entschlüsselt werden können. Mit dem privaten Schlüssel können die verschlüsselten Daten entschlüsselt werden und Nachrichten signiert werden.

Zu beachten ist bei der Verschlüsselung, dass je nach verwendetem Schlüssel bei der Verschlüsselung derselben Daten unterschiedliche verschlüsselte Daten entstehen können. [Kryptowissen 2]

Anwendung finden asymmetrische Kryptosysteme bei Verschlüsselungen, Authentifizierungen und der Sicherung der Integrität. Bekannte Beispiele die auf asymmetrische Verfahren aufbauen sind OpenPGP oder auchS/MIME. Aber auch kryptografische Protokolle wie SSH, SSL/TLS oder auch https bauen auf asymmetrische Kryptosysteme. Weiter Anwendung findet bei digitalen Signaturen statt.[Kryptowissen 2]

Vorteile:

- Relativ Hohe Sicherheit

- Es werden nicht so viele Schlüssel benötigt wie bei einem symmetrischen Verschlüsselungsverfahren, somit weniger Aufwand der Geheimhaltung des Schlüssels
- Kein Schlüsselverteilungsproblem, da Public Key für jeden ohne Probleme zu erreichen ist
- Möglichkeit der Authentifikation durch elektronische Unterschriften (digitale Signaturen)

[Kryptowissen 2]

Nachteile:

- Asymmetrischen Algorithmen arbeiten sehr langsam ca. 10 000 Mal langsamer als symmetrische.
- Große benötigte Schlüssellänge
- Probleme bei mehreren Empfänger einer verschlüsselten Nachricht, da jedes Mal die Nachricht extra verschlüsselt werden muss. Abhilfe schaffen hybride Verfahren
- Sicherheitsrisiko durch für jeden zugänglichen Public Key, Man in the Middle

[Kryptowissen 2]

Literaturverzeichnis

[Kryptowissen 1] *https://www.kryptowissen.de/symmetrische-verschluesselung.html*, used: 28.03.2020

[Kryptowissen 2] *https://www.kryptowissen.de/asymmetrische-verschluesselung.html*, used: 28.03.2020