Symmetrische und Asymmetrische Verschlüsselungsverfahren

Verschlüsselungssysteme

Es gibt heutzutage viele Wege, Daten zu schützen. Einer der wichtigeren Wege ist es, Daten zu verschlüsseln. Dies bedeutet, dass die Daten für alle, die nicht den richtigen Schlüssel haben, unlesbar gemacht werden. Somit können die Daten übers Internet übermittelt werden ohne die Sicherheit zu komprimieren. Es gibt zwei Arten von Verschlüsselung, symmetrische und asymmetrische.

Symmetrische Verschlüsselung

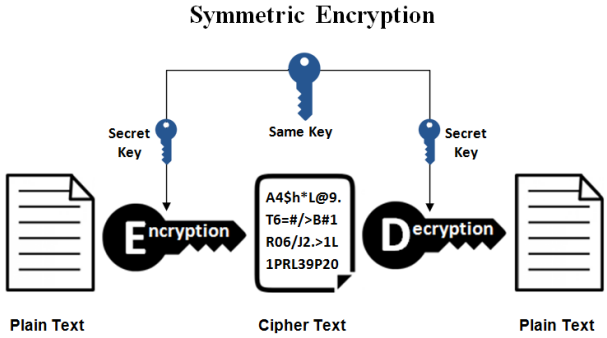
Bei symmetrischen Verschlüsselungsverfahren wird ein Schlüssel zum ver- und entschlüsseln verwendet. Aus diesem Grund ist es ein symmetrisches Verfahren.

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

[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.



[ssl2buy]

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 der Schlüssel gut geschützt werden, da er direkten Zugriff auf die Daten gibt. Die grösste Gefahr für den Schlüssel liegt in der Übermittlung übers Internet. Aus diesem Grund gibt es spezielle Protokolle, dafür. Das bekannteste Protokoll ist der Diffie-Hellman Key exchange.

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

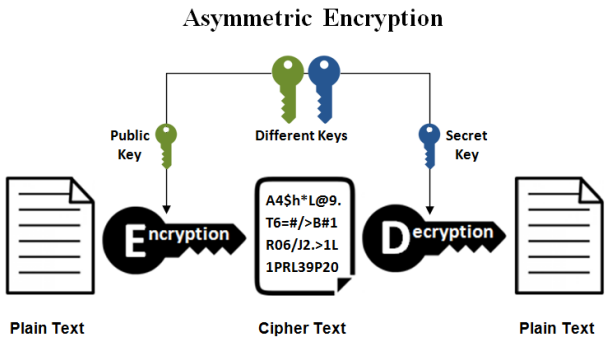
Nachteile:

- 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 zum ver- und entschlüsseln verwendet. Dieses sogenannte Schlüsselpaar setzt sich aus einem privaten Schlüssel und einem öffentlichen Schlüssel zusammen. Mit dem privaten Schlüssel werden Daten entschlüsselt oder es wird eine digitale Signatur erzeugt. Mit dem öffentlichen Schlüssel kann man Daten verschlüsseln und erzeugte Signaturen auf ihre Authentizität überprüfen. Wie der Namen schon sagt, kann der öffentliche Schlüssel veröffentlicht werden. Der private Schlüssel sollte jedoch um jeden Preis geschützt werden.



[ssl2buy]

Asymmetrische Kryptosysteme:

- Ed25519, Ed448

- X25519, X448
- Elliptic curve cryptography
- RSA
- Diffie-Hellman key exchange
- DSA
- Asymmetric Utilities

[Kryptowissen 2]

Asymmetrische Systeme werden an vielen Orten eingesetzt. Das bekannteste Verfahren ist PGP(Pretty Good Privacy) für Mails. PGP ermöglicht, grundsätzlich unsichere Mailprotokoll sicherer zu machen. Mit PGP können Mails ver- und entschlüsselt werden. Mails können auch signiert und auch verifiziert werden.

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]

Literatur

[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

[ssl2buy] *https://www.ssl2buy.com/wiki/wp-content/uploads/2015/12/Symmetric-Encryption.png*, used: 03.04.2020

[ssl2buy] *https://www.ssl2buy.com/wiki/wp-content/uploads/2015/12/Asymmetric-Encryption.png*, used: 03.04.2020