Symmetrische Verschlüsselungsverfahren

Die Verschlüsselungsverfahren der symmetrischen Kryptografie arbeiten mit einem einzigen Schlüssel, der bei der Ver- und Entschlüsselung vorhanden sein muss. Diese Verfahren sind schnell und bei entsprechend langen Schlüsseln bieten sie auch eine hohe Sicherheit. Es gibt zwei Haupttypen von symmetrischen Verschlüsselungsverfahren: Blockchiffre-basierte Verfahren und Stromchiffren.

Blockverschlüsselung

Eine Blockverschlüsselung ist ein deterministisches Verschlüsselungsverfahren, das einen Klartextblock, d. h. einen Klartextabschnitt fester Länge, auf einen Geheimtext- oder Schlüsseltextblock fester (in der Regel der gleichen) Länge abbildet. Diese Abbildung wird dabei durch einen Schlüssel beeinflusst.

- Funktionsweise: Bei einer Blockchiffre wird der Klartext in Blöcken verschlüsselt. Jeder Block hat eine feste Länge (typischerweise 64 Bit bis 256 Bit). Die Verschlüsselung erfolgt durch Anwendung einer mathematischen Funktion auf den Klartextblock unter Verwendung eines Schlüssels.
- Deterministisch: Blockchiffren sind deterministisch, d.h., für denselben Klartextblock und denselben Schlüssel wird immer derselbe Geheimtextblock erzeugt.

Stromchiffren

Eine Stromverschlüsselung, auch als Stromchiffre bezeichnet, ist ein kryptographischer Algorithmus zur symmetrischen Verschlüsselung. Bei der Stromverschlüsselung werden Zeichen des Klartextes einzeln mit den Zeichen eines Schlüsselstroms verknüpft, typischerweise durch die XOR-Operation bei Bits.

- Anwendung. Im Gegensatz zur Blockchiffre ist eine Stromverschlüsselung nicht darauf angewiesen, dass sich genügend zu verschlüsselnde Daten ansammeln, bis sie die Größe für einen Eingabeblock einer Blockchiffre erreichen. Stattdessen kann sie jedes Klartextzeichen sofort in ein chiffriertes Ausgabezeichen übersetzen. Daher sind Stromchiffren besonders für Echtzeitübertragungen geeignet
- Arbeitsweise: Synchron oder Selbstsynchronisierend

Vor- und Nachteile der Symmetrischen Verschlüsselung:

- **Vorteile**:
  - Effizient und schnell
  - Geeignet für große Datenmengen
  - Weniger Rechenleistung erforderlich
- **Nachteile**:
  - Schlüsselaustauschproblem
  - Jeder Kommunikationspartner benötigt denselben Schlüssel

Schlüsselaustauschproblem

- Bei der symmetrischen Verschlüsselung verwenden beide Kommunikationspartner denselben Schlüssel.
- Das Problem besteht darin, wie der Schlüssel sicher übertragen werden kann, ohne dass ein Dritter ihn abhört. Dieses Problem wird mit asymmetrischen Verschlüsselungsverfahren gelöst.

Bekannte symmetrische Verschlüsselungsverfahren

- DES (Data Encryption Standard): 56 bit Schlüssellänge, in kurzer Zeit entschlüsselbar → unsicher
- Triple-DES: 168 bit → besser
- AES (Advanced Encryption Standard): 256 bit, empfohlen bei Hardwareunterstützung (spezieller Befehlssatz für Prozessor)
- IDEA (International Data Encryption Algorithm): 128 bit

Caesar-Chiffre

Caesar-Chiffre ist eine der einfachsten Formen der Verschlüsselung.
Sie wurde bereits vor etwa 2500 Jahren verwendet.

Beispiel:
Angenommen, wir haben den Klartext “HELLO” und möchten ihn mit der Caesar-Chiffre verschlüsseln. Der Schlüssel für die Verschiebung beträgt **3** (dies bedeutet, dass jeder Buchstabe im Alphabet um 3 Positionen nach rechts verschoben wird).

Klartext: HELLO

Verschlüsselung:

H -> K

E -> H

L -> O

L -> O

O -> R

Das verschlüsselte Ergebnis lautet also “KHOOR”. Um den Klartext aus dem verschlüsselten Text zu erhalten, verwenden wir denselben Schlüssel und verschieben jeden Buchstaben um 3 Positionen nach links:

Verschlüsselter Text: KHOOR

Entschlüsselung:

K -> H

H -> E

O -> L

O -> L

R -> O