3.2 Symmetrische Verschlüsselung

Die Verschlüsselungsverfahren der *symmetrischen Kryptographie* (*Private-Key-Verschlüsselung*) arbeiten mit einem **einzigen Schlüssel**, der bei der Ver- und Entschlüsselung vorhanden sein muss. Vor der verschlüsselten Datenübertragung müssen sich die Kommunikationspartner auf den Schlüssel einigen und diesen austauschen. Diese Verfahren sind schnell und bei entsprechend langen Schlüsseln bieten sie auch eine hohe Sicherheit. Vertreter der *symmetrischen Kryptographie* sind *Blockchiffren*[1].

Blockchiffren

Bei *Blockchiffren* werden die zu verschlüsselnde Nachricht in Blöcken von je *k* Bit verarbeitet. Beträgt zum Beispiel *k = 64*, dann wird die Nachricht in Blöcke von 64 Bit Länge aufgeteilt und jeder Block wird unabhängig von den anderen bearbeitet. Beim Verschlüsseln eines Blocks verwendet die Chiffre eine Eins-zu-eins-Zuordnung, um einen *k*-Bit-Block des Klartextes auf einen *k*-Bit-Block des Chiffretexts abzubilden.

Dazu ein Beispiel: Nehmen Sie an, dass *k = 3*, sodass die Blockchiffre 3 Bit lange *Eingaben* als Klartext auf 3 Bit lange *Ausgaben* als Chiffretext abbildet. Eine mögliche Zuordnung enthält Tabelle 1.

Eingabe	Ausgabe	Eingabe	Ausgabe
000	110	100	011
001	111	101	010
010	101	110	000
011	100	111	001

Tabelle 1: 3-Bit-Blockchiffre

Beachten Sie, dass dies eine Eins-zu-eins-Zuordnung ist, das heißt, die *Ausgabe* ist bei jeder Eingabe anders. Diese Blockchiffre unterteilt die Nachricht in 3 Bit lange Blöcke und verschlüsselt jeden Block entsprechend der oben abgebildeten Zuordnung. Sie können nachprüfen, dass die Nachricht `010 110 001 111` zu `101 000 111 001` verschlüsselt wird.

Im Beispiel gibt es $2^3 = 8$ mögliche Eingaben und es können $8! = 40.320$ verschiedene Kombinationen für Schlüssel permutiert werden. Die *Brute-Force-Methode*[2] ist dabei eine beliebte Angriffsmethode, den Chiffretext zu entschlüsseln. Bei 40.320

[1] Siehe: Blockverschlüsselung – Wikipedia
[2] Siehe: Brute-Force-Methode – Wikipedia

Kombinationen gelingt dies sehr schnell. Um solche Angriffe zu vereiteln, verwenden Blockchiffren normalerweise viel größere Blöcke, die aus *k = 64* Bit oder mehr bestehen.

Heute gibt es eine ganze Reihe beliebter *Blockchiffren*, darunter *AES (**A**dvanced **E**ncryption Standard)*, *DES (**D**ata **E**ncryption **S**tandard)* oder *3DES*.

AES

AES ein Produktverschlüsselungsverfahren, welches in mehreren Runden die Bits transformiert. Dazu wird zunächst der Klartext in Blöcke mit 128-Bit eingeteilt. Die Schlüssel können 128, 192 und 256 Bit lang sein. Die Anzahl der Transformationsrunden hängt dabei von der Block- und der Schlüssellänge ab und beträgt 10, 12 oder 14. Abbildung 1 zeigt beispielhaft das Verfahren mit 64-Bit-Blöcken:

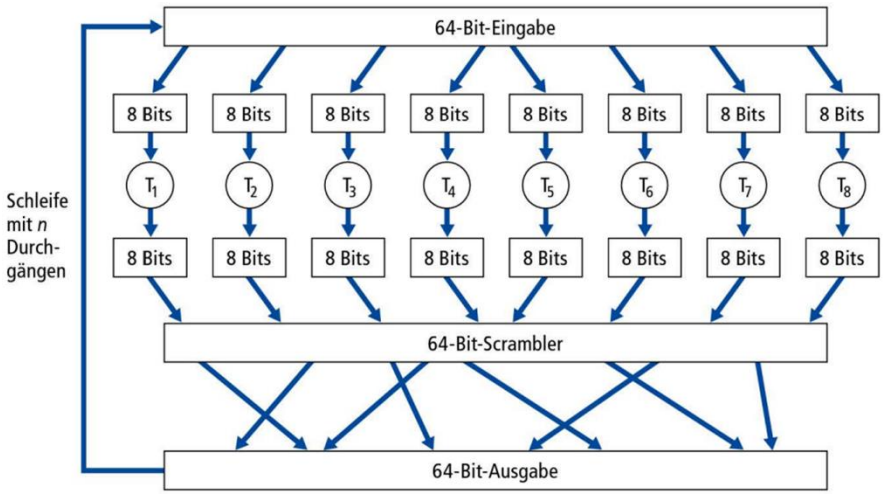

Abbildung 1: Beispiel einer Blockchiffre mit 64-Bit-Blöcken

Der Brute-Force-Angriff auf jede dieser Chiffren besteht darin, alle Schlüssel zu durchlaufen und den Entschlüsselungsalgorithmus mit jedem Schlüssel anzuwenden. Beachten Sie, dass es bei einer Schlüssellänge von *n* genau 2^n mögliche Schlüssel gibt. *NIST*[3] schätzt, dass eine Maschine, die einen *56-Bit-DES* in einer Sekunde knacken könnte (also alle 2^{56} Schlüssel in einer Sekunde testet), etwa 149 Billionen Jahre benötigen würde, um einen *128-Bit-AES-Schlüssel* zu knacken.

[3] **N**ational **I**nstitute of **S**tandards and **T**echnology, „Advanced Encryption Standard (AES)", FIPS 197, Advanced Encryption Standard (AES) (nist.gov)

