8.7 Moderne symmetrische Verfahren

Heutige symmetrische Verfahren verschlüsseln keine Buchstaben, sondern Bitblöcke fester Länge (**Blockchiffren**). Der Standard ist seit 2001 **AES** (Advanced Encryption Standard) mit Schlüssellängen von 128, 192 oder 256 Bit. AES wendet auf jeden 128-Bit-Block mehrere Runden aus Substitution und Transposition an – dieselben zwei Ideen wie in Abschnitt 8.3, nur auf Bits und vielfach verschachtelt.

Bei 128 Bit gibt es $2^{128} \approx 3{,}4 \cdot 10^{38}$ Schlüssel. Eine Maschine, die eine Billion Schlüssel pro Sekunde prüft, wäre damit rund 10^{19} Jahre beschäftigt. Brute Force ist hier endgültig kein Weg mehr.

Ein Problem bleibt aber, und es ist kein mathematisches: Sender und Empfänger brauchen denselben geheimen Schlüssel. Bei n Teilnehmern, die alle paarweise vertraulich kommunizieren wollen, sind das

$$\frac{n \cdot (n-1)}{2}$$

Schlüssel – bei 1000 Teilnehmern also fast eine halbe Million, und jeder einzelne muss sicher ausgetauscht werden, bevor die erste Nachricht fließt. Das ist das **Schlüsselverteilungsproblem**.

Arbeitsauftrag 6

24. Berechnen Sie die Zahl der nötigen Schlüssel für eine Schule mit 900 Personen.
25. Ein Angreifer kann eine Milliarde AES-Schlüssel pro Sekunde testen. Schätzen Sie die Dauer eines Brute-Force-Angriffs auf einen 128-Bit-Schlüssel und vergleichen Sie mit dem Alter des Universums (rund $1{,}4 \cdot 10^{10}$ Jahre). Vergleichen Sie auch mit Abschnitt 8.3.3: Warum ist der Unterschied zur monoalphabetischen Substitution so gewaltig, obwohl beide Schlüsselräume „riesig" heißen?

Gymnasium Ottweiler