1.1 Verschiedene Stufen der Bitstrom-Verschlüsselung

Stufe 1: Periodischer Schlüssel

Hier wird eine mehr oder weniger lange Bitfolge als Schlüssel periodisch wiederholt. Technisch handelt es sich um eine BELASO-Chiffre über dem Alphabet $\mathbb{F}_2$, und gebrochen wird sie wie andere periodische polyalphabetische Chiffren auch durch Periodenanalyse oder Finden eines wahrscheinlichen Wortes.

Stufe 2: Lauftext

Hier wird eine vorhandene Bitfolge als Schlüssel verwendet, z. B. der Inhalt einer CD ab einer bestimmten Stelle. Die Analyse verläuft nach den Methoden aus Kapitel I.5. Außerdem ist, sobald die Quelle der Bits, etwa die CD, dem Gegner bekannt ist, der Schlüsselraum viel zu klein – das lineare Durchprobieren von 700 MB Daten ist wenig aufwendig.

Stufe 4: One Time Pad

Das Extrem auf der sicheren Seite. Wegen der aufwendigen Schlüsselverteilung ist es allerdings für eine Massenanwendung nicht geeignet.

Stufe 3: Pseudozufallsfolgen

Der realistische Mittelweg. Hier wird versucht, die idealen Eigenschaften des One Time Pad zu approximieren, indem man statt einer „echten“ Zufallsfolge eine von einem Algorithmus („Zufallsgenerator“) aus einem „effektiven Schlüssel“ (= kurzen Startwert) erzeugte „pseudozufällige“ Bitfolge verwendet. Sogar bei mäßiger Qualität des Zufallsgenerators ist der Geheimtext dann resistent gegen statistische Analysen. Es bleibt das Problem, die Sicherheit gegen einen Angriff mit bekanntem Klartext in den Griff zu bekommen. Diesem Problem ist der Rest des Kapitels gewidmet.