4 Symmetrische Verschlüsselung

In unserem Alice-Bob-Mallory-Modell wollen wir uns nun die Frage stellen, welche **Verschlüsselungsverfahren** Alice und Bob einsetzen können, um ihre Nachrichten vor Bösewicht Mallory zu verbergen. Wie Sie im Verlauf dieses Kapitels erfahren werden, ist es sinnvoll, wenn die beiden ein Verschlüsselungsverfahren einsetzen, in das eine Geheiminformation (der sogenannte **Schlüssel**) mit eingeht. Je nach Verfahren ist der Schlüssel ein Passwort, eine Geheimnummer oder einfach nur eine Folge von Bits. Bei einem guten Verschlüsselungsverfahren ist es für Alice und Bob bei Kenntnis des Schlüssels einfach, die verschlüsselte Nachricht zu entschlüsseln. Für Mallory ist eine Entschlüsselung dagegen ohne Kenntnis des Schlüssels schwer bis unmöglich, selbst wenn er das Verfahren genau kennt.