Kryptologie

Zuordnung	IuD
Klassenstufe	Kursstufe BF und LF
Bildungsplanbezug	BF, LF
Werkzeug	BJ
Autoren	L. Dietrich, U. Lautebach

Inhalt

Landläufig wird die Kryptografie meistens nur mit dem →1Verschlüsseln (Chiffrieren) von Nachrichten in Verbindung gebracht: Der Absender verschlüsselt sie, weil er ihrem Überbringer nicht ausreichend vertraut. Der soll den Inhalt aber nicht erfahren. Tatsächlich ist die Kryptografie aber bei Weitem vielseitiger: Sie kommt immer dann zum Einsatz, wenn irgendwo eine bestimmte Art von Vertrauen fehlt; ihre Aufgabe ist es jeweils, dieses Vertrauen entweder herzustellen oder zu ersetzen. Insofern behandelt die Kryptografie als Teilgebiet der Informatik durchaus ein menschliches Grundbedürfnis. Auch eine verschlüsselte Nachricht kann dem Boten immer noch einiges verraten: Er erfährt Absender und Empfänger der Nachricht sowie (zumindest ungefähr) ihre Länge. Auch Zeitpunkte und Häufigkeit des Nachrichtenaustauschs kann er protokollieren und daraus seine Schlüsse ziehen. Diese „Metadaten“ haben den zweifelhaften Charme, dass sie sich platzsparend speichern und sehr leicht auch automatisiert auswerten lassen, was für den Inhalt selber in der Regel nicht so einfach geht. Der Bote kann die Nachricht auch verspätet zustellen, verändern, verschwinden lassen oder auch komplett durch eine andere ersetzen – eine intakte Verschlüsselung bietet nur Vertraulichkeit, mehr nicht. Sie stellt das Vertrauen her, dass der Bote den Inhalt der Nachricht nicht erfährt. Alle anderen Probleme lässt sie offen; für einige davon gibt es kryptografische Methoden, für andere nicht.