# Moderne Anwendungen der Kryptographie

## Sicherheit heute

Sicherheit wird heute in vielen Bereichen mit kryptographischen Methoden gewährleistet. Wir betrachten ein System als sicher, wenn es ausreichend gegen *Datenverlust* und *Vertrauensverlust* geschützt ist.

*Datenverlust* entsteht durch versehentliches Löschen, durch Hardwarefehler, durch Viren und Würmer oder durch nicht berechtigte Zugriffe.

*Vertrauensverlust* entsteht durch Nachlässigkeiten der Anwender, durch Zweifel an der Authentizität oder durch nicht berechtigte Zugriffe.

Beide Punkte haben starke Überschneidungen; gerade in den Überschneidungen spielen kryptographische Methoden eine besondere Rolle. Der Schutz vor Vertrauensverlust beinhaltet weit mehr an Sicherheitserwartungen als der Datenverlust.

*Schutz vor Lauschern:* Kein Anderer soll mithören können. Dies ist das klassische Thema der Kryptologie.

*Schutz vor Eindringlingen:* Niemand soll unerlaubt Zugang zu Daten erhalten können. Dazu werden kryptologische und biometrische Methoden verwendet.

*Schutz vor Fälschung:* Die Echtheit von Dokumenten soll sichergestellt werden. Mit Hilfe digitaler Unterschriften kann nachgewiesen werden, von wem ein Dokument stammt.

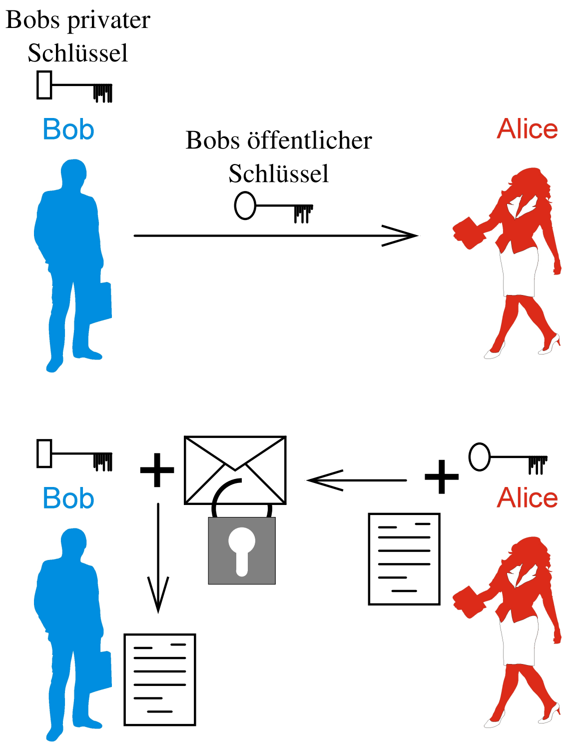
*Schutz vor Diebstahl geistigen Eigentums:* Mit digitalen Wasserzeichen können Daten so gekennzeichnet werden, dass beim Kopieren diese Kennzeichnung nicht gelöscht oder verändert werden kann.

*Beispiel: Ein Kunde möchte etwas über das Internet einkaufen.*

- *Er möchte auf die Echtheit des Angebotes vertrauen können.*
- *Wenn er dem Angebot vertraut, dann möchte er bezahlen. Allerdings möchte er sich darauf verlassen können, dass niemand außer dem Anbieter seine Kreditkartennummer oder Bankverbindung erfährt.*
- *Die Kreditkartengesellschaft möchte sicherstellen, dass nur der Besitzer der Kreditkarte mit dieser auch bezahlen kann.*

# Kryptographie heute

Der Schutz vor Lauschern ist die klassische Aufgabe der Kryptologie. Hierzu gibt es die Auslagen *Kryptographie in der Antike*, *Kryptographie im Mittelalter* und *Visuelle Kryptographie*.




Heutzutage ist *Public-Key-Kryptographie* weit verbreitet. Dabei besitzt jeder einen *öffentlichen Schlüssel* und einen *privaten Schlüssel*. Wenn Alice eine Nachricht an Bob senden möchte, benutzt sie Bobs öffentlichen Schlüssel, um die Nachricht zu chiffrieren. Die verschlüsselte Nachricht kann nur mit Bobs privatem Schlüssel dechiffriert werden, den natürlich nur er kennen sollte (siehe Abbildung). Verschlüsselt Alice die Nachricht außerdem mit ihrem eigenen privaten Schlüssel (Bob kann zum Entschlüsseln Alice' öffentlichen Schlüssel verwenden), so kann sich Bob sicher sein, dass die Nachricht wirklich von Alice kam (*digitale Unterschrift*). Das bekannteste Programm ist hier *Pretty-Good-Privacy* (PGP), das Ende der achtziger Jahre von Phil Zimmermann entwickelt wurde. Es gibt verschiedene Anbindungen von PGP an andere Programme, insbesondere Email-Programme.

Ein weiteres Programm, das heute eingesetzt wird, ist die *Secure Shell* (SSH). Damit kann man sich sicher über das Internet auf anderen Rechnern einloggen. Daten wie Benutzername und Passwort werden bei SSH nur verschlüsselt übertragen. Ein wichtiges Verschlüsselungsprotokoll ist *Secure Socket Layer* (SSL). Mit diesem Protokoll können zwischen einem Server und einem Client Daten sicher ausgetauscht werden. SSL steht in allen aktuellen Webservern und Internetbrowsern zur Verfügung und schafft die Sicherheit, dass persönliche Daten wie Kreditkarteninformationen nicht von Anderen wahrgenommen werden können. (Meist wird eingeschaltete SSL-Verschlüsselung durch ein geschlossenes Vorhängeschloss angezeigt.)

Eine neuere Form der Sicherheit wird durch digitale Wasserzeichen geliefert. Digitale Wasserzeichen sind Veränderungen von Daten, die nur schwer zu entfernen sind. Mit dieser Veränderungen werden Informationen versteckt, die uns z.B. Auskunft über Urheberrechte geben. Auf diese Weise kann ein Urheber nachweisen, dass jemand anderes diese Daten widerrechtlich benutzt oder besitzt. Mehr dazu in der Auslage *Sicherheit von multimedialen Daten — Digitale Wasserzeichen*.