ZMATH 2006d.02525

Lezius, Christoph

Asymmetric cryptosystems. (Asymmetrische Kryptosysteme.)

Leuders, Timo, Materialien für einen projektorientierten Mathematik- und Informatikunterricht. Franzbecker, Hildesheim (ISBN 3-88120-382-6). 99-107 (2004).

Asymmetrische Kryptosysteme kommen sehr oft zum Einsatz, wenn wichtige Daten oder geheime Informationen auf sichere Art übermittelt werden sollen, z.B. bei Überweisungen per Online-Banking oder bei Bestellungen in Internet-Shops. Bekannte Vertreter dieser Klasse sind PGP ('Pretty Good Privacy') und RSA. Asymmetrische Ver- und Entschlüsselungsverfahren haben im Vergleich zu symmetrischen Kryptosystemen eine andere bzw. einfachere Schlüsselverwaltung; sie sind zwar aufgrund ihres mathematischen Fundaments im Allgemeinen schwieriger nachzuvollziehen, aber dafür auch sicherer als symmetrische Verfahren. Diese Sicherheit basiert insbesondere auf dem Einsatz großer natürlicher Zahlen mit mehreren hundert Stellen, für die die gängigen Programmiersprachen keinen passenden Datentypen bereithalten. (orig.)

Asymmetric cryptosystems are very often used to secure the transmission of important data or secret information, e.g. online money transfers or Internet shop orders. PGP (Pretty Good Privacy) and RSA are well-known representatives of these class. Compared to symmetric cryptosystems, asymmetric encoding and decoding methods have a different or easier key management; generally, they are more difficult to understand due to their mathematical foundation, but they are more safe than symmetric methods. This safety is based in particular on the use of large natural numbers with several hundred digits, for which the common programming languages do not have fitting data types.

Classification: P24 Q84 M54 D84