ZMATH 2010d.00590

Haftendorn, Dörte

Crypto-logical. (Krypto-logisch.)

Kortenkamp, Ulrich (ed.) et al., Informatische Ideen im Mathematikunterricht. Bericht über die 23. Arbeitstagung des Arbeitskreises "Mathematikunterricht und Informatik" in der Gesellschaft für Didaktik der Mathematik e. V. vom 23. bis 25. September 2005 in Dillingen. Hildesheim: Franzbecker (ISBN 978-3-88120-471-2/pbk). 73-75 (2008).

Zusammenfassung: Ohne PIN-Nummern, sicheren Datentransfer, digitale Signatur u.a. ist unsere Welt nicht mehr denkbar. Die moderne Kryptografie beruht auf Berechnungen modulo großer Primzahlen oder Primzahlprodukten. Sie hat ihre Wurzeln damit in Algebra und Zahlentheorie, ist aber schon mit überschaubaren Primzahlen ohne Computer nicht zu bewältigen. Zentrale algorithmische Anforderungen liegen beim erweiterten Euklidischen Algorithmus und beim Potenzieren im Modul. Informatische Aspekte sind also die Entwicklung von entsprechenden Funktionen. Die großen CAS können das, für den TI voyage werden Lösungen vorgestellt. Auch die Abarbeitung eines kryptografischen Protokolls ist ein Algorithmus im klassischen Sinn. Der Vortrag beruht auf Erfahrungen im Informatikunterricht des Gymnasiums und in Vorlesungen für Lehramtsstudierende. Für letztere dient die Kryptografie als Ziel und Sinngebung für die Themen "Algebra und Zahlentheorie". Es ist faszinierend wie hier ein gesellschaftlich außerordentlich wichtiges Thema in schulisch überschaubarem mathematischen Handeln transparent wird.

Classification: M54 M55 M59 F64 F65 F69
Keywords: cryptography; mathematical applications; number theory; RSA algorithm