ZMATH 2016c.00978

Witten, Helmut; Schulz, Ralph-Hardo; Esslinger, Bernhard

RSA&Co. in school. Modern cryptology, old mathematics, ingenious protocols. VII: Alternatives to RSA or: discrete logarithm instead of factorization. (RSA&Co. in der Schule. Moderne Kryptologie, alte Mathematik, raffinierte Protokolle. VII: Alternativen zu RSA oder: diskreter Logarithmus statt Faktorisierung.)

Log In 35, No. 181-182, 85-102 (2015).

Zusammenfassung: In den vorangehenden Folgen dieser Beitragsserie haben wir uns mit unterschiedlichen Aspekten bei der Behandlung von RSA im Schulunterricht beschäftigt, u.a.: Wie funktioniert der RSA-Algorithmus? Warum funktioniert RSA? Wie sicher ist RSA? Dort haben wir jeweils auch kleine Ausflüge in die algorithmische Zahlentheorie unternommen, einem faszinierenden Wissenschaftsgebiet an der Grenze zwischen Mathematik und theoretischer Informatik. Die Wurzeln der Zahlentheorie reichen bis ins Altertum wie beispielsweise beim euklidischen Algorithmus, dessen Verfahren von Euklid in seinem Werk Die Elemente bereits im dritten Jahrhundert v. Chr. beschrieben wurde. Aufgrund der modernen Kryptologie hat die Zahlentheorie enorme praktische Bedeutung erlangt. For Part VI see [the first two authors, ibid. 31, No. 172–173, 59–69 (2012; ME 2013e.00764)].

Classification: P20 F60 M50
Keywords: RSA; public keys; factorization; cryptology; encryption; discrete logarithm