ZMATH 2008e.00474

Baumann, Rüdeger

Authentication without giving away knowledge: Cryptographic protocols in computer science lessons. (Authentisierung ohne Wissenspreisgabe: Kryptografische Protokolle im Informatikunterricht.)

Log In 27, No. 145, 35-43 (2007).

Summary: The topic "IT security" is of great significance for education in general and computer science education in particular – but it has not really reached the schools, as some people think to notice. The article pleads for giving priority to the treatment of the topic of authentication (within the general context of security protocols), and still embedding the topic of coding in it.

Classification: P20 P70 M50 N70
Keywords: data encryption; information theory; data presentation; protection of data; data protection; didactics of informatics; graph isomorphism problem; Fiat-Shamir protocol; congruence; number theory; modular arithmetic Datenverschlüsselung; Informationstheorie; Datendarstellung; Datensicherung; Datenschutz; Informatikdidaktik; Graphen-Isomorphieproblem; Fiat-Shamir-Protokoll; Kongruenz; Zahlentheorie; Restklassenarithmetik