© 2019 FIZ Karlsruhe

ZMATH 2003a.00437

Haas, Nicola; Müller, Angelika

Public encoding methods as an answer to problems of data security - a project week. (Öffentliche Chiffrierverfahren als Antwort auf Probleme der Sicherheit im modernen Datenverkehr - eine Projektwoche.)

Peschek, Werner, Beiträge zum Mathematikunterricht 2002. Vorträge. Franzbecker, Hildesheim (ISBN 3-88120-334-6). 207-210 (2002).

In diesem Vortrag geht es um die Vorstellung einer Projektwoche zur Kryptologie, die eine Hinführung zu den asymmetrischen Verschlüsselungsverfahren zum Inhalt hat. Kryptologischer Kern ist dabei das Aufzeigen, historische Verankern und Begreifbarmachen der wesentlichen revolutionären Ideen, die die moderne, aktuelle Kryptologie von der klassischen Kryptologie unterscheidet und die Antworten auf Probleme ermöglichen, die durch die zunehmende Verbreitung elektronischer Netze entstehen (Möglichkeit zum geheimen Schlüsseltausch, Vereinbarung eines Geheimnisses im öffentlichen Gespräch, öffentliche Schlüssel, elektronische Signatur u.a.). Die Materialien (inkl. Computerprogramme) sind so strukturiert, dass die Schüler sich die Grundlagen öffentlicher Verschlüsselungen selbständig erarbeiten können.

Classification: F64
Keywords: public key systems