ZMATH 2010a.00532

Esslinger, Bernhard, Koy, Henrik

Cryptology in class with CrypTool. (Kryptologie im Unterricht mit CrypTool.)

Log In 29, No. 157-158, 75-78 (2009).

Aus der Einleitung: Das auf den ersten Blick sehr abstrakte Thema Kryptologie lässt sich am effizientesten durch praktische Beispiele veranschaulichen und erlernen. Praktische Experimente führen zu konkreten Erfahrungen und erläutern die primären Schutzziele der IT-Sicherheit: Vertraulichkeit, Integrität und Authentizität. Sie helfen dabei, die Gefahren und verfügbaren Schutzmethoden im Rahmen der elektronischen Kommunikation besser zu verstehen. Zur Veranschaulichung kann die frei verfügbare Software CrypTool eingesetzt werden, die bereits in zahlreichen Schulen, aber auch in Firmen und Behörden zur Mitarbeiterschulung verwendet wird. Mithilfe von CrypTool lassen sich klassische und moderne Verfahren visualisieren und mit verschiedenen Parametern praktisch durchspielen. Darüber hinaus lassen sich kryptanalytische Angriffe, also das "Knacken" einer (schwachen) Verschlüsselung, praxisnah durchführen. Ziel von CrypTool ist, eine umfassende Plattform für Kryptografie und Kryptanalyse bereitzustellen, die für den Einsatz im Unterricht gut geeignet ist. Speziell für die Unterstützung des Schulunterrichts wurde zudem das Cryptoportal für Lehrer geschaffen. Es bietet Lehrenden eine Plattform, auf der sie Unterrichtsmaterialien rund um das Thema Informationssicherheit und Kryptologie veröffentlichen und darüber diskutieren können. Verfügbare Materialien können direkt heruntergeladen werden.

From the introduction (translation): The most efficient way to illustrate and learn the, at first glance, abstract topic of cryptology is by using practical examples. For this, the freely available software CrypTool can be used to visualize and practically go through classic and modern methods with different parameters. In addition, realistic cyrpto-analytical attacks, i.e. the "hacking" of a (weak) encryption, can be carried out with it. Additionally, for the support of school teaching, the Cryptoportal for Teachers has been specially set up. On this platform, teachers can publish and discuss teaching materials all around the topic of information security and cryptology. Available materials can be downloaded immediately.

Classification: P20 R30 F60 M50
Keywords: cryptography; coding; data protection; protection of data; encryption of data; educational media; educational software; computer as educational medium; teaching aids; concretizing; internet Kryptografie; Codierung; Datenschutz; Datensicherung; Verschlüsselung von Daten; Unterrichtsmedium; Unterrichtssoftware; Computer als Unterrichtsmedium; Lehrmittel; Konkretisieren; Internet