COALA - System for Visual Representation of Cryptography Algorithms

Z. Stanisavljevic, J. Stanisavljevic, P. Vuletic, Z. Jovanovic

References:

Abstract:
Educational software systems have an increasingly significant presence in engineering sciences. They aim to improve students’ attitudes and knowledge acquisition typically through visual representation and simulation of complex algorithms and mechanisms or hardware systems that are often not available to the educational institutions. This paper presents a novel software system for CryptOgraphic ALgorithm visuAl representation (COALA), which was developed to support a Data Security course at the School of Electrical Engineering, University of Belgrade. The system allows users to follow the execution of several complex algorithms (DES, AES, RSA, and Diffie-Hellman) on real world examples in a step by step detailed view with the possibility of forward and backward navigation. Benefits of the COALA system for students are observed through the increase of the percentage of students who passed the exam and the average grade on the exams during one school year.

Keywords:
Diffie-Hellman, Security education, Data security, Algorithm visualization, Cryptographic algorithms, DES, AES, RSA