Abstract

Most of the engineering programs especially computer science have two or more security related subjects, but lack of active learning and practical experience in the classroom. Cryptographic algorithms which solve Security problems relay on specific mathematical areas such as modular arithmetic, probability and number theory. Unfortunately students feel difficulty to follow the concepts due to the underlying sophisticated mathematics; it is necessitating a fundamental change in our curriculum. Interactive pedagogical tools need to be introduced incrementally along with standard content in a way that makes the standard content easier to learn and vice versa. This work describes an interactive visualization tool which helps the student community to understand the mathematical concepts behind public cryptography algorithms using Microsoft Excel Spreadsheet. It is shown how the sophisticated maths can be visualized and implemented and also discussed some of the famous public key algorithms that the students at various level can do with the help of Microsoft Excel Spreadsheet.
An Interactive Visualization Tool for the Interpretation of Mathematical Concepts behind Public Key Cryptography

- Information Security Course Based on Applications of Management Techniques in Digital Systems for Business Colleges, Herath et al., The 2002 International Conference on Security and Management, (SAM02), Las Vegas, USA, 23-25, June 2002
- Integration of computer security laboratories into computer architecture courses to enhance undergraduate curriculum, Herath et al., Proceedings of Workshop on Computer Architecture Education, June 9-11, 2003, San Diego, CA
- DESvisual: A Visualization Tool for the DES Cipher, Jun Tao, Jun Ma, Melissa Keranen, Jean Mayo, Ching-Kuang Shene, March 26, 2011
- Learning the Related Mathematics to Cryptography by Interactive Way, Mohamed Salim Trigui, Daniyal M. Alghazzawi, MECS, March 2012
- C. E. Iglesias, et al., "Calculus b-learning with java tools," WSEAS Transactions on ADVANCES in ENGINEERING EDUCATION, pp. 295-305

Index Terms

Computer Science Security

Keywords
Interactive tool Maths behind public key cryptography RSA visualization tool ECC visualization tool