SHAvisual: A Secure Hash Algorithm Visualization Tool

Jun Ma, Jun Tao
Department of Computer Science
Michigan Technological University
Houghton, MI
{junm,junt}@mtu.edu

Melissa Keranen
Department of Mathematical Sciences
Michigan Technological University
Houghton, MI
msjukuri@mtu.edu

Jean Mayo, Ching-Kuang Shene, Chaoli Wang
Department of Computer Science
Michigan Technological University
Houghton, MI
{jmayo,shene,chaoliw}@mtu.edu

ABSTRACT

This poster presents a visualization tool SHAvisual for instructors to teach and students to learn the SHA-512 algorithm visually with demo and practice modes. This poster will also discuss some findings of classroom use and student reactions, which are very positive and encouraging.

Categories and Subject Descriptors

K.3.2 [**Computers and Education**]: Computer and Information Science Education

General Terms

Algorithms, Security

Keywords

Cryptography, visualization

1. INTRODUCTION

Cryptography is the foundation upon which secure communication rests and the topic is now a component in many courses, such as Computer Security, Network Security and Cryptography. The diversity of courses that cover cryptography together with its mathematical sophistication makes teaching this topic challenging. Students have diverse backgrounds and abilities and the time that can be devoted to the topic varies based on the focus of the course. We have developed a visualization tool, SHAvisual, that helps students learn the SHA algorithm. We believe this tool will help instructors manage the classroom time devoted to this algorithm and will substantially enhance independent study for interested students.

Software tools for demonstrating cryptography algorithms have started to appear in recent years. Although SHA plays an important role in cryptography, not many visualization tools include SHA. The web-based applet SHA1-VA [1] was claimed by the authors as the first interactive software to demonstrate the SHA-1 algorithm step by step. Our SHAvisual and SHA1-VA are significantly different. First, SHA1-VA is for SHA1 while SHAvisual is designed for a more advanced algorithm, SHA-512. Second, SHAvisual has the demo and full modes separately. Third, the practice mode in SHAvisual provides instructors a convenient check for teaching effectiveness. Finally, SHA1-VA presents the algorithm with a few graphical demonstrations, while SHAvisual shows each component individually with a better and more graphical presentation in a straightforward way.

ITICSE '14, Jun 21-25 2014, Uppsala, Sweden
ACM 978-1-4503-2833-3/14/06.
http://dx.doi.org/10.1145/2591708.2602663 .

2. CONTENT OF POSTER

This poster will explain our new tool SHAvisual for learning the SHA-512 algorithm. It will discuss some preliminary classroom evaluation and self-study assessment by students who were not taking the course and only used SHAvisual for self training through reading some documents and web sites. A live demonstration will be available. This tool is one component of a larger NSF project to develop a set of materials for teaching cryptography. Electronic versions of the SHAvisual, as well as the other tools developed as part of this NSF project, will be available at `www.cs.mtu.edu/~shene/NSF-4`.

3. SIGNIFICANCE AND RELEVANCE

Our work focuses on two fronts: the tool must be easily used for demonstration by instructors in the classroom, showing the algorithm step by step, and the tool can be used for self training by students who wish to learn the basic cryptography methods. Our tool is designed to match the layout of those found in most cryptography and/or data security textbooks to minimize user confusion. Since there are not many published visualization tools for the SHA algorithms, our work is not only relevant to this conference but also helpful to those who are teaching cryptography and data security courses and to students who may need additional aid to learn cryptography methods.

4. REFERENCES

[1] D. B. Nasr, H. M. Bahig, and S. S. Daoud. Visualizing Secure Hash Algorithm (SHA-1) on the Web. In *Proceedings of International Conference on Active Media Technology*, pages 101–112, 2011.

Acknowledgements

This work is supported by the National Science Foundation under grants DUE-1140512, DUE-1245310 and IIS-1319363.