A Comparison of Different Methods of Instruction in Cryptography

Frank H. Katz
Department of Computer Science and Information Technology
College of Science and Technology
Armstrong State University
11935 Abercorn Street
Savannah, GA 31419
United States of America
Frank.Katz@armstrong.edu

ABSTRACT: *Cryptography is the foundation on which information and cyber security is built. As Mark Stamp has written, "cryptography or 'secret codes' are a fundamental information security tool." (Stamp, et al., 2006) Without the ability to encrypt and decrypt messages or data, the fundamental characteristic of confidentiality, which is the prevention of "unauthorized reading of information," (Stamp, et al., 2006) is lost. This could cause the potential exposure of trusted information. Given the importance of this discipline, teaching students the basics of cryptography should be an integral part of any curriculum in information and cyber security. For years students have been taught to perform cryptographic exercises by hand performing paper-and-pencil exercises, or by writing programs in a computer language to perform the cryptographic methods. Today, open-source GUI software exists that can teach students the methods of encrypting and decrypting messages. Consequently, it is of value to measure the effectiveness of teaching cryptography using paper-and-pencil exercises versus using software with a GUI interface.*

Keywords: Information security, Cyber security, Curriculum, Pedagogy, Cryptography.

Received: 18 January 2015, Revised 14 February 2015, Accepted 20 February 2015

1. Introduction

The need for students to understand and apply cryptographic methods has never been greater. Numerous real-world incidents, from PayPal's Two Factor Authentication being temporarily broken (Higgins, et al., 2014) to the hacking of various commercial sites such as Target and Michael's have demonstrated the need for strong cryptographic methods to prevent similar events from happening again. The proliferation of passwords and the conundrum of having to create so many complex passwords that are easy to remember has also shown that cryptography is an important academic discipline and practical component of any information security program. The students of today will graduate and become the Information Security professionals of the future who will have to understand and employ secure and effective cryptographic methods in order to better secure our data and information.

2. Various Approaches to Teaching Cryptography

Cryptography is based on various "diverse mathematical disciplines (number theory, abstract algebra, probability), so students with a less substantial mathematical background are often intimidated" by the mathematics of cryptography. These students could definitely benefit from "teaching through practical examples." (Adamoviæ, S.Branoviæ, I., •ivkoviæ, D., Tomaševiæ, V., &Milosavljeviæ, M, 2011) Even though mathematics is the foundation of cryptography, there are multiple approaches to teaching information security and cryptography, some of which do not require an extensive use of mathematics. "Cryptography can be taught from several different perspectives: the mathematics can be the main element, or cryptographic practice, or there can be a mixture of the two. Most current courses which teach cryptography require mathematics to be mastered as part of the curriculum; courses which de-emphasize mathematics seem more properly to be generic security courses, rather than formal cryptography courses." (Mc Andrew, et al., 2008) "Cryptographic practice" could involve various non-mathematical methods of teaching the topic. Two such different approaches could include the "traditional lecture approach" and the "project approach." (Yurick& Doss, et al., 2001) The "traditional lecture approach" is similar to how information security and cryptography had been taught at Armstrong – in a "survey breadth course" with lectures, case studies, "hand-cranked" problems in class and on assignments. The "project approach," including the use of hands-on tools, "engages with interactivity and entertainment value, and there is room for creativity in the interfaces, architecture, and protocols" (Yurick& Doss, et al., 2001) used, providing students with a more realistic learning experience.

3. Previous Work

Information Security has been an integral component of Armstrong State University's Information Technology degree since 2004, and cryptography has been an important component of this curriculum. Instruction in cryptography at Armstrong has, for the most part, consisted of case study examples and "paper and pencil" exercises. The lecture material included a fascinating look into the history of cryptography and its effect on military history and espionage, such as the Zimmerman Telegram's effect on the United States' entry into World War I and the breaking of the Japanese Purple Code leading to the defeat of the Japanese fleet at the battle of Midway in 1942. (Yurick& Doss, et al., 2001)The "paper-and-pencil" exercises included classwork and homework assignments in using methods such as various transposition ciphers, combinations ciphers, the Vigenère Square, and the use of the RSA algorithm to encrypt and decrypt simple messages.

Since returning from an NSF-sponsored workshop in Information Assurance in 2012, the curriculum has included more hands-on exercises, using, in particular, laboratory exercises. During the Fall 2011 and 2012 courses in Information Security (ITEC 5001, Cyber Security I), students were given identical surveys of learning outcomes from the course. These were the basis of the paper "Measuring the Effectiveness of Instruction Based on Material From a Hands-On Workshop in Information Assurance," presented at InfoSecCD 2013 at Kennesaw State University.(Katz, et al., 2013)

The results of that paper (Katz, et al., 2013)showed significant gains in students' understanding of cryptographic principles when hands-on exercises were added to the curriculum. In 2011, before attending the NSF-sponsored workshop and incorporating the use of CrypTool 1(CrypTool 1), students only performed paper-and-pencil exercises in cryptography. At the beginning and the end of the semester, students were given a 21 question learning outcomes questionnaire, which contained two questions regarding cryptography. Under the same before-and-after scenario, students in the 2012 ITEC 5001 class were given the same questionnaire. The difference was that the 2012 students had been exposed to hands-on exercises that the 2011 students were not. Whereas the 2011 students showed an 11.11% increase in their understanding of cryptography, as measured by their responses to the statement, "I understand the basic principles of cryptography and can perform several very basic cryptographic schemes such as substitution and transposition ciphers," the 2012 students showed a 48.81% increase in their understanding of cryptography. Students also responded to the statement, "I can describe the differences between symmetric and asymmetric encryption." The 2011 class exhibited a 14.29% increase in understanding, while the 2012 class showed a 49.38% improvement in understanding. Nonetheless, these results did not give a true indication of what cryptographic methods were being taught, or how they were being taught. In order to improve instruction in cryptography, it was clear that another, more precise survey, might be warranted.

Consequently, a new survey was created, focusing solely on the effectiveness of various means of teaching cryptography. This survey was administered to ITEC 5001, Cyber Security I students during the Fall 2013 semester.

4. Comparison of Learning Outcomes

The survey administered in November, 2013 was based on the semester's assignment in cryptography. Before being given this

assignment, the students were first taught how to perform the cryptographic operations by hand, in a "paper and pencil: exercise, from material in the textbook. (Whitman & Mattord et al., 2012)Then they were given a demonstration in how to use CrypTool 1 to perform the same cryptographic algorithms. By working through the cryptographic algorithms by hand from the instructions in the textbook [7], the students were initially exposed to the underlying concepts of cryptography before applying them in CrypTool 1.

In the assignment, students were required to encrypt and decrypt the same message using three different algorithms, first by hand (and for RSA, using a calculator), and then using CrypTool 1. The three different algorithms were XOR, the Vigenère Square, and RSA. Students were required to use the RSA algorithm to encrypt and decrypt the message by hand. (Whitman &Mattord et al., 2012) They were then required to use CrypTool 1 to encrypt and decrypt that same message. However, their use of CrypTool 1 was not just limited to encrypting and decrypting a message. The textbook example gave them a P of 3 and Q of 11 (Whitman &Mattord et al., 2012). They used CrypTool 1 to find another pair of relatively prime numbers, each no greater than 100. They then had to use that new pair to execute the algorithm to encrypt and decrypt the message by hand, and using CrypTool 1. In this way, they learned an important additional function of the application.

While these were the same algorithms assigned to ITEC 5001 in 2012, and referenced in "Measuring the Effectiveness of Instruction Based on Material From a Hands-On Workshop in Information Assurance," (Katz, et al., 2013), the survey questions were different than those administered in 2012. They were not based on any before-and-after implementation of pedagogical methods, as was the case in 2012.

Instead, they were specifically focused on the method of teaching the algorithms. Thus the survey was given after the assignment had been completed.

The survey consisted of seven questions:
1.My ability to use the Vigenère cipher to solve an encryption problem was improved by performing the pencil-and-paper exercise.
2.My ability to use the Vigenère cipher to solve an encryption problem was improved by performing the CrypTool 1 lab exercise
3.My ability to use the XOR (exclusive OR) cipher to solve an encryption problem was improved by performing the paper-and-pencil exercise.
4.My ability to use the XOR (exclusive OR) cipher to solve an encryption problem was improved by performing the CrypTool 1 lab exercise.
5.My ability to use the RSA encryption algorithm to solve an encryption problem was improved by performing the paper-and-pencil exercise.
6.My ability to use the RSA encryption algorithm to solve an encryption problem was improved by performing the CrypTool 1 lab exercise.
7.Overall, using the CrypTool 1 lab to solve an encryption problem gave me a greater understanding of the cryptographic algorithms than performing them by the pencil-and-paper exercises.

The statements required the students to answer with the traditional Strongly Agree (5), Agree (4), Neither (3), Disagree (2), and Strongly Disagree (1) rankings. Fifteen students participated in the survey. The results are shown in the Appendix, and were somewhat surprising. For the paper-and-pencil exercise to perform the Vigenère cipher, students recorded a weighted average of 4.133 to 3.733 for using CrypTool 1. For the XOR algorithm, students recorded a weighted average of 3.933 for the paper-and-pencil version to 3.786 for the CrypTool 1 exercise. The RSA encryption exercise saw a reversed result, as the students recorded a 3.867 weighted average for the paper-and-pencil exercise and a 4.133 weighted average for using CrypTool 1. Overall, the students recorded a weighted average of 3.533 when asked if using CrypTool 1 gave them a greater understanding of the cryptographic algorithms than the paper-and-pencil exercises.

Given the small ($N = 15$) sample size of the survey, the student responses were entered into SPSS to provide paired sample T-Test results. This was done to test the significance of the pencil-and-paper vs. CrypTool 1 weighted average survey results for each cryptographic algorithm.

The T-Test for the Vigenère cipher algorithm resulted in a mean of 4.13 and standard deviation of .915 for the paper-and-pencil exercise and a mean of 3.73 and a standard deviation of .884 for CrypTool 1. With a P of 0.288 and a t(14) of 1.103 it can be said that the survey results for the pencil-and-paper exercise were not significantly different than those for using CrypTool 1.

Similar comparisons resulted in similarly insignificant differences for each of the other algorithms. The XOR algorithm resulted in a P of 0.861, and a t(14) of 0.179 with a mean of 3.86 and standard deviation of 1.099, while CrypTool 1's for XOR was 3.79 and 0.802 respectively.. The RSA algorithm resulted in a P of 0.512 and a t of -0.673. Its mean for the paper-and-pencil was 3.87 with a standard deviation of 1.187, and CrypTool 1's was a mean of 4.13 with a standard deviation of 0.834.

5. Conclusions and Recommendations

At first glance, the results make it hard to draw a conclusion. For the two cryptographic algorithms that were not based wholly on mathematics, the Vigenère Square and XOR, students saw a 10.71% and 3.88% improvement, respectively, in their ability to solve an encryption problem, when using the manual paper-and-pencil method over using CrypTool 1. Neither of these percentage increases based on the weighted average responses were very large, indeed, the 3.88% improvement in the ability to perform the XOR algorithm via a paper-and-pencil exercise over using CrypTool 1 was rather small. On the other hand, there was a 6.88% increase in the ability to use CrypTool 1 to encrypt and decrypt a message using the RSA algorithm over using the hand-calculated method. Overall, with a 3.533 weighted average, the students barely felt that using CrypTool 1 was better than a paper-and-pencil exercise for learning and understanding the three encryption algorithms.

With the margins of improvement in understanding between both methods so small, and the SPSS-calculated T-Test results showing no significant difference between using the two methods, can any conclusion be drawn from these results, and what implication does this study have for the future of teaching cryptography at Armstrong? It appears that it for the two algorithmic methods that are not math-intensive, the Vigenère Square and XOR, manually manipulating the data by hand may result in a somewhat greater understanding of the algorithm than using the GUI tool. For the RSA algorithm, which requires complex mathematics, CrypTool 1, which displays the step-by-step results of intermediate and final calculations, is slightly more effective. This is in keeping with the findings of Adamoviæ, et al: that "students are able to follow every cryptographic system step by step. More importantly, students can easily and quickly implement their ideas by dragging objects from the palette that contains algorithms and run the simulation in real time." (Adamoviæ, S.et al., 2011)

Nonetheless, the overall results only showed a marginal advantage for the use of CrypTool 1. This implies that future classes of ITEC 5001 should incorporate both the use of manual methods and the use of an interactive system such as CrypTool 1 to teach cryptography.

References

[1] Adamoviæ, S., Branoviæ, I., •ivkoviæ, D., Tomaševiæ, V., &Milosavljeviæ, M. (2011). Teaching interactive cryptography: the case for CrypTool *In:Proceedings of the IEEE Conference, ICEST.*

[2] Higgins, Kelly Jackson (2014). Voxpopuli: the public searching of the Web. http://www.darkreading.com/mobile/paypal-two-factor-authentication-broken/d/d-id/1278840?, retrieved June 25.,

[3] CrypTool 1, http://www.cryptool.org/en

[4] Katz, Frank H. (2013). Measuring the Effectiveness of Instruction Based on Material From a Hands-On Workshop in Information Assurance. *In: Proceedings of the Information Security Curriculum Development Conference (InfoSecCD '13)*, p 8-12

[5] McAndrew, Alasdair (2008). Teaching cryptography with open-source software.*In: ACM SIGCSE Bulletin,* 40 (1), p 325-329. ACM.,

[6] Stamp, Mark. (2006). Information Security, Principles and Practice. John Wiley & Sons.

[7] Whitman., Michael, E., Mattord, Herbert, J. (2012). Principles of Information Security, 4th ed. Course Technology, 369-372

[8] Yurcik, William and Doss, David (2001). Different Approaches in the Teaching of Information Security.*In: Proc. of Information Systems Education Conference (ISECON).*

Author Biography

Frank H. Katz is an Assistant Professor of Information Technology at Armstrong State University. He completed 21 years of IT industry experience before joining the faculty at Armstrong State University in 2002. He was instrumental in the creation of Armstrong's courses in Cyber Security and the university's Interdisciplinary Minor in Cyber Security. He has presented several times at the Computer Security Conference, the Information Security Curriculum Development Conference, the Southeastern Conference of the Consortium for Computing Science in Colleges (CCSC-SE), has been published in the Journal of the CCSE-SE, and in the Digital Library of the ACM.