THE DESIGN AND IMPLEMENTATION OF A CRYPTOGRAPHIC EDUCATION TOOL

Abdrah Abuzaid, Huiming Yu, Xiaohong Yuan
Department of Computer Science, North Carolina A&T State University, Greensboro, NC, U.S.A.

Bill Chu
Department of Software and Information Systems, University of North Carolina at Charlotte, Charlotte, NC, U.S.A.

Keyword: Encryption, Decryption, Education tool.

Abstract: A Cryptographic Education Tool (CET) has been designed and implemented to aid teaching ciphers. This tool exhibits how change case, simple cipher, RSA and SDES work, and guides students step by step to generate encryption keys and uses generated keys to encrypt and decrypt messages. The design principles of the CET are user friendly, visualization-based, and easy to install and use. This tool has been successfully used in the Web Security class for spring 2010 in the Department of Computer Science at North Carolina A&T State University. Our experience exhibits that using this tool in the Web Security course helped students not only better understand the concepts of cryptography, but also gain significant knowledge of various algorithms and processes of key generation, encryption and decryption. Students' survey and feedback reflected that this tool is very valuable for their educational experience. This tool could also be used in senior cryptography, networking and first year graduate level courses.

1 INTRODUCTION

With dramatic growth of e-commerce, wireless network and cloud computing, security has become a major concern throughout the world. In business environments and individual's daily life people require a certain level privacy, integrity, confidentiality and availability (Stallings, 2006). Increasing Information Assurance education and teaching knowledge of security techniques to students who major in computer science, information technology and management information system, and satisfying new expectation for Information Technology professionals become very urgent.

Cryptography is a major technique to keep data, communication and information systems safe and is a core topic in Information Assurance and computer security. It involves multiple fields such as mathematics, computer science, communication and information processing. Cryptography has been taught in different courses and curriculum for years (,Khambari, Othman, Motsida and Abdollah, 2009, Schweitzer and Baird, 2006, Yang, Zhong, Yin and Huang, 2009). A theory-algorithm-practice-application mode has been proposed to teach cryptology (Yang, Zhong, Yin and Huang, 2009). Schweitser and Baird used an interactive visualization applet to aid teaching ciphers (Schweitzer and Baird, 2006). We have taught cryptography in Web Security courses for several years. According to students' feedback some of them have difficulty to fully understand how different ciphers work through textual presentation and mathematical notations, as used by traditional lectures. . For many students a visualization-based education tool can help them to understand different ciphers by getting hands-on and to practice encryption and decryption step by step. A Cryptographic Education Tool has been developed in the Department of Computer Science at North Carolina A&T State University (NC A&T SU) to help students better understand the concepts of cryptography, algorithms and processes of key generation, encryption and decryption, and let students get hands-on experience. This tool can be used in cryptography, network security, and Web security courses by instructors in the classroom or by

Abuzaid A., Yuan X., Yu H. and Chu B..
THE DESIGN AND IMPLEMENTATION OF A CRYPTOGRAPHIC EDUCATION TOOL.
DOI: 10.5220/0003301301930198
In *Proceedings of the 3rd International Conference on Computer Supported Education* (CSEDU-2011), pages 193-198
ISBN: 978-989-8425-49-2

students outside the classroom.

In this paper, we discuss designs and implementation of the Cryptographic Education Tool, and present our teaching experience and lessons learned. In section 2 the teaching objectives will be discussed. The detail of the designs and implementation of the Cryptographic Education Tool will be presented in section 3. In section 4 functions of the tool will be exhibited. In section 5 experimental results will be discussed. The conclusions will be given in section 6.

2 OBJECTIVES

Cryptography is an import topic of Information Assurance and computer security. In order to help students effectively learn techniques of ciphers a Cryptographic Education Tool (CET) has been developed by the Department of Computer Science at NC A&T SU. The objective of this tool is to provide students with a visualization-based interactive tutorial and step by step demonstrations of ciphers, to help them better understand the concepts of cryptography, algorithms and the processes of key generation, encryption and decryption. CET can be used in cryptography, network security, and Web security courses by instructors in classroom or by students outside classroom as supplemental material.

3 DESIGNS AND IMPLEMENTATION

The principle of the design of the Cryptographic Education Tool is user friendly, visualization-based, highly interactive and easy to install. This tool will help students understand the concepts of cryptography, algorithms, the process of generating keys, and how to use these algorithms and generated keys to encrypt and decrypt messages. Several main considerations are described in the following sections.

- Visualization-based

Visualization has been used in Computer Science to help students understand algorithms and data structures for years. In CET visualization technique is used to let students interact with the tool, to view key generation step by step, and to view encryption and decryption results. This tool allows students to input initial data, to modify parameters, and to view generated keys. This tool also allows students to input plaintext, to select an algorithm, to encrypt plaintexts and to view encrypted results.

- High Interactivity

Each page of the CET supports students to interact with it. Students can select an algorithm, choose to generate keys, encrypt message or decrypt message. At any step students can click the *Help* button to read the algorithm, to view key generating steps, and to see the processes of encryption and decryption. Students can input expected encryption or decryption results. If the expected result is not right CET allows student to try again.

- Consistency of Displays

An important consideration of CET design is how long it takes students learn using this tool. CET supports three categories of ciphers: Transmission of Passwords, Secrete Key Cryptography and Public Key Cryptography. If each category has its own display format, or changes format from one view to another view, students may need more time to learn it. In this tool the same layout was used in all of three categories as shown in figure 1. The screen is divided into three parts. The first part contains selected algorithm and generated key. In this example the algorithm is SDES. The second part is encryption section. A user must input message and expected encrypted result. Clicking *Clear* button can erase all inputted information. Clicking *Check Encryption* button will first check the expected encrypted result, then display the result is correct or not. The third part is decryption section. A user can input encrypted result and expected decrypted result. Clicking *Check Decryption* button will first check the expected decrypted result, then display if the result is correct or not. The Cryptographic Education Tool was designed to be very user friendly. The tool consists of *Help, Encryption, Decryption* and *Demonstration* button. A user can click *Help* button to read the algorithm. He/she can click *Encryption* button to input the message and expected encrypted result. If the expected encrypted result is not correct the user can click *Demonstration* button to follow an example to go through the encryption process step by step.

- Platform Independent

A major consideration during implementation of the Cryptographic Education Tool is platform independence. This tool is implemented using Java language in a multi layered model. The controller layer controls user requests and the navigation flow. The service layer encapsulates the encryption logic. Java Swings Framework is used to design the pages and JFrames is used to implement the code. The Cryptographic Education Tool can run under

Windows XP/2003, Linux and UNIX operating systems. It requires Java Run Time Environment 1.4 or higher.

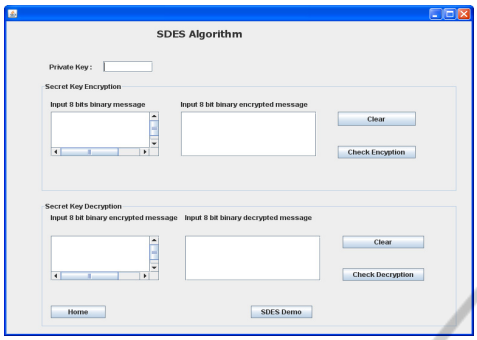

Figure 1: Basic layout.

4 FUNCTIONS OF THE CRYPTOGRAPHIC EDUCATION TOOL

The Cryptographic Education Tool implements three categories of ciphers: Transmission of Password, Secrete Key Cryptography and Public Key Cryptography. First the Cryptographic Education Tool demonstrates how these algorithms work. Secondly it lets students get hands-on experience to practice cryptography. Finally if the student cannot generate correct results it will show students how to generate the correct result step by step. To use this tool, a user must first access the homepage. The homepage is the Introduction that briefly describes the three categories. The homepage also contains three links as shown in Figure 2. These links are Transmission of Password, Secret Key Cryptography and Public Key Cryptography. Each link brings users to the corresponding category that consists of demonstration, encryption and decryption. Each category also has *Encryption, Decryption, Previous, Clear* and *Demonstration* function buttons.

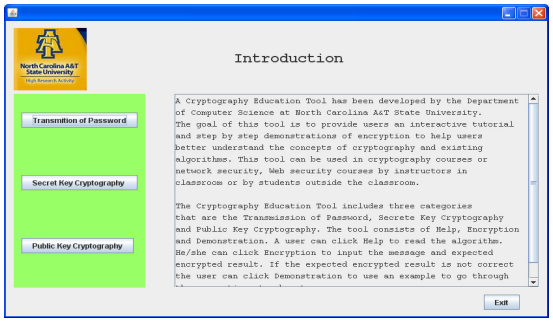

Figure 2: The homepage.

4.1 Transmission of Password

Transmission of Password demonstrates the concepts of classical encryption. It consists of two algorithms that are change case and simple cipher. The change case algorithm changes an input capital letter into an output lower case letter and an input lower case letter into an output capital letter. The simple cipher algorithm substitutes characters in the input plaintext according to the given table to produce the output ciphertext (Bishop, 2005). Encrypting a user ID and password is one of applications of these algorithms. Figure 3 is a snapshot of Change Case algorithm. A user inputs user ID *Anna* and password *test*, and expected encrypted user ID *aNNA* and password *TEST*. By clicking Check *Encryption* button the message "Encryption was successful" is displayed on the screen.

4.2 Secret Key Encryption

Secrete Key Cryptography is referred to as single-key encryption or symmetric encryption. A secrete key is shared between communication peers, and the key is used to encrypt and decrypt the messages on either side. There are two categories of secrete key cryptosystems that are block ciphers and stream ciphers. The Encryption Education Tool uses Simplified Data Encryption Standard (SDES) to demonstrate how a block cipher works (Perry). Data Encryption Standard (DES) is a block cipher algorithm that can be used to encrypt or decrypt blocks of data consisting of 64 bits using a 64-bit key. The key 56-bit – the last bits of each of the 8 bytes in the key is a parity bit for the byte. Simplified Data Encryption Standard is an educational encryption algorithm. It has similar properties and structure to DES with much smaller parameters. SDES takes an 8-bit block of plaintext and a 10-bit key as input and produces an 8-bit block of ciphertext as output. It invokes 2 rounds of permutations, swaps, and substitutes. Demonstration, encryption and decryption using SDES are implemented. The SDES demonstration page contains two demonstrations that are key generation and encryption as in figure 4. In the key generation demonstration a user must input a 10-bit binary number as the initial key, then input expected results of initial permutation, expected results of distinct selection and shift to generate key 1 and key 2. Figure 4 is a snapshot of demonstration how using SDES. In the encryption demonstration a user must input an 8-bit binary number and use generated keys to encrypt the binary message. The demonstration

shows the processes of key generation and encryption step by step. Figure 5 is a snapshot of using SDES to encrypt and decrypt messages. In the encryption a user must input a 10-bit key, an 8-bit binary message and expected encrypted output. Then clicks *Encrypt* button to check the data that the user inputted are correct or not. A user can also input an encrypted 8-bit binary message and expected decrypted output, then click *Check Decryption* button to check the result. Figure 5 shows the details of encryption and decryption.

4.3 Public Key Cryptography

Public key cryptography is referred to as asymmetric cryptography. A user has a pair of mathematically related keys that are a public key and a private key. A public key can be published. A private key can never leave the possession of its owner. A user sends a secret message that was simply encrypted with the recipient's public key. The recipient can decipher it using his private key. Public key cryptography has been used in various areas. Ronald Rivest, Adi Shanir and Leonard Adleman (RSA) algorithm is a public key algorithm and has been used for key exchange, digital signature and encryption of small blocks of data (Bellars and Rogaway, 1994, Bishop, 2005). RSA uses a variable size encryption block and a variable size key.

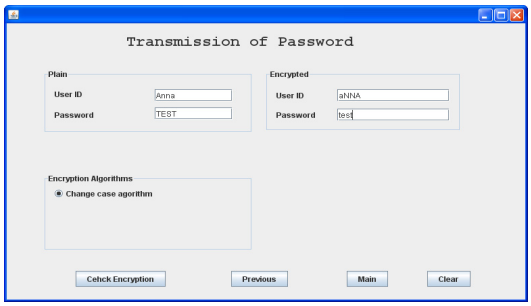

Figure 3: An application example of change case algorithm.

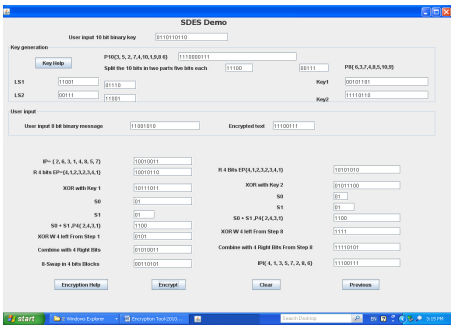

Figure 4: A demonstration of using SDES.

The public key cryptography demonstration consists of two parts that are key generation, and message encryption and decryption. Students must understand how the RSA algorithm works. The demonstration page allows a student to input two prime numbers P and Q, and to choose an integer e. The user clicks *Generate Key* button. If input numbers are not right the tool will display which number is not valid and will allow the user to try again. If all input numbers are correct it will display private and public key pairs as in figure 6. The public key is (33, 17) and the private key is (33, 13). Students can use generated keys to encryption messages that can be ASCII code or decimal code. For example a user selects that the input format is decimal. The user inputs decimal number 5 and expected encrypted result is 14. The user clicks *Check Encryption* button. If the expected result is correct the tool displays "Your answer was correct" as in figure 7. Otherwise it displays "The encrypted message was wrong". The user can try again.

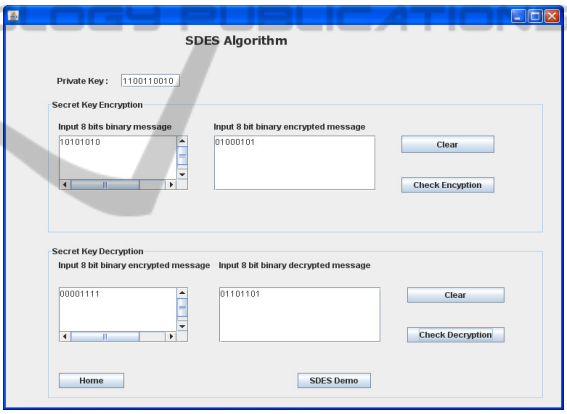

Figure 5: Using SDES to encrypt and decrypt messages.

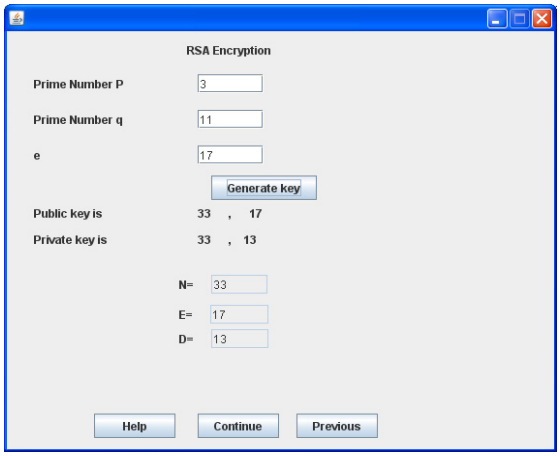

Figure 6: Use RSA to generate keys.

5 EXPERIMENTAL RESULTS

We have successfully used the Encryption Education Tool in COMP 621 Web Security class in the Department of Computer Science at NC A&T SU in Spring 2010 and received excellent results. First we demonstrated the tool in the classroom when we taught Cryptographic Techniques. When we taught cryptographic hash functions we showed students how to use this tool to implement simple user ID and password encryption by using *Transmission of Password*. After we explained how DES algorithm works we demonstred how the CET implements the SDES algorithm in *Secret Key Cryptography*, and required students to practice generating keys step by step. Students used these keys to encrypt a message. Students were required to read the RSA algorithm, to use the CET to genereste private and public keys, and to encrypte messages using generated keys.

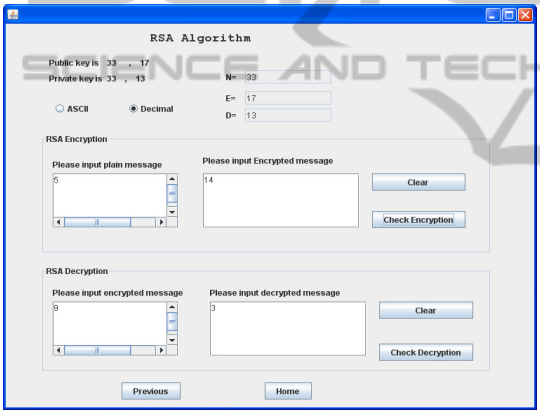

Figure 7: Use RSA to encrypting a message.

Forteen students took the Web Security class. Four of them were undergraduate seniors. Ten of them were graduate students. Students were very excited to use the Cryptographic Education Tool to pactice the processes of key generation, encrypting and decrypting messages. To evaluate students' reactions and get feedback a survey was conducted at the end of spring 2010 semester. This survey was in addition to standard university course evaluation. The survey consisted of three-groups of questions. The questions in the first group reflected knowledge after students attended the lectures of encryption classes and used the Encryption Educational Tool. Six questions were presented that were 1) understanding the Simple Cipher algorithm, 2) understand the Substitution algorithm, 3) knowledge of the Simple Data Encryption Standard, 4) understand RC4 algorithm, 5) understand RSA algorithm, and 6) identify the difference between secrete key and public key encryptographics. Students could select very low, low, medium, high and very high. All students attended the survey. The results are displayed in figure 8. For all questions no students selected "very low". The questions in the second group were general questions. These questions were 7) the demonstration examples are helpful, 8) the graphic interface is user friendly, and 9) the encryption education tool is practical and helps understand encryption algorithms. Students could select Strongly Agree, Agree, Neither Agree or Disagree, Disagree, or Strongly Disagree. 100% students selected agree or strongly agree for all questions. Questions in the third group were 10) what did you like best about the tool, 11) what did you like least about the tool, and 12) comments. All students liked this tool because it is very friendly and is easy to understand, install and use. Several students commented "It is very simple to install the Cryptographic Education Tool" "It is a very user-friendly tool" "Users not only understand the concept of algorithms but also he/she can practice by self using th Cryptographic Education Tool" "There are helpful buttons and popup guides that assist students when an incorrect input is given", etc.

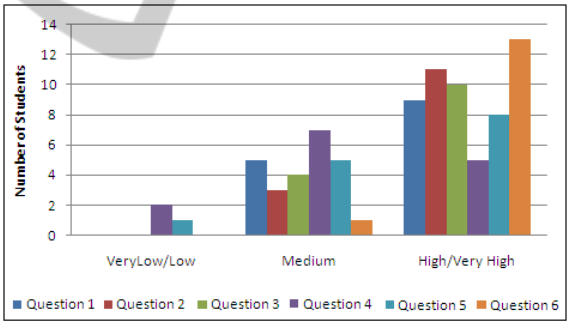

Figure 8: Results of students survey.

6 CONCLUSIONS

We designed and implemented a Cryptographic Education Tool that provides a visualization-based interactive tutorial, step by step demonstrations of key generation, encryption and decryption. Students can use the CET to select an algorithm, to generate keys, and to encrypt and decrypt messages. This tool helps students better understand the concepts of cryptography and algorithms, practice processes of key generation, encrypting and decrypting messages. This tool demonstrates how change case, simple cipher, RSA and SDES work, and guides students

step by step to generate encryption keys and uses generated keys to encrypt messages.

We used the Encryption Education Tool in COMP 621 Web Security course for undergraduate seniors and graduate students in Spring 2010. Students' survey and feedback reflected that this it was a very friendly, helpful and easy to use tool. By using this tool students can quickly learn and practice ciphers, and get hands-on experiences. This Encryption Education Tool can be used in any classes involving cryptography techniques.

ACKNOWLEDGEMENTS

This work was partially supported by National Science Foundation under the award number DUE-0830686.

REFERENCES

Bellare, M. and Rogaway, P., 1994, Optimal Asymmetric Encryption – How to Encrypt with RSA, *Proceeding of Eurocrypt.*

Bishop, M., 2005, Introduction to Computer Security, *Addison-Wesley Pearson Education*.

Cocks, C., November 1973, A Note on Non-Secret Encryption, *CESG report*.

Khambari, M., Othman, M., Motsida, M. and Abdollah, M., 2009, A Novel Approach on Teaching Network Security for ICT Courses, *Proceedings of IEEE Int. Conf. on Engineering Education*.

Perry, R., SDES, Available at: <http://homepage.smc.edu/morgan_david/vpn/website-perry-sdes/all-sdes.html> (Accessed 1 October 2010).

Schweitzer, D. and Baird, L., 2006, The Design and Use of Interactive Visualization Applets for Teaching Ciphers, *Proceedings of the 2006 IEEE Workshop on Information Assurance*.

Stallings, W., 2006, Cryptography and Network Security Principles and practices, Fourth edition, Publishing *House of Electronics Industry*.

Yang, F., Zhong, C., Yin, M. and Huang, Y., 2009, Teaching Cryptology Course Based-on Theory-Algorithm-Practice-Application Mode*, Proceedings of IEEE First Workshop on Education Technology and Computer Science*.