International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Crypto View: Visual Representation of Cryptographic Algorithms

Surumi Basheer[1], Sreena Sreedhar[2]

[1]Computer Science and Engineering, ICET, Muvattupuzha, India

[2]Assistant Professor, Information Technology, ICET, Muvattupuzha, India

Abstract: ***Cryptography is a fundamental topic in an information assurance curriculum. Educational software systems have an increasingly significant presence in engineering sciences. They aim to improve students' attitudes and knowledge acquisition typically through visual representation. This paper presents a software solution for Crypto View: Visual Representation of Cryptographic Algorithms, which was developed to support a Data Security course at the School of engineering level. The system allows users to follow the execution of several complex algorithms (DES, AES, RSA, and Diffie-Hellman, Vigenere cipher and Symmetro-Asymmetro) on real world examples in a step by step detailed view with the possibility of forward and backward navigation. It also provides the analysis of these algorithms by calculating the computation time and efficiency. Benefits of the Crypto View system for students, it help them to understand the complex algorithms in a simplified manner and that facilitate the students to reduce their fear to attempt the exams.***

Keywords: AES, algorithm visualization, cryptographic algorithms, data security, DES, Diffie-Hellman, RSA, *Vigenere cipher ,Symmetro-Asymmetro*

1. Introduction

IN the modern e-world era security and reliability of e-services are of the utmost importance. Now day's people live their entire life, both private and professional, online. This would not be possible without complete trust in e-services that are in use. Confidentiality and authentication are the two services that became indispensable in the everyday use of Internet. Therefore many schools that teach computer engineering worldwide have supplemented their curriculums with courses in this area. Cryptographic algorithms are one of the crucial parts of the course, since the confidentiality and authentication services are achieved by using various combinations of different cryptographic algorithms. In previous years we have analyzed exam results from the Data Security course and noticed that students had trouble understanding cryptographic algorithms, which resulted in lower grades on the part of the exam covering. This area and consequently the final grades for the exam. The reason for this was the difficulty for students to closely follow the execution of algorithms, because they are too complex to be calculated manually on paper. In order to help students to better understand the material many teachers in different areas use educational software systems. These systems have a significant presence in engineering sciences, where it is important for students to have practical work in addition to classes. The software system is designed to support laboratory exercises, which cover complex cryptographic algorithms that caused most of the problems for students. Supported algorithms are: Data Encryption Standard (DES), Advanced Encryption Standard (AES), RSA, and Diffie-Hellman. We have developed a system for CryptOgraphic Algorithm and designed the related laboratory exercises that make use of the Crypto View System.

The system aims to enable students to study the various complex algorithms covered by the course in a user-friendly, visual, and interactive environment. For every algorithm that is supported, the system is able to visually represent complete execution with the possibility of navigating forward and backward through the execution, obtaining intermediate results for every operation of the algorithm, and presenting details of every operation in the algorithm. The laboratory exercises intend to enable students to execute complex algorithms quickly on real examples, where manual execution on paper would be time consuming, and to help them learn details and notice important attributes of these algorithms. The Crypto View system and experiences from using it in the Data Security course are presented in this paper.

1.1 Contributions

- Present a novel software system for visual representation of Cryptographic algorithms.
- Create step by step execution of common algorithms such as AES, DES, Deffie-Hellman, RSA, Vigenere Cipher and Symmetro-Asymmetro.
- Also provide the choice to users to use any of these algorithms for encrypt and decrypt data.
- The Crypto View systems provide the detailed analysis of computation.

2. Related Work

2.1 The ANIMAL Algorithm Animation Tool

In this paper, present ANIMAL, a new tool for developing animations to be used in lectures. ANIMAL offers a small but powerful set of graphical operators. Animations are generated using a visual editor, by scripting or via API calls. All animations can be edited visually. ANIMAL supports source and pseudo code inclusion and highlighting as well as precise user-dined delays between actions. The paper evaluates the functionality of ANIMAL in comparison to other animation tools.

In order to improve the quality of teaching, many educators have become interested in using animations in their courses. This is especially true for dynamic behaviour that is often hard to explain using slides or blackboards. In computer science education, the main focus of animation tools available for this purpose is the animation of algorithms and data structures. ANIMAL avoids many of the shortcomings of other animation tools. It offers a set of powerful features to create, modify and display animations in a simple manner without being limited to specific topics. Due to its flexibility, usage is not limited to these areas. Animal's visual editor can easily be used by laypersons to generate and edit animations.

2.2 The Design and Use of Interactive Visualization Applets for Teaching Ciphers

Cryptography is a fundamental topic in an information assurance curriculum. Students should understand the basic concepts and weaknesses of both historical and current cipher algorithms. Visualization tools can help students understand these concepts, both in the classroom and as out-of-class exercises. This paper describes a set of such tools designed for a Cryptography Course at the United States Air Force Academy. The design goals, implementation details, and classroom experiences are addressed. As a result of this emphasis on security education, a greater number of courses And programs are being offered at the undergraduate level in security-related topics such as cryptography, information security, network security, and information warfare. These courses have benefited from an increasing number of textbooks, curriculum development, and student competitions such as the Cyber Defence Exercise. These educational resources provide a solid foundation for developing a series of courses in information assurance education. The cipher visualization tools described in this paper are part of a suite of visualization tools for security education being developed at the Air Force Academy known as VISE (Visualization for Information Security Education). The purpose of VISE is to provide a set of education visualizations for teaching undergraduate information security classes. The tools cover common security topics such as cryptography.

2.3 Active Learning in the Security Classroom

Information assurance is a critical topic in undergraduate education and has received a lot of attention in recent literature. At the United States Air Force Academy, the paper has taught multiple security courses for several years and has tried different approaches to make the material interesting and meaningful to the students. One approach that has proven effective is the application of active learning techniques. Now developed interactive visualization tools for in-class use, designed hands on laboratories, created an inter-school assessment competition, and employed active learning activities in the classroom. All of these techniques are designed to engage the student in the learning process;
to develop a deeper understanding of security concepts; and to act as a motivational tool. The paper will describe the different tools and techniques used and how they into an active learning approach. And present experience with using the tools, their effectiveness, and student reactions. Many educators advocate active learning techniques as contrasted to traditional lecture-based teaching in which the primary student role in the classroom is passive listening. Ideally active learning techniques supplement rather than replace lecturing.

2.4 A Meta-Study of Algorithm Visualization Effectiveness

Algorithm visualization (AV) technology graphically illustrates how algorithms work. Despite the intuitive appeal of the technology, it has failed to catch on in mainstream computer science education. Some have attributed this failure to the mixed results of experimental studies designed to substantiate AV technologies educational effectiveness. However, while several integrative reviews of AV technology have appeared, none has focused specially on the software's electiveness by analyzing this body of experimental studies as a whole. In order to better understand the effectiveness of AV technology, We present a systematic meta-study of 24 experimental studies. The paper pursue two separate analyses: an analysis of independent variables, in which we tie each study to a particular guiding learning theory in an attempt to determine which guiding theory has had the most predictive success; and an analysis of dependent variables, which enables us to determine which measurement techniques have been most sensitive to the learning benefits of AV technology.

In this article, presented an integrative review of empirical studies of algorithm visualization effectiveness, in order to uncover trends in the research that might help us better understand how and why AV technologies effective.

3. Key Crypto View Design issues

Crypto View system is designed to be at the responding level of engagement, which means that students are answering questions concerning the visualization presented by the system. Previously our students were at the no viewing engagement level, since no visualization tool was used. In order to have high interactivity, the Crypto View system was designed to enable students to control the execution of algorithms forward and backward, it allows them to configure the algorithm parameters before starting an execution, and it makes it possible for them to follow the result of every operation in any time. Abstractions used to present concepts are quite intuitive and thus easy to understand. The Crypto system include AES, DES, RSA, Diffie-helman,Vigenere cipher, Symmetro-Asymmetro Algorithms.

3.1 AES and DES Implementation

DES and AES are both symmetric block algorithms that Operate with data in several iterations before producing ciphertext. The DES algorithm consists of the initial permutation, 16 identical iterations, 32-bit swap and inverse of the initial permutation. Each iteration in the DES algorithm starts by the expansion permutation which permutes and extends the right 32 bits to 48 bits in order to match the size of a round key. This expanded value is XORed with the round key for that iteration and the result is reduced to 32 bits using the substitution. After the

substitution, the value is permuted once again, this time without the changes in the size, and XORed with the left 32 bits in order to make the right 32 bits for the next iteration. The left 32 bits for the next iteration are the right 32 bits from the current iteration. The iteration key creation includes an initial permutation of the original key and a left circular shift and a permutation in each iteration to create a 48-bit iteration key.

The AES algorithm consists of the initial XOR with the original key, nine identical iterations and the incomplete final iteration. Each iteration in the AES algorithm starts with the substitute bytes operation, which substitutes each byte of the state with a byte determined by a specially designed substitution matrix. The iteration continues with the shift rows operation, which performs a byte circular left shift on each row of the state matrix. The mix columns operation is next for all iterations except the last one, which does not have this operation. The mix columns operation makes that each byte in a column is calculated based on all four bytes in that column. Each iteration finishes with a simple XOR of the state matrix with the iteration key. Iteration keys are created by using the expansion function on the original key.

3.2 Diffie-Hellman and RSA Implimentation

Diffie-Hellman and RSA are both asymmetric public key cryptography algorithms. The key difference between them is that Diffie-Hellman can be used only for key exchange between two users, while RSA can be used for encryption and decryption of data. Even though these algorithms are not the same it was still possible to create a uniform visual representation for them. The Diffie-Hellman algorithm enables two users to securely exchange a secret value. First, global public elements must be defined (prime number q and its primitive root a). Then each user selects a private value X which is less than q, and calculates a public value Y as aX mod q, using the previously selected private value. Public values are then exchanged by the users. At the end, each user calculates a common secret value by himself using the formula K ¼ Y X mod q, where X is his private value and Y is the public value obtained from the other user.

The RSA algorithm starts with the key generation process. At the beginning of this process two large prime numbers (p,q) are selected and multiplied to form n. Next, the Euler's totient function for n ($\phi(n)$) is calculated. Then integer e is selected and it must fulfil the following conditions: $gcd(\phi(n),e)=1$ and $1 < e < \phi(n)$. After that integer d is calculated based on a formula $d = e^{-1} \bmod (\phi(n))$.Finally, the public key is created as {e, n} and the private key is created as {d, n}. Encryption of a message M, which must be less than n, is done using public key and formula $M^e \bmod n$. Decryption of a message C, which must be less than n is done using private key and formula $C^d \bmod n$.

3.3VigenerecipherandSymmetro-Asymmetro implementation

In our work The Vigenère cipher is a method of encrypting alphabetic text by using a series of different Caesar ciphers based on the letters of a keyword. It is a simple form of polyalphabetic substitution. The Vigenère cipher has been reinvented many times. The method was originally described by Giovan Battista Bellaso in his 1553 book La cifra del. Sig. Giovan Battista Bellaso; however, the scheme was later misattributed to Blaise de Vigenère in the 19th century, and is now widely known as the "Vigenère cipher".

Symmetric encryption uses a secret key value to encrypt and decrypt the data. Both the sender and receiver need the same key in order to encrypt or decrypt. There are two types of symmetric algorithms, stream algorithms and block algorithms. The stream algorithms work on one bit or byte at a time, whereas the block algorithms work on larger blocks of data (typically 64 bits). The drawback to this type of system is that if the key is discovered, all messages can be decrypted.

Asymmetric encryption uses a separate key for encryption and decryption. The decryption key is very hard to derive from the encryption key. The encryption key is public so that anyone can encrypt a message. However, the decryption key is private, so that only the receiver is able to decrypt the message. It is common to set up "key-pairs" within a network so that each user has a public and private key. The public key is made available to everyone so that they can send messages, but the private key is only made available to the person it belongs to.

If we want the benefits of both types of encryption algorithms, the general idea is to create a random symmetric key to encrypt the data, and then encrypt that key asymmetrically. Once the key is asymmetrically encrypted, we add it to the encrypted message. The receiver gets the key, decrypts it with their private key, and uses it to decrypt the message.

4. Conclusion

In this paper we have described the novel Crypto View system for visual representation of the cryptographic algorithms. The software system is designed to support the complex cryptography algorithms like: DES, AES, RSA and Diffie-Hellman, vigenere cipher, Symmetro-Asymmetro Algorithms that are taught in the course. The main goal of the introduction of the Crypto View system in the Data Security course was to help students to better understand the algorithms taught in the course and to help them prepare for the exam. , also the users can securely store their data using any of these algorithms and done an analysis to algorithms by calculating the computation time and efficency.

5. Acknowledgment

The Author would like to thank Sreena Sreedhar Assistant Professor, Department of Information Technology, Ilahia College of Engineering and Technology, Muvattupuzha for her moral and technical support.

References

[1] Tao, J. Ma, J. Mayo, C. K. Shene, and M. Keranen, DESvisual: A visualizationtool for the DES cipher, J.Comput. Sci. Colleges, vol. 27, no. 1, pp. 8189, 2011

[2] C. A. Shaff er, M. L. Cooper, A. J. D. Alon, M. Akbar, M.Stewart, S. Ponce,and S. H. Edwards, Algorithm visualization: The state of the _eld, ACM Trans. Comput. Educ., vol. 10, no. 3, article 9, pp. 122, Aug. 2010.
[3] D. Schweitzer, D. Gibson, and M. Collins, Active learning in the security classroom, in Proc. IEEE 42nd Hawaii Int. Conf. Syst. Sci., Jan. 2009, pp. 18.
[4] D. Schweitzer and W. Brown, Interactive visualization for the active learning classroom, ACM SIGCSE Bull., vol. 39, no. 1, pp. 208212, Mar. 2007.
[5] D. Schweitzer and L. Baird, The design and use of interactive visualization applets for teaching ciphers, in Proc. IEEE Inf. Assurance Workshop, Jun. 2006, pp. 6975.
[6] C. D. Hundhausen, S. A. Douglas, and J. T. Stasko, A meta-study of algorithm visualization e_ectiveness, J. Vis. Languages Comput., vol. 13, no. 3, pp. 259290,Jun. 2002.
[7] G. Roling, M. Schuer, and B. Freisleben, The ANIMAL algorithm animation tool, ACM SIGCSE Bull., vol. 32, no. 3, pp. 37 40, Jul. 2000.

Author Profile

Surumi Basheer received the Bachelor of Technology degree in Information Technology from Mahatma Gandhi University, Kerala. She is currently doing Master of Technology degree in Computer Science and Engineering with Specialization in Information Systems from Mahatma Gandhi University, Kerala.

Sreena Sreedhar She is currently assistant professor at ICET, Muvattupuzha, Mahatma Gandhi University, Kerala.