Proceedings of the 4th International Conference on
Information Technology and Multimedia at UNITEN (ICIMU' 2008), Malaysia
17th – 19th November 2008

Algorithm Animation of LOKI97, MARS, Pseudo-Hadamard Transform and Latin Square

[1]Sapiee Haji Jamel, [2]Nurulashikin Saidin, [3]Ahmad Fathihalil Mohamed Hasan, [4]Ahmad Naqiyuddin Mahdzir and [5]Nurzahanim Zainol
Faculty of Information Technology and Multimedia,
Universiti Tun Hussein Onn Malaysia (UTHM),
86400 Parit Raja, Batu Pahat JOHOR.
E-mail : [1]sapiee@uthm.edu.my , [2]nurulashikin08@yahoo.com, [3]afhalil@gmail.com, [4]naqiyuddin@gmail.com, [5]hanimz_85@yahoo.com

Abstract

Cryptographic algorithms are used to protect the confidentiality and integrity of information or data from unintended parties. The process to understand these cryptographic algorithms requires students to read through academic papers or technical reports which mainly consist of mathematical formulations as their building blocks. The availability of various multimedia tools can be used to create a more interesting and fun learning process. In this paper, we use Macromedia Flash 8 to create an algorithm animation for LOKI97, MARS, Pseudo- Hadamard Transform (PHT) and Latin Square. Furthermore, the use of algorithm animation with multimedia element can be adopted by students as an extra tool to easily understand the concept and some applications behind each cryptographic algorithm.

1. Introduction

An algorithm animation is a technique that combines multimedia tools with other disciplines to simulate how specific algorithm or process work. It offers an alternative method for better understanding of complicated process with a help of computer software [1,2]. In this paper, we developed algorithm animation for two cryptographic algorithms and two cryptographic transformations.

Our main motivation for developing these algorithm animations is to increase the number of available algorithm animations for our students enrolling in Computer Security Subject. Algorithm animations help our students to understand the complicated algorithms. Some of the examples of algorithm animations are Rijndael [5] and Twofish [9].

The rest of the paper is organized as follows. Section 2 describes the overview of cryptographic algorithm and transformation. Section 3 discusses the algorithm animation for LOKI97, MARS, PHT and Latin Square and Section 4 gives the conclusion and future work of this research.

2. Overview of Cryptographic Algorithm and Transformation

LOKI97 [8] and MARS [4] algorithms are two of the candidates from an Advanced Encryption Standard competition (AES) in 1997. Even though these two algorithms were not chosen as the winner, each design element was unique and may be useful for future cryptographic algorithm development. MARS designers always select security as their main goal as compared with speed in the encryption and decryption process. Transforming each of these algorithms description into an animation hopefully will enlighten the process of understanding its complex algorithm.

Pseudo-Hadamard Transform (PHT) and Latin Square are two techniques used as an input mixing function for cryptographic algorithm such as Twofish [3] and Ritter Cipher [10].

The next sub-sections will briefly describe LOKI97, MARS, PHT and Latin Square.

2.1. LOKI97

LOKI97 is an advancement of LOKI91 with the additional improvement on the key schedule algorithm [8]. This cryptographic algorithm used 256-bit key and set standard input and output block of 128-bit. LOKI97 adopted Feistel structure as its building block design where input bit (plaintext) are modified using a complex non-linear f-function to create a random

output (ciphertext). The uses of Feistel structure (self inverting structure) avoid the need for using inverse in the confusion and diffusion transformations.

The total number of round in this algorithm is 16 to ensure that the ciphertext is appeared random in order to safeguard it from attack by cryptanalysts. In each round, two 64-bit subkeys are added to the right half of the 128-bit block. Its value, after the first subkey is added, is used as the input to the f-function for that round. A third 64-bit subkey is used as an input to the f-function; it is not directly added or XORed to the right half of the block or a transformed version of it, but instead controls the f-function's nonlinearity.

For purposes of the key schedule, this 64-bit subkey is the second one; the two added to the right half are the first and third, respectively. The output of the f-function is, as in Data Encryption Standard (DES), Exclusive-OR (XORed) to the left half of the block [5]. All these process and steps are transformed into algorithm animation as described in Section 2.1.

2.2. MARS

MARS algorithm was developed by IBM as part of AES candidates similar to LOKI97 [4]. MARS developer adopted different design philosophy where security always comes before the algorithm performance. Unlike other candidates in the AES competition, this algorithm can take longer keys (up to 400-bit). MARS algorithm consists of two layers of mixing function which sandwich the main cryptographic core.

The developer of MARS integrates several design technique to ensure that it will withstand known shortcut attacks. The only short coming of this style is the processing time will increase significantly as compared with other algorithm such as LOKI97.

Similar to LOKI97, MARS cryptographic core uses 16 iteration for data encryption and decryption, 8 rounds of preprocessing before entering cryptographic core and 8 rounds after it. MARS users have the option to turn off this 16 rounds iteration and only use the cryptographic core.

2.3. Pseudo-Hadamard Transform (PHT)

Pseudo-Hadamard Transform was named after French mathematician Jacques Solomon Hadamard [11]. PHT is an input mixing function for two equal length bit data of size (n) to provide diffusive function for cryptographic algorithm. Diffusive function plays an important role in any cryptographic algorithm to ensure that all ciphertext depends on all of the plaintext. Any small changes to the plaintext will result in devastating changes in the ciphertext. Hence, make it difficult for an attacker to predict the original message encrypted using the cryptographic algorithm without the original key. Given two input a and b of n bits, the n-bit PHT is defined as:

$$a' = a + b \bmod 2^n \qquad (1)$$
$$b' = a + 2b \bmod 2^n$$

and the reverse of a' and b' is defined as

$$b = b' - a' \bmod 2^n \qquad (2)$$
$$a = 2a' - b' \bmod 2^n$$

This transformation is used as one of the diffusion function in Twofish [3] and SAFER+ [7] encryption algorithms.

2.4. Latin Square

Latin Square was introduced by Leonhard Euler [9]. Euler defined Latin Square and represented it as matrix which consists of n rows and n columns where n is a natural number ($1..n$). Two n-by-n Latin Square can be used to create Orthogonal Latin Square of order n (Latin Square with n different elements). Ritter Cipher used Latin Square concept as the foundation for the input mixing function [10].

3. Algorithm Animation

The major part of this research is dedicated to understanding of each algorithm and transformation before it can be translated into animation. This section will highlight algorithm animations for LOKI97, MARS, PHT and Latin Square using screen snapshots. By going through each of this algorithm animation, student can anticipate the overall process of each algorithm and transformation.

Figure 1 for example, shows the LOKI97 interface. The algorithm animation is divided into 3 parts: Introduction to basic cryptographic algorithm concept, the inventor of LOKI97 and The Family of LOKI's. The user of this algorithm animation can choose to have the narration switch on or off.

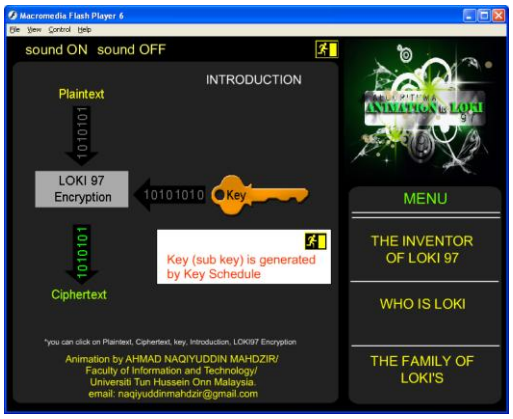

Figure 1. LOKI97 Main Interface

Clicking on some the object on the screen (for example, the key) will result in popup note displayed about this item. Similarly, selecting the Inventor of LOKI97 Menu, the information about all the team members who developed this algorithm will be displayed once the user of this animation click on any of the team members photograph as shown in Figure 2.

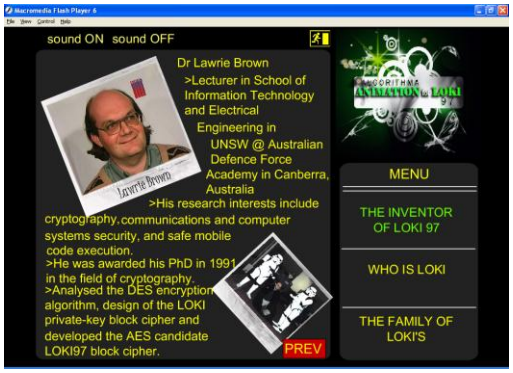

Figure 2. One of LOKI97 Inventor

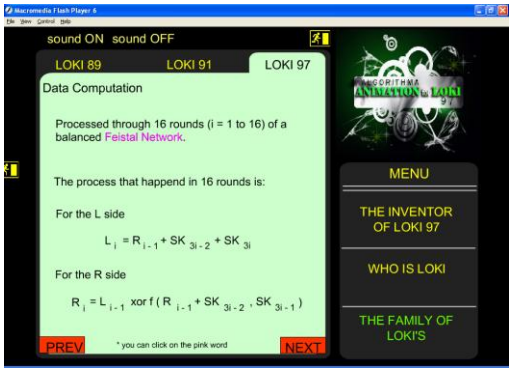

Figure 3. Animation of Data Computation

Exploring into the main part of this algorithm animation will allow students to understand more about how this algorithm worked. As shown in Figure 3, the operation on Data Computation is executed step-by-step to ensure that it is clearly understood by students using this animation.

This approach hopefully will provide alternative for students who are interested to know more about this algorithm.

Figure 4 shows the animationof MARS. MARS algorithm animation shows the overall process in this algorithm. Complicated structure of this algorithm which is only written in technical papers can be easily converted into a livelier format.

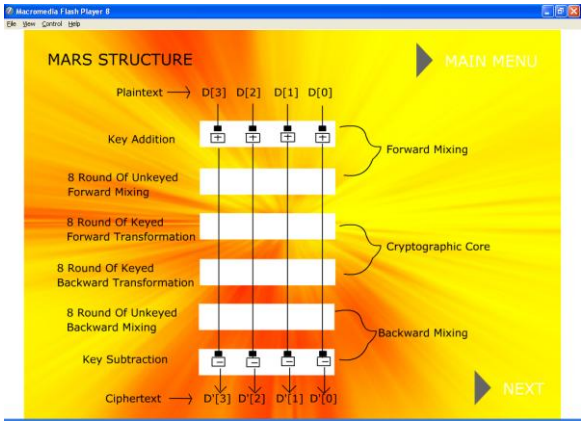

Figure 4. Animation of MARS

Each part of this algorithm is elaborated using animation technique as shown in Figure 5.

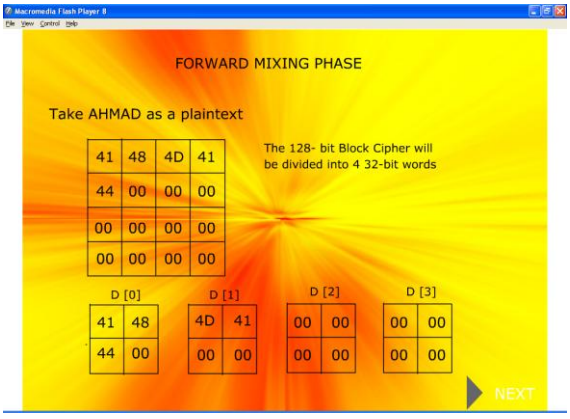

Figure 5. Forward Mixing Phase

Figure 6 shows the Pseudo-Hadamard Transformation (PHT) interface. Adopting different style and approach, PHT animation offers students with a basic definition and elements required to

understand the application of PHT as shown in Figure 6.

Figure 6. PHT Main Interface

Short history about the inventor of this transformation is added to the animation so that student can appreciate the work of our earlier mathematician.

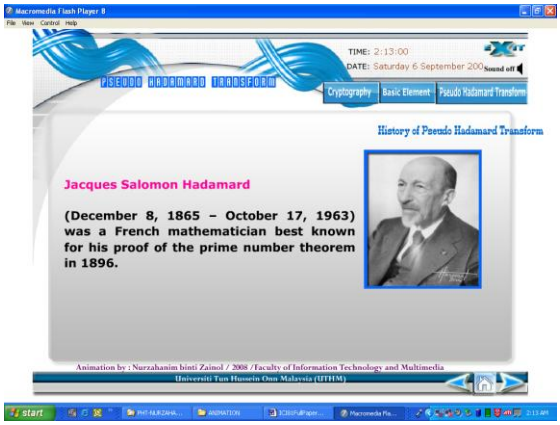

Figure 7. The Inventor of PHT

The application of this transformation in Twofish as an example is also included in this animation. This approach is to ensure students understand how PHT is applied within cryptographic algorithm. Figure 8 shows PHT is applied after Maximum Distance Separable (MDS) transformation as part of Twofish diffusion process.

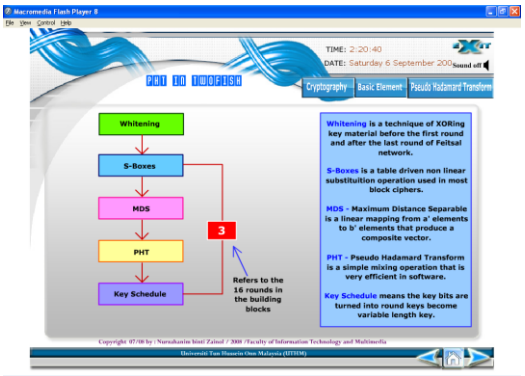

Figure 8. Application of PHT in Twofish Algorithm

Figure 9, on the other hand, shows the Latin Square animation. In this animation, the basic concept of Latin Square (LS) is defined and extended into LS of order 2, 3 and 4. Mixture of LS to create Orthogonal LSs are also available in this animation. Figure 9 shows all the possible permutations for Latin Square of order 3.

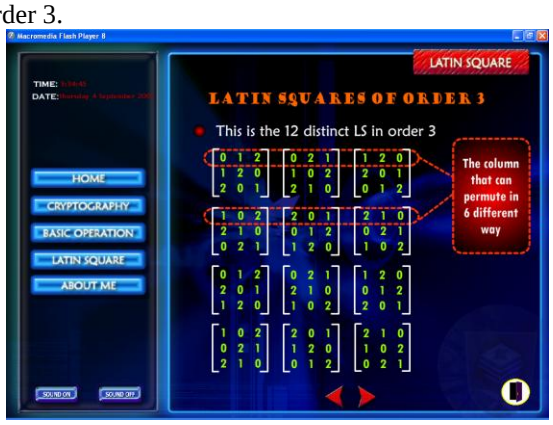

Figure 9. Permutation of LS of Order 3

Latin Square of order 4 (Figure 10) will generate 576 different distinct Latin Squares.

Figure 10. Permutation of LS of order 4

Orthogonal Latin Square which is a combination of two Latin Squares (Figure 11) can be used as input mixing approach for plaintext as used in Ritter Cipher.

Figure 11. Generation of Orthogonal Latin Square

4. Conclusion and Future Work

This paper has discussed the animation of two cryptographic algorithms and two cryptographic transformations. This animation is developed using Macromedia Flash 8. It helps the students to better understand complicated algorithms and transformations. Future work of this research will involve expansion of mathematical details of each animation and add more interactive features to this animation.

5. References

[1] Animation 2007. *Introduction to Algorithm Animation,*URL: http://www.ickn.org/elements/hyper/cyb105.htm, 2007. (Accessed on 2 February 2007)

[2] B. A Price., I. S Small. and Baecker M.,. *A Taxonomy of Software Visualization*, Proceedings of the Twenty-Fifth Hawaii International Conference on System Sciences, 1992.

[3] B. Schneier, J Kelsey, D. Whiting, D. Wagner, C. Hall and N. Ferguson, *The Twofish Encryption Algorithm*, John Wiley and Sons, New York. 1999.

[4] C. Burwick, D. Coppersmith, E. A'vignon, *MARS – A Candidate Cipher for AES*, http://www.research.ibm.com/security/ mars.pdf (Accessed On 2 January 2008).

[5] E. Zabala, *Rijndael Cipher: 128-bit Version Data Block and Key Encryption*, ORT Uruguay University, Montevideo. Uruguay, 2004.

[6] J. G. Savard, *A Cryptographic Compendium*, http://www.quadibloc.com/crypto/jscrypt.htm ,1999. (Accessed On 19 September 2007)

[7] J.L. Massey, On the Optimality of SAFER+Diffusion, Cylink Corporation, Sunnyvale, CA, USA, 1999.

[8] L. Brown, *Design of LOKI97*, URL:http://www.unsw.adfa.edu.au/~lpb/papers/ssp97/loki97 b.html , 1998.(Accessed 19 September 2007).

[9] S. Jamel, S. N. B. Musfafa and S. M. Zainal Azizan, *A Fun Way of Learning Mathematical Applications in Cryptography*, National Seminar on Applied Sciences and Mathematics (SKASM), UTHM, 2007.

[10] T. Ritter, *Ciphers by Ritter*, URL:http://www.ciphersbyritter.com/ (Accessed On 2 January 2008).

[11] Wikipedia Page, URL:http://en.wikipedia.org/ (Accessed On 2 January 2008).