Proceedings

of The Third International Conference on
Mathematics and Natural Sciences

(ICMNS 2010)

SCIENCE FOR SUSTAINABLE DEVELOPMENT

ITB, Bandung, Indonesia, 23-25 November 2010

90 Tahun Pendidikan Tinggi Teknik Di Indonesia

ISBN : 978-979-17090-3-3

SECOND LEVEL PASSWORD GENERATOR

Tay Choo Chuan, Hamzah Sakidin, Nanna Suryana Herman, Mohd Rizuan Baharon

Faculty of Electrical Engineering, Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka

Abstract. Password gives user access to the university computing services. Every time the user connects, he or she must provide the magic word; he must prove he is who he says he is. The intruder with the necessary knowledge, experience, and tools gains entry to a system, he or she may be able to monitor other machines and systems on the same network and capture information about local users logging on to those machines. And if these users then connect to other networks, the intruder has the potential to penetrate and monitor the remote systems to which the local users connect, thereby increasing the likelihood of a breach in the security of those systems as well. Therefore, it is important to have a second level security to the user's password. Cryptography is an art to convert a message into other forms by using some algorithms. It is used widely in many fields such as securing message before sending through email, sending confidential documents or letters through networks, doing business online and etc. The two algorithms chosen to develop this system are Advanced Encryption Standard (AES) and Data Encryption Standard (DES). The purpose of choosing AES and DES is because they are two of the most popular algorithms for modern encryption.

Keywords: password, generator, secure.

1 Introduction

Should someone else guesses or steals the user's password, he or she can masquerade as the user, which means the intruder would then have access to the user's files, e-mail, funds, personal information, and more. This intruder will have the power to modify or destroy the user's files, to send electronic mail threats in the user's name, or to subscribe to unwanted services for which the user has to pay. In short, an insecure password can easily wreak havoc in the user's life. In addition to these, the user won't be the only person affected by a stolen password. Other users on networks along the Internet could potentially be affected as well. Once an intruder with the necessary knowledge, experience, and tools gains entry to a system, he or she may be able to monitor other machines and systems on the same network and capture information about local users logging on to those machines. And if these users then connect to other networks, the intruder has the potential to penetrate and monitor the remote systems to which the local users connect, thereby increasing the likelihood of a breach in the security of those systems as well. Therefore, it is important to have a second level security to the user's password.

2 Background

Data Encryption Standard (DES) was introduced in 1977 and it is used widely due to the rapid development in hardware with memory and the use of computer networks until today. It is used to encrypt data to store in personal computer or to send over internet for security purpose. Owing to the fast pace development in Science and Technology, there are many machines or hardware created to break the DES code which is in 56-bits in several minutes. As a result, AES started to develop in year 2000 with more possibilities of key and more time needed to break the code. In order to have a second level security to the user's password, AES system will be developed. This system will encrypt user's password from plaintext to ciphertext using their preferred key. This systems will be developed using Java Language which can work offline or normally known as standalone software.

3 Problem Statement

Nowadays, most of information recorded in a system. One of them is user's password which is stored in a database of a system. It is stored as a plaintext. This means that, there is no security feature implemented to the user's password. So, the intruder has a chance to enter the system if they can get the password from the database.

4 Methodology

Algorithm of the system. It is better to define the algorithms first as one of the steps of planning before starting to code any system. Basically, this system would accept message longer that one block (16 bytes per block for AES and 8 bytes per block for DES). Hence, Array List and array (one-dimensional array and two-dimensional array) were chosen to store the message and key when processing them. The reason of choosing Array List was because the size of Array List is expandable. Data encryption involves a lot of methods or steps need to be done before the results can be achieved. The most challenging part when developing this system was to convert these steps into coding. Since Java is an OOP, the steps were coded in different classes and methods so that it would be more. There are 16 rounds in DES before getting the final results. The algorithm of DES is shown below:

Algorithm 4.1

```
BEGIN
block = 1

        LOOP WHILE !

                messageInHex.isEmpty()
                Arrange the message into array form
```

```
        Process key:
        doPermutedChoice1(encryption)
        doHalves(encryption)

        Process message:
        doInitialPermutation(encryption)
        doHalves(encryption)


                LOOP For i=0 to 15

                        Process Key:
                        doLeftShift(encryption, i)
                        doPermutedChoice2 (encryption)

                        Process Message:
                        doExpansionPermutation(encryption)
                        doEXORPC2(encryption)
                        doSBox(encryption)
                        doPBox(encryption)
                        doPBoxXORLeftHalf(encrypption, i+1)

                        i++

                END LOOP

        doFinalPermutation(encryption, block)
        Display the results to all text areas
        block++

    END LOOP
END
```

Meanwhile, for AES, the number of rounds needs to be performed depends on the key size chosen by user. There are three types of key size for AES which are 128

bits, 192 bits and 256 bits. The table below shows how many rounds need to be gone through to process a block of message or plaintext according to the key size:

Table 4.1: Number of rounds for AES

Key Size (bits)	128	192	256
Number of round, Nr -1	9	11	13

5 Finding

The input page is shown in figure 4 as below. First of all, user is required to choose the type of algorithm (AES or DES) they want to use. Then, the message and key are entered in the text area as shown in figure 1. One of the advantages of this system is it could accept message more than one block. Besides that, user can choose the form of input either in Hexadecimal String or ASCII characters. On the other hand, the output page is shown in figure 2. It will show the plaintext, ciphertext and the results obtained in every round. The results will be in hexadecimal if the chosen method was AES and in binary if the DES was chosen.

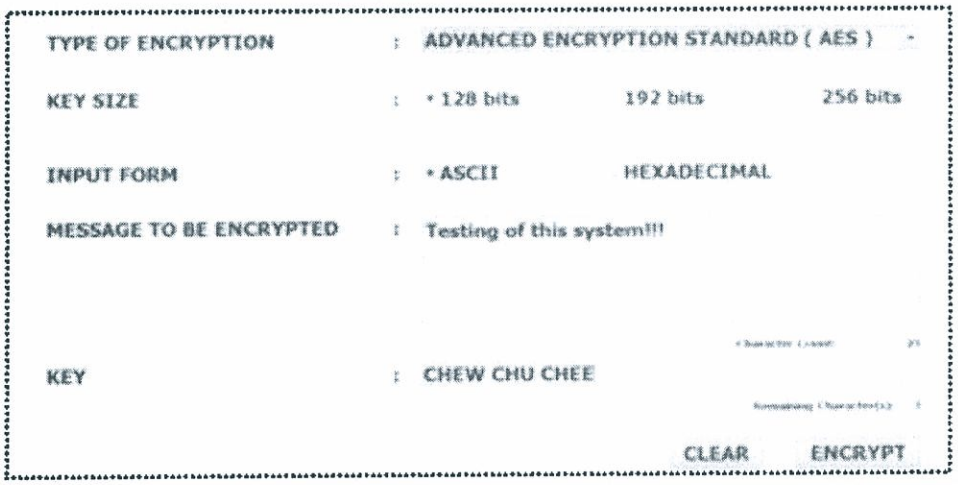

Figure 5.1: Input Interface

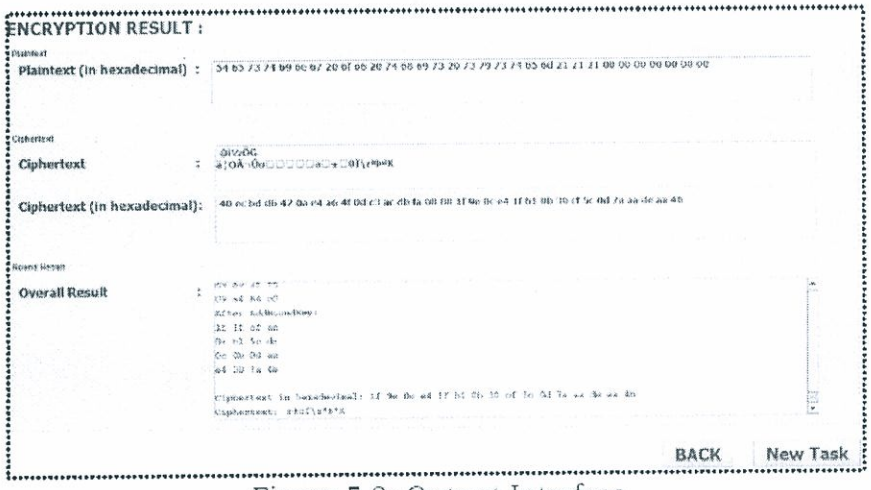

Figure 5.2: Output Interface

6 Conclusion and Discussion

In conclusion, it is important to have a second level security to the user's password. The encryption system is very useful for the purpose of password security. The strengths of this system is, it has a simple and user-friendly user interface which users do not need to refer much to the manual guide to use the system. On the other hand, it can handle message or plaintext which is more than one block.

References

[1] William Stallings, (2003). *Cryptography and Network Security.* 3rd ed. Upper Saddle River, N. J.: Prentice Hall.

[2] John B. Fraleigh, (2000). *A first course in Abstract Algebra.* 6th ed. N.Y.: Addison Wesley Longman.

[3] Kenneth H. Rosen, (2000). *Elementary Number Theory and its applications.* 4th ed. AT&T Laboratories : Addison Wesley Longman.

[4] Niels Freguson and Bruce Schneiner, (2003). *Practical Cryptography.* Canada: Wiley Publishing, Inc., Indianapolis, Indiana.

[5] Kenneth H. Rosen, (1998). *Elementary Number Theory and its applications.* 2th ed. AT&T Laboratories : Addison Wesley Longman.

[6] Bryan J. Higgs, (2005). Computer Security "*Modern Cryptography: Public-Key Cryptosystems*".

[7] Phongsak Prasith Sangaree, (2002). *Providing Network Security to Wireless Devices Using Public Key Cryptography Based on Elliptic curves over Finite Fields.* University of Pittsburgh: Comprehensive Exam Paper.

[8] Diffie, W., and Hellman, M.E., (1976). *New Directions in Cryptography.* IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654.

[9] Yenuguvanilanka, J. and Elkeelany, O. (2008). "Performance Evaluation of Hardware Models of Advanced Encryption Standard (AES) Algorithm." IEEE Southeastcon, 2008. pp.222 - 225

[10] Eskicioglu, A. and Litwin, L. (2001). "Cryptography." IEEE Potentials. 20. pp. 36 – 38.

DR. TAY CHOO CHUAN
Mathematics, Quality and Productivity Improvement division
Research program coordinator Faculty of Electrical Engineering
Universiti Teknikal Malaysia Melaka
E-mail: tay@utem.edu.my

DR. HAMZAH BIN SAKIDIN
Applied Mathematics and Mathematical Modeling division
Faculty of Electrical Engineering
Universiti Teknikal Malaysia Melaka
E-mail: hamzahsakidin@utem.edu.my PROF.

DR. NANNA SURYANA HERMAN
System and GIS interoperability, Spatial Modeling, GIS division
Faculty of Information and Communication Technology
Universiti Teknikal Malaysia Melaka
E-mail: nsuryana@utem.edu.my

MOHD. RIZUAN BAHARON
Mathematics and Cryptography division
Faculty of Information and Communication Technology
Universiti Teknikal Malaysia Melaka
E-mail: mohd.rizuan@utem.edu.my

SUPPORTED BY :

Chevron

IJP Indonesian Journal of Physics
http://ijp.fi.itb.ac.id/index.php/ijp

biofarma

Faculty of Mathematics and Natural Sciences
School of Life Sciences and Technology
School of Pharmacy
INSTITUT TEKNOLOGI BANDUNG

ISBN 978-979-17090-3-3
9 789791 709033