PDF file encryption on mobile phone using super-encryption of Variably Modified Permutation Composition (VMPC) and two square cipher algorithm

D Rachmawati¹, M A Budiman² and F Atika³
Departemen Ilmu Komputer, Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Sumatera Utara, Jl. Universitas No. 9-A, Kampus USU, Medan 20155, Indonesia
dian.rachmawati@usu.ac.id¹, mandrib@usu.ac.id², fadhilahatika@students.usu.ac.id³

Abstract. Data security is becoming one of the most significant challenges in the digital world. Retrieval of data by unauthorized parties will result in harm to the owner of the data. PDF data are also susceptible to data security disorder. These things affect the security of the information. To solve the security problem, it needs a method to maintain the protection of the data, such as cryptography. In cryptography, several algorithms can encode data, one of them is Two Square Cipher algorithm which is a symmetric algorithm. At this research, Two Square Cipher algorithm has already developed into a 16 x 16 key aims to enter the various plaintexts. However, for more enhancement security it will be combined with the VMPC algorithm which is a symmetric algorithm. The combination of the two algorithms is called with the super-encryption. At this point, the data already can be stored on a mobile phone allowing users to secure data flexibly and can be accessed anywhere. The application of PDF document security on this research built by Android-platform. At this study will also calculate the complexity of algorithms and process time. Based on the test results the complexity of the algorithm is $\theta (n)$ for Two Square Cipher and $\theta (n)$ for VMPC algorithm, so the complexity of the super-encryption is also $\theta (n)$. VMPC algorithm processing time results quicker than on Two Square Cipher. And the processing time is directly proportional to the length of the plaintext and passwords.

1. Introduction
Data security becomes one of the most significant challenges in the digital world. If someone has data that should be confidential but instead known by unauthorized parties, so it would be detrimental to those who have the data. There are so many things that can be done to ensure the security of data, one of them by encoding the data into data that can not be read or understood by others but can be read by the authorities. For these security problems, it needs a method to maintain data security, one of them with cryptography. Cryptography is a field of science that studies the process of encoding data using mathematical equations. Cryptography is an art and science that maintain data security [1].

In this study the writer will use PDF files to make it safe, because the PDF file is susceptible to damage to the security of the information contained within it, allowing one to know clearly and be able to modify the contents of the file.

In cryptography, there are several algorithms that can encode data, one of them is Two Square algorithm or another name Double Playfair is derived from Playfair Cipher algorithm.
For better security, Two Square Cipher algorithm with square 5x5 will be developed into a 16x16 square, so the length of each key in the square is 256 characters that can be loaded with a 256-character ASCII code. Development of keys to 16x16 is of course also useful in plaintext that is entered, so that it is not just an alphabet letter only. For better security the Two Square Cipher 16x16 algorithm will be combined with the Variably Modified Permutation Composition (VMPC) algorithm. VMPC is a modern symmetric algorithm and designed by Bartosz Zoltak, published in 2004 [2].

The combination of Two Square Cipher and Variably Modified Permutation Composition (VMPC) algorithm is intended for obtaining stronger ciphers than using only one cipher, so it is not easy to solve. This method is called super-encryption. Super-Encryption is algorithm that combines two of cipher [3]. Super encryption aims to increase the encryption complexity of a data so that unauthorized users can not decrypt the data, if some key lock is known [4].

In this study, the authors build applications based on Android. Because now the data can be stored on the mobile phone making it possible to secure data and more flexible in mobile.

Based on the background, the author tries to implement super encryption method with 16x16 Two Square Cipher algorithm which will be combined with Variably Modified Permutation Composition (VMPC) algorithm to create security application of PDF file based on Android.

2. Method

The first encryption process will be done with Two Square Cipher algorithm and then encrypted again using VMPC algorithm. And then the first decryption process will be done with the VMPC algorithm then Two Square Cipher algorithm.

Password will be randomized with KSA and PRGA in encryption and decryption process. The PRGA will be randomized along the ciphertext. Pseudo-Random Generation Algorithm (PRGA) is run after VMPC Key Scheduling Algorithm (KSA). The pseudocode of KSA and PRGA as shown on table 1.

| Table 1. Key Scheduling Algorithm and Pseudo-Random Generation Algorithm [5]. |
|-------------------------------------------------------------------------------------------------|
| 1. $k = 0$                                                                                     |
| 2. repeat step 3 until length + 6 along plaintext length:                                       |
| 3. $x = S[x + S[k]]$ modulo 256                                                                  |
| 4. $S[k] = S[x]$                                                                                |
| 5. $S[x] = Temp$                                                                                |
| 6. $k = (k + 1)$ modulo 256                                                                    |

The Two Square Cipher algorithm is a derivative of the Playfair Cipher algorithm. This algorithm is a classical symmetric algorithm. In the Two Square Cipher algorithm there are two 5 x 5 squares placed side by side, where the first letter of each plaintext diagraph is placed on the left square, and the second letter in each plaintext diagraph is placed on the right square. So that every character in the plaintext diagraph can not be in the same column, but they can be on the same line. [6].

In encrypting the message, the message to be encrypted is first set as follows:

1. If the number of characters in the message is odd, then inserted a space in the last character of the message to have a pair.

2. To create a square, the key is selected on each square, preferably using two different keywords. The keys are placed sequentially from the top left to the side, then down, without repetition. Next, all unused ASCII codes are entered sequentially into square.

Two Square Cipher Encryption Method

The encryption algorithm has rules include [7]:

Encryption algorithm has rules include (Widjayanti, 2010):

1. Separate plaintext into digraph by two characters.
2. One by one matched into the square. The first character digraph is inserted into the left square and the second character is positioned on the right.
3. If it is located on different rows and columns, look for the intersection of the character. The first characters that are listed from the encryption result are characters parallel to the first character plaintext. And if both characters are in the same row, slide to the right.

Two Square Cipher Decryption Method
For decryption is done the inverse of encryption, as described as follows [7]:
1. Separate the ciphertext into digraph by two characters.
2. The first character of the digraph is inserted into the right square and the second character is inserted into the left.
3. Search the intersection of the characters. If characters are in the same row, slide to left. If it are in a different line, the decrypted characters are characters parallel to the first character ciphertext.

3. Result and Discussion
The system was built using Android Studio 1.4.1. with the programming language is Java. This system is tested with Personal Computer with 2.7 GHz processor specification Intel Core i5, 8 GB Memory 1867 MHz DDR.

The result of the complexity of the algorithm Two Square Cipher is $\Theta(n)$, and VMPC algorithm is $\Theta(n)$. So the complexity value of super-encryption with Two Square Cipher algorithm and VMPC algorithm is $\Theta(n)$.

In this test, the parameters used are algorithm complexity and real running time. The system testing criteria as follows:
1. Plaintext in the form of PDF files with the total length 24, 50, 129, and 180 characters.
2. Passwords with overall length 10, 20, and 30 characters.
3. The calculation of real running time is done manually using Java programming language.

The result of processing time Two Square Cipher algorithm plaintext with 24, 50, 129, and 180 character lengths respectively is 16 ms, 25.6 ms, 26.6 ms, and 39.6 ms. For VMPC algorithm is 1 ms, 1.3 ms, 6.3 ms and 15 ms. And for super-encryption is 14.3 ms, 21 ms, 39 ms, and 64.6 ms. It can be seen that the process time of the VMPC algorithm is faster than the Two Square Cipher. The results can be illustrated in a graph of Figure 1

![Figure 1](image_url)

**Figure 1.** Graph of Plaintext Length Against the Process Time of Two Square Cipher, VMPC and Super-Encryption

Figure 1 shows a graph of plaintext length for the process time of the Two Square Cipher Algorithm, VMPC, and super encryption, where the length of the plaintext is directly proportional to the processing time that produces a linear state.
The result of processing time Two Square Cipher algorithm password with 10, 20, and 30 character lengths respectively is 8 ms, 8.3 ms, and 8.6 ms. For VMPC algorithm is 1 ms, 2 ms, and 2.3 ms. And for super-encryption is 13 ms, 22.67 ms, and 28.3 ms. It can be seen that the process time of the VMPC algorithm is faster than the Two Square Cipher. The results can be illustrated in a graph of Figure 2.

![Figure 2](image)

Figure 2. Graph of Password Length Against the Process Time of Two Square Cipher, VMPC, and Super-Encryption

Figure 2 shows a graph of plaintext length for the process time of the Two Square Cipher Algorithm, VMPC, and super encryption, where the length of the password is directly proportional to the processing time that produces a linear state.

4. Conclusion

- The results of encryption testing on the plaintext and passwords show a meaningful linear result. If the length of characters plaintext and passwords is longer then the longer processing time required.
- The result of the complexity Two Square Cipher Algorithm is $\Theta(n)$, VMPC algorithm is $\Theta(n)$, So for the complexity of super-encryption is also $\Theta(n)$.
- The results of processing time VMPC algorithm are faster than the Two Square Cipher algorithm although the results of complexity show the same thing.

References

[1] Schneir, Bruce 1996, *Applied Cryptography 2nd ed Cryptography: Protocols, Algorithms, and Source Code in C* 15-20.

[2] Karahan, M. 2015. *New Attacks On RC4A and VMPC*. Bilkent University.

[3] Setyaningsih, E. et. al. December 2012. *Image Encryption on Mobile Phone using Super Encryption Algorithm*, TELKOMNIKA, Vol.10, No.4, pp. 837–845 ISSN: 1693-6930

[4] Gupta, H. & Sharma, V.K. 2011. *ROLE OF MULTIPLE ENCRYPTION IN SECURE ELECTRONIC TRANSACTION*. International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6. Amity Institute of Information Technology, Amity University Campus, Sector – 125, Noida (Uttar Pradesh), India.

[5] Zoltak, B. 2004. *VMPC One-Way Function and Stream Cipher*: Delhi, India.

[6] Churchhouse, R.F. 2004. *Codes and ciphers Julius Caesar, the Enigma and the internet*: Cambridge.

[7] Widjajayanti, R. 2010. *Two SquareCipher*. Program Studi Teknik Informatika, Institut Teknologi Bandung.