Implementation Cryptography Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES) Method in Communication System Based Near Field Communication (NFC)

Ratnadewi¹, Roy Pramono Adhie¹, Yonatan Hutama¹, A. Saleh Ahmar²,³, M I Setiawan⁴

¹Electrical Engineering Department, Universitas Kristen Maranatha, Bandung, Indonesia
²Department of Statistics, Universitas Negeri Makassar, Makassar, Indonesia
³AHMAR Institute, Makassar, Indonesia
⁴Narotama University, Surabaya, Indonesia

ratnadewi.bandung@gmail.com

Abstract. Cryptography is a method used to create secure communication by manipulating sent messages during the communication occurred so only intended party that can know the content of that messages. Some of the most commonly used cryptography methods to protect sent messages, especially in the form of text, are DES and 3DES cryptography method. This research will explain the DES and 3DES cryptography method and its use for stored data security in smart cards that working in the NFC-based communication system. Several things that will be explained in this research is the ways of working of DES and 3DES cryptography method in doing the protection process of a data and software engineering through the creation of application using C++ programming language to realize and test the performance of DES and 3DES cryptography method in encrypted data writing process to smart cards and decrypted data reading process from smart cards. The execution time of the entering and the reading process data using a smart card DES cryptography method is faster than using 3DES cryptography.

Keywords: Cryptography, Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), NFC

1. Introduction

In a process of communication, there are exchanging the messages. Delivery of a message that is sensitive and must be protected in order to avoid the theft of information by parties who are not responsible. One way to protect the delivery of a message is to use cryptographic methods. One method that is most commonly used cryptography in securing the delivery of messages, especially messages in the form of text data, is a cryptographic method Data Encryption Standard (DES). DES cryptographic methods developed by scientists in the field of computer network security in the US computer company, the International Business Machines Corporation (IBM) since 1974. [1] DES
cryptographic methods developed by the cryptographic algorithm Lucifer made by Horst Feistel and were first published in 1971.

Cryptographic methods Triple Data Encryption Standard (3DES), can also be called Triple Data Encryption Algorithm (TDEA), is a further development of DES cryptographic methods. Cryptographic 3DES method was first published in 1998 and was made to replace the DES cryptographic method as standard cryptographic text data in the world. Difference between the two is 3DES using triple DES-step process used for encryption and decryption process by using a three key combination for each process.

Near Field Communication (NFC) protocol and interface for data exchange process in a simple wireless communication system devices connected in near distance. NFC is one of the development of communications technology Radio Frequency Identification (RFID) and belong to the category of High frequency (HF) and has a working frequency of 13.56MHz. Examples of devices that support NFC based communication process is a contactless smart card and smart card reader. Smart card reader is used as a device supporting the process of data writing and data reading contactless smart cards.

2. Theoretical Basis

2.1. Data Encryption Standard (DES)

DES encryption method is a text data cryptographic method with the type of symmetric - key block cipher and consists of two processes, namely the process of encryption and decryption process. [2] Each of that process has an eight-step process. Decryption process is done by reversing the steps - steps encryption process. Key used in DES cryptography method has 56 bits of effective length.

The process of encryption using DES cryptographic method consists of the eight-step process, [3] [4], that are:
1. Convert plaintext and the key that will be processed into binary bits. Plaintext and the key that has been converted and then broken down into data blocks form with each of the block has a 64 bits (eight bytes) length. If the message is in the form of the alphabet or symbols, it must be first converted into decimal and hexadecimal form following the ASCII character table, and then are converted into binary bit.
2. Randomize the bits in plaintext data block based on Initial Permutation (IP) table, so that the bit sequence randomized compared to bits sequence of early plaintext block. The bits sequence after the second step followed the results from the IP table, with the first bit derived from the 58th sequence bit of early plaintext blocks, and then the second bit derived from the 50th sequence bits until the 64th sequence bit derived from the seventh. sequence bits.
3. The scrambling of key bits based on permuted Choice 1 (PC - 1) table. Results from the PC - 1 has a 56 bit length because the last bits of each byte of the key (8, 16, 24, 32, 40, 48, 56 and 64 bits) that acts as the parity bit is not used again in the next step process. Once completed the results of PC - 1 then divided into C0 and D0, with C0 is 28 leftmost bits and D0 is 28 rightmost bits from PC – 1 results bits sequence.
4. Shift bits to the left (left shift) at C1 and D1 as much as one or two times, with the value of i based on encryption process round that consists of 16 rounds. The result of the shift bits from every round of the C1 and D1 are then combined into C2D2 with a length of 56 bits. After that the C2D2 key bits are randomized based on PC - 2 (permuted Choice 2) table until produce the Ki variable.
5. Running the data expansion process of Ri-1 with a length of 32 bits (starting from the R0 of second process step results) becomes Ri with a length of 48 bits, where i is the round during the process. This process will be carried out as much as 16 times with the value of turnover 1 <= i <= 16 using the Expansion Table. The results of the expansion process is referred to as E(Ri-1), starting from E(R0) to E(R15). Afterwards, E(Ri-1) will be XOR processed with Ki that has been obtained from the fourth step process for each bit corresponds to running process round to produce Ai variable with a length of 48 bits and in a vector form.
6. Once obtained, $A_i$ then broken down into eight blocks with each block consist of six bits. Each block is then distributed into eight pieces of $S-$ Box (Substitution Box), with the first block distributed to the $S-$ Box 1, the second block distributed to the $S-$ Box 2 and so on. The result of the substitution process using $S-$ Box will be collected and produce $B_i$ variable.

7. Once $B_i$ variable obtained, the next step is do the permutation process on each bit of $B_i$ variable using $P-$ Box table. The results obtained from the permutation using $P-$ Box referred to as $P(B_i)$, with $i$ adapted to the round during the process, starting from $P(B_1)$ through $P(B_{16})$. Thereafter, $P(B_i)$ will be XOR processed with the $L_{i-1}$obtained from the second process step in accordance with the processes running round to produce an $R_i$ variable with a length of 32 bits and in a vector form. $R_i$ results will then be merged with $L_i$, which came from the $R_{i-1}$, into $L_iR_i$ which is the result of the encryption process of plaintext for each round process with a length of 64 bits.

8. The eighth process step carried out when the seventh process step has obtained the $L_{16}$and $R_{16}$ from the 16th process round. The next step is the process of reversing positions on $L_{16}$ and $R_{16}$, and then combined to obtain the $R_{16}L_{16}$ form. These results are then permuted using IP-1 (Inverse Initial Permutation) table. Results obtained from the eight process step is referred to as cipher, which is a data block that has been encrypted and is ready to be sent to the recipient along with the other ciphers. A combination of several cipher is called ciphertext.

For the note, the first and second step of the process is done only once at the beginning of the DES encryption process, while the eight step of the process is done only once at the end of the DES encryption process. The third step process to the seventh step process carried out 16 times according to the number of rounds of Feistel process used by DES cryptographic method. DES encryption process block diagram is shown in Figure 1.

2.2. *Triple Data Encryption Standard (3DES)*

3DES cryptography method is the development of DES cryptographic method. The difference between the two methods is 3DES using triple times the DES process step used in encryption process and decryption process by using three key combination.[5] In addition, the effective length of the key used for encryption process and decryption process using 3DES cryptographic method is 168 bits (consisting of three sub - key that each have a length of 56 bits), in contrast to DES cryptographic method that uses a key with and effective length of 56 bits.[6]
There are three options to use a combination of sub-key that has become standard in the encryption process and decryption process using 3DES cryptographic method,[7] that are:

1. Three sub-key have different combinations (3K3DES).
2. K1 and K2 have different combinations, whereas K1 and K3 have the same combinations (2K3DES).
3. Three sub-key has the same combinations.

Of the three options, the use of sub-key, the first option is the best because the three sub-key has a different combination, with an effective key length of 168 bits, so that the data is encrypted using the first option is more difficult to resolve than the use of the second and third options.[8] The second option has an effective key length of 112 bits, because the first sub-key has same combination as the third sub-key, but this option is still better than using the DES encryption process twice. The third option is the weakest compared to the previous option because the first sub-key and the second sub-key negated each other in the process so that the key used in this option has an effective length of 56 bits, the same as the length of the key used by DES cryptographic method. The second option will be used in the performance examination process of 3DES cryptographic method in this research. 3DES encryption process block diagram is shown in Figure 2.

![3DES Encryption Process Block Diagram](image)

**Figure. 2** 3DES Encryption Process Block Diagram

2.3. Near Field Communication (NFC)

NFC is one of the latest communication technology and developed from RFID communication technology with working frequency of 13.56 MHz.[9] The device used in NFC based communication process is divided into two types, namely active devices and passive devices. An example of active device is a smart card reader, while an example of a passive device is a contactless smart card. Each NFC based active device can work in three modes of operation,[10], that are:

1. Card Emulation.
2. Card Reader / Writer.
3. Peer - to - Peer.

Card Emulation operating mode is used to change the function of active devices such as smart phones that can be used like a smart card. Card reader / writer operating mode is used to perform the writing process and reading process of the data contained in a passive device. Peer - to - peer operation mode used to perform data exchange process between two active device with similar condition, such as two smart phone devices. The second operating mode will be used in this research to examine the performance of DES and 3DES cryptography method.
3. Implementation and Testing

3.1. Program Implementation

In this research, the authors implemented DES and 3DES cryptographic methods into programs created using the Microsoft Visual Studio 2008 software and in C++ programming language. Programmes built in the form of application can be used on computers that have been based on the .NET framework. There is one application made in this research, that is the application of data writing and data reading of ACOS3 smart card using DES and 3DES cryptographic method in NFC-based systems. Contactless smart card and smart card reader that will be used in this research are ACOS3 8 KB smart card and ACS ACR1252U reader. The application display can be seen in Figure 3.

![Figure 3 Application Data Charging and Data Reading Method Using Cryptographic Smart Card ACOS3 DES and 3DES in NFC-Based Systems](image)

The ACOS3 smart card data writing process using DES and 3DES encryption method have two inputs, that are the message that will be encrypted (plaintext / data) and key (card key and terminal key), and a single output, that is the message that has been encrypted perfectly (ciphertext) and also will be loaded into the ACOS3 smart card. The data writing process is executed by pressing the “Write Data” button. The ACOS3 smart card data reading process using DES and 3DES decryption method have two inputs, the ciphertext and key, and a single output, the message that has been perfectly decrypted (plaintext) and also will be displayed in the “Data” text box in the application. The data reading process is executed by pressing the “Reading Data” button.

3.2. DES and 3DES Performance Testing

Performance examination was conducted to examine two things, the data writing execution time and data reading execution time of ACOS3 smart card using DES and 3DES cryptographic method. There are 10 observational data for each trial based on the length of data to be processed, starting from 8 ASCII characters up to 4096 ASCII characters. Each data observation tested three times to generate
the average execution time. The performance examination results table that is carried out can be seen in Table 1 up to Table 3.

Performance examination that is done on ACOS3 smart card shows the result that the data writing execution time using DES encryption method is faster than using 3DES encryption method for each observational data. It also occurs in the data reading process using DES decryption method that is faster than using 3DES for each observational data. The execution time difference between that two cryptographic method is growing along with increasing length of the data processed.

Table 1. DES Cryptographic Method Performance Examination Results

| No. | Data Length (ASCII Character) | Execution Time DES Cryptography Method (milliseconds) | Data Write Process | Data Read Process |
|-----|-------------------------------|-----------------------------------------------------|--------------------|-------------------|
|     |                               |                                                     | Test 1  | Test 2  | Test 3  | Average | Test 1  | Test 2  | Test 3  | Average |
| 1   | 8                             |                                                     | 57     | 57     | 57     | 57     | 44     | 41     | 40     | 42      |
| 2   | 16                            |                                                     | 60     | 59     | 62     | 61     | 43     | 42     | 43     | 43      |
| 3   | 32                            |                                                     | 64     | 63     | 68     | 65     | 47     | 46     | 48     | 47      |
| 4   | 64                            |                                                     | 78     | 77     | 78     | 78     | 56     | 56     | 58     | 57      |
| 5   | 128                           |                                                     | 99     | 99     | 100    | 100    | 73     | 72     | 71     | 72      |
| 6   | 256                           |                                                     | 148    | 149    | 146    | 148    | 113    | 113    | 115    | 114     |
| 7   | 512                           |                                                     | 208    | 206    | 209    | 208    | 145    | 145    | 147    | 146     |
| 8   | 1024                          |                                                     | 265    | 263    | 263    | 264    | 181    | 180    | 183    | 182     |
| 9   | 2048                          |                                                     | 321    | 327    | 326    | 325    | 217    | 219    | 220    | 219     |
| 10  | 4096                          |                                                     | 387    | 383    | 390    | 387    | 255    | 254    | 258    | 256     |

Table 2. 3DES Cryptographic Method Performance Examination Results

| No. | Data Length (ASCII Character) | Execution Time 3DES Cryptography Method (milliseconds) | Data Write Process | Data Read Process |
|-----|-------------------------------|-----------------------------------------------------|--------------------|-------------------|
|     |                               |                                                     | Test 1  | Test 2  | Test 3  | Average | Test 1  | Test 2  | Test 3  | Average |
| 1   | 8                             |                                                     | 62     | 62     | 60     | 62     | 44     | 43     | 44     | 44      |
| 2   | 16                            |                                                     | 64     | 66     | 66     | 66     | 46     | 49     | 46     | 47      |
| 3   | 32                            |                                                     | 68     | 70     | 68     | 69     | 53     | 50     | 50     | 51      |
| 4   | 64                            |                                                     | 84     | 84     | 85     | 85     | 61     | 61     | 61     | 61      |
| 5   | 128                           |                                                     | 110    | 111    | 112    | 111    | 83     | 85     | 84     | 84      |
| 6   | 256                           |                                                     | 169    | 172    | 170    | 171    | 133    | 133    | 131    | 133     |
| 7   | 512                           |                                                     | 253    | 255    | 260    | 256    | 192    | 195    | 194    | 194     |
| 8   | 1024                          |                                                     | 321    | 325    | 331    | 326    | 244    | 248    | 247    | 247     |
| 9   | 2048                          |                                                     | 393    | 399    | 402    | 398    | 297    | 294    | 300    | 297     |
| 10  | 4096                          |                                                     | 472    | 468    | 473    | 471    | 365    | 369    | 372    | 369     |

Table 3 – DES and 3DES Cryptographic Method Performance Examination Average Results

| No. | Data Length (ASCII Character) | Execution Time 3DES Cryptography Method (milliseconds) | Data Write Process | Data Read Process |
|-----|-------------------------------|-----------------------------------------------------|--------------------|-------------------|
|     |                               |                                                     | DES    | 3DES  | DES    | 3DES  |
| 1   | 8                             |                                                     | 57     | 62    | 42     | 44    |
| 2   | 16                            |                                                     | 61     | 66    | 43     | 47    |
| 3   | 32                            |                                                     | 65     | 69    | 47     | 51    |
Through conducted performance examination, it also found that the data writing execution time of ACOS3 smart card using DES and 3DES decryption method is faster than the data writing execution time of ACOS3 smart card using DES and 3DES encryption method for each observational data. The average execution time chart of ACOS3 smart card data writing process and data reading process using DES and 3DES cryptographic method for each observational data can be seen in Figure 4 and Figure 5.

![Average Execution Time Chart of ACOS3 Smart Card Data Writing Process Using DES and 3DES Encryption Method](image1)

**Figure 4** Average Execution Time Chart of ACOS3 Smart Card Data Writing Process Using DES and 3DES Encryption Method

![Average Execution Time Chart of ACOS3 Smart Card Data Reading Process Using DES and 3DES Decryption Method](image2)

**Figure 5**. Average Execution Time Chart of ACOS3 Smart Card Data Reading Process Using DES and 3DES Decryption Method
4. Conclusion
Based on performance examination conducted on DES and 3DES text data cryptographic method with the help of the application of data writing and data reading of ACOS3 smart card using DES and 3DES cryptographic method in NFC-based systems, there are several things that can be concluded:
1. DES and 3DES text data cryptographic method can be implemented on application of ACOS3 smart card data writing process and data reading process in NFC-based systems.
2. The execution time of ACOS3 smart card data writing process and data reading process using DES cryptographic method is faster than 3DES cryptographic method.
3. The execution time of data reading process is faster than data writing process for ACOS3 smart card, using DES or 3DES cryptographic method.

References
[1] S. Mankotia and M. Sood. 2015 “A Critical Analysis of Some Symmetric Key Block Cipher Algorithms”. International Journal of Computer Science and Information Technologies, Vol. 6.
[2] G. Singh and Supriya. 2013. “A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security”. International Journal of Computer Applications Vol. 67, No. 19.
[3] C. Paar and J. Pelzl. 2010. Understanding Cryptography – A Textbook for Students and Practitioners. Heidelberg : Springer – Verlag GmbH & Co.
[4] W. Stallings. 2014. Cryptography and Network Security – Principles and Practice 6th Edition. Upper Saddle River, New Jersey : Pearson Education Limited.
[5] S. Rao. 2015. “Performance Analysis of DES and Triple DES”. International Journal of Computer Applications. Vol. 130, No. 14.
[6] M. Mathur and A. Kesarwani. 2013. “Comparison Between DES, 3DES, RC2, RC6, BLOWFISH and AES”. Proceedings of National Conference on New Horizons in IT.
[7] P. Kumar and N.S. Rajaanandan 2016. “Data Encryption and Decryption Using By Triple DES Performance Efficiency Analysis of Cryptosystem”. International Journal of Innovative Research in Computer and Communication Engineering Vol. 4, No. 3.
[8] A. Kahate. 2003. Cryptography and Network Security. Singapore : Tata McGraw – Hill Publishing Company Limited.
[9] A. Makhmali and H. M. Jani. 2013. “Comparative Study On Encryption Algorithms And Proposing A Data Management Structure”. International Journal of Scientific & Technology Research Vol. 2, No. 6.
[10] H. A. Al-Ofeishat and M.A.A.AI Rababah. 2012. “Near Field Communication (NFC)”. International Journal of Computer Science and Network Security Vol. 12, No. 2.