Sms Encryption Application Using 3Des (Triple Data Encryption Standard) Algorithm Based on Android

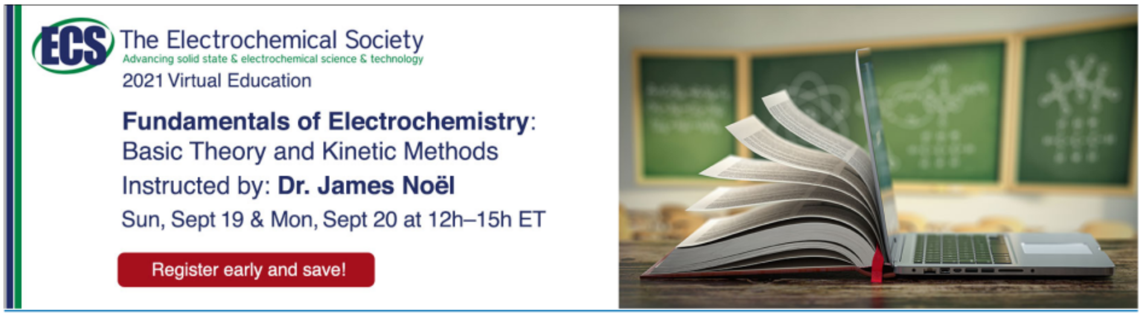
by Nurdin, Dahlan A , Widia F, R Ratnadewi, Nuning K Dian R,b Kusuma R , Edi S , Very K, Febry L, Dian

Journal of Physics: Conference Series

PAPER • OPEN ACCESS

Sms Encryption Application Using 3Des (Triple Data Encryption Standard) Algorithm Based on Android

To cite this article: Nurdin *et al* 2019 *J. Phys.: Conf. Ser.* **1363** 012077



Sms Encryption Application Using 3Des (Triple Data Encryption Standard) Algorithm Based on Android

Nurdin[1]*, Dahlan Abdullah[1], Widia Fatimah[1], R Ratnadewi[2], Nuning Kurniasih[3], Dian Rianita[4], Berliana Kusuma Riasti[5], Edi Sofian[6], Very Karnadi[7], Febri Liantoni[8], Dian Ade Kurnia[9], Triawan Adi Cahyanto[10], Arief Aulia Rahman[11] and I Ketut Sudarsana[12]

[1]Department of Informatics, Universitas Malikussaleh, Aceh Utara, Indonesia
[2]Electrical Engineering, Universitas Kristen Maranatha, Bandung, Indonesia
[3]Faculty of Communication Sciences, Library and Information Science Program, Universitas Padjadjaran, Bandung, Indonesia
[4]Department of Administration, University of Lancang Kuning, Pekanbaru, Indonesia
[5]Department of Informatics Engineering, Universitas Sebelas Maret, Surakarta, Indonesia
[6]Faculty of Economics, Universitas Islam Sumatera Utara, Medan, Indonesia
[7]Department of Informatics Engineering, University of Putera Batam, Batam, Indonesia
[8]Department of Informatic, Faculty of Information Technology, Institut Teknologi Adhi Tama, Surabaya, Indonesia
[9]Departement of Information Technology, STMIK IKMI Cirebon, Indonesia
[10]Department of Informatics Engineering, Faculty of Engineering, University of Muhammadiyah Jember
[11]Department of Mathematics, STKIP Bina Bangsa Meulaboh, Meulaboh, Indonesia
[12]Department of Religious Education, Institut Hindu Dharma Negeri Denpasar, Indonesia

*nurdin@unimal.ac.id

Abstract. Security is an important aspect in communicating using information technology. SMS is a service provided by mobile phones to communicate by sending short messages quickly and cheaply. Short message delivery is done by SMS network, so the messages are not sent directly to the destination mobile phone. Therefore the messages that are sending by the SMS service need to be protected, so the security of the messages sent to the SMS network remains protected by its confidentiality. In this study the software will be built to improve the security of messages on SMS communication. The software that is built serves to encrypt messages that will be sent and decrypt messages with entered through the SMS service. Software built using the 3DES (Triple Data Encryption Standard) algorithm. The 3DES algorithm is a flow algorithm (block cipher) which belongs to the type of symmetry key cryptography system. The implementation of the 3DES algorithm on software that is built using the Java-based programming language Java. So only software that uses the Android operating system can use this encryption and decryption application.

1. Introduction

Along with the times, human needs for information and communication technology also increased. One of the communication device technologies is a mobile phone or known as a cellular phone. Mobile phone is a primary need for people who need information and communication throughout the world. In Indonesia, mobile phone is commonly used, the users are from all of ages. Mobile phone has standard voice communication facilities, namely telephone and SMS (Short Message Services). In everyday life, SMS facilities are the choice of many people to communicate because it is relatively cheap, easy, clear and fast [1]

The messages sent are stored first in the SMSC (Short Message Service Center). This is an advantage of the SMS service that can still send messages even though the destination mobile phone is busy. But it is also becomes a security gap for SMS services. This is due to the attacker can infiltrate the SMSC to get messages stored in the SMSC before being sent to the destination of mobile phone.

This is very important to note when mobile phone users want to send important and confidential messages. To reduce the risk of the security gap, one method that can be applied is to use cryptographic techniques or encrypt the sent messages. Altough, even if the attacker manages to infiltrate the SMSC and get a message, it will be difficult to find out the contents of the encrypted message [2].

One of cryptographic method is 3Des (Triple Data Encryption Standard), 3DES is an enhanced and far more complicated version of DES achieving a high level of security by encrypting data using DES three times using three different DES keys [3].

2. Related Works

The DES algorithm is the most widely used encryption algorithm in the world adopted by NIST (National Institute of Standards and Technology) as the US Federal information processing standard. The plaintext data is encrypted in 64-bit blocks into 64-bit ciphertext data using an internal key 56 key. DES transforms 64-bit input in several stages of encryption into 64-bit output. Thus, DES includes block ciphers. With the same stages and keys, DES is used to reverse encryption. The internal key in the DES algorithm is generated from a 64-bit external key [4].

3. Research Methodology

3.1 System Design

At this stage the author designs an application / program. The author designs an SMS text encryption program to assist the users send secret messages, using Android-based Java programming language[5]. The first step in designing this program is to design a system work process using a scheme that explains in detail the processes that will be carried out by the program until text text encryption can be run. Next designing the form of program display (User Interface).

3.2 System Implementation

System implementation is the final stage in the process of creating this application. At this stage the author does runing or testing the program in advance of the application that has been made. The program test aims to anticipate errors so that errors can be corrected immediately before they are implemented. After there are no more errors, then this system can be directly implemented to system users [6].

3.3 Network System Scheme

The SMS encryption network system scheme built in this study is illustrated in Figure 1 [7].

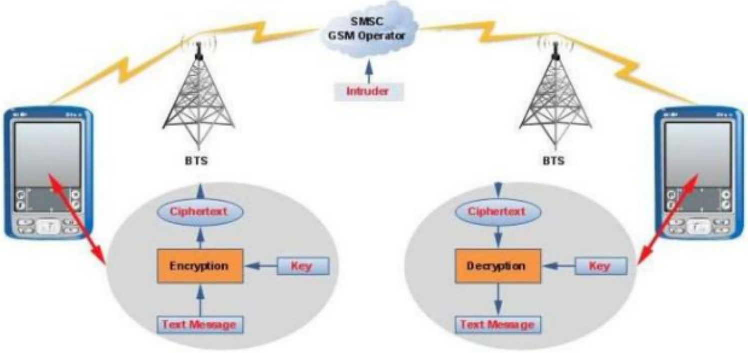


Figure 1. Encryption Process on SMS

Based on the picture above, the encryption application system can be described as follows:

a. The application is installed on both mobile phone and run first then type the message in the available textbook, the message is encrypted and the user can continue the process of sending messages.
b. The message is sent to the SMSC via the GSM network by passing several Base Transceiver Station (BTS) first (the message is not directly sent to the recipient's mobile phone, but through the SMSC first).
c. In the previous BTS (closest to the SMSC) the message is sent to the SMSC via a cable network. In this SMSC messages that have been encrypted are temporarily stored for information needs such as delivery reports, pending or failed status.
d. Then it is forwarded by one BTS to another BTS to the BTS that serves the recipient's mobile phone network.
e. When a message is sent to the sender's mobile phone application, the recipient's mobile phone will know that there is an incoming message on the specified port, then displays the results to the user that there is a message.
f. The recipient who approves the read message then the system performs the decryption process on the message and displays the results to the user.

4. Result and Discussion

4.1 System Analysis

In a computer-based system design process, problem analysis plays an important role in making detailed applications that will be developed, problem analysis is a step to understanding the problem before taking an action or final settlement decisions. System analysis aims to identify the problems that exist in the system, where the applications built include the operating environment, user and related elements. This analysis is the basis for the stages of system design, which includes selecting a sample, determining the mobile phone can support in running the application to be built and determining the binary code summarized in the number of characters that will make the sample in the system testing, and the measurement of time during the encryption process and description of data on the system.

4.2 System Design

In designing this application there are two dominant processes that apply in this system, namely encryption and decryption. In the encryption process, the data in the text input SMS form will be changed by the algorithm 3 Des (Triple Data Encryption Standard) cryptography which produces chipertext in hexadecimal form. Next, the decryption process will be carried out, which is to return the chipertext in the hexadecimal form to the plantext return.

The design aims to provide an overview of the system will be built and understand the flow of processes in the system. The design will begin after the system analysis phase has been completed. Design can be defined as depiction. Started with the entry of users into the application and immediately enter the main menu, if you want to encrypt text sms, users can directly select the menu available in the main menu, such as the SMS encryption menu. If the user wants to decrypt SMS text, the user can directly select the SMS decryption menu.

Activity Diagram focuses on describing the sequence of activities in a process. This Activity Diagram has a diagram structure similar to a flowchart or data flow diagram in a structured design, and is useful to help understand the overall process. The following Activity Diagram for SMS encryption application.

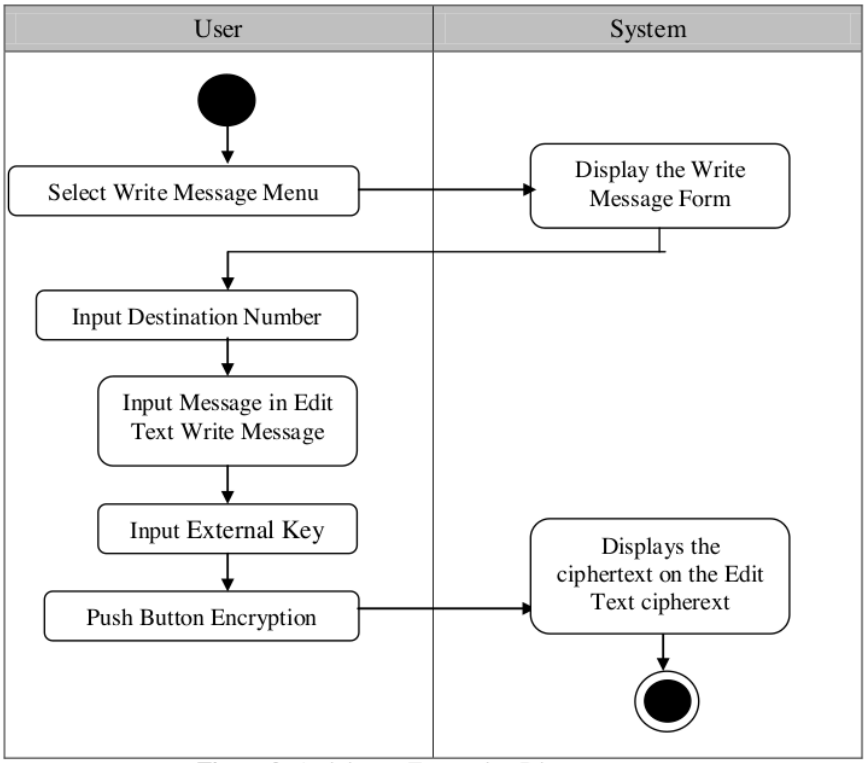

User
System
Select Write Message Menu
Display the Write Message Form
Input Destination Number
Input Message in Edit Text Write Message
Input External Key
Push Button Encryption
Displays the ciphertext on the Edit Text cipherext

Figure 2. Activity on Encryption Diagram

From Figure 2 above it can be seen that the user is doing the encryption process. In this process the user must input the message to be encrypted then the user inputs the external key then the user chooses the encryption button then the system will respond by displaying the chipertext on the edittext provided.

Table 1. Message Encryption Specifications

Use Case	Encryption the message
Actors	User
Descriptions	This Use Case describes the process of encrypting ordinary messages

Preconditions	Write Message Menu	
Post Conditions	Display the Write Message Form	
	Actor Action	*System Respon*
Success Scenario	1. This use case starts when the user is already on the message form.	
	2. Users input messages that will be encrypted on edittext write messages and input external keys.	
	3. User push Encryption button	The system displays ciphertext on edittext chiperteks

4.3 How the DES Algorithm Works (Data Encryption Standard)

The steps to encrypt data using the DES (Data Encryption System) algorithm are:
Plaintext (ptx) = 1q2w3e4r
Key (k) = /.,mnbvc
First Step:
Change (ptx) and (k) into binary form:
Binary (ptx) = 00110001 01110001 00110010 01110111 00110011 01100101 00110100 01110010
Biner (k) = 00101111 00101110 00101100 01101101 01101110 01100010 01110110 01100011
Second Step:
Performs Initial Permutation (IP) in the plaintext bit using the following IP table:

Table 2.Table of Initial Permutation (IP)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

The sequence of bits in the 58th plaintext is placed in position 1,
The sequence of bits in plaintext in the 50th order is placed in position 2,
The sequence of bits in the 42nd plaintext is placed in position 3, etc.

Furthermore, due to this application using 3 key (key) or 3DES algorithm, it must doing by the internal key generation process again with:
Key (k)2 = 12345678
Key (k)3 = qwertyui
Then doing the DES algorithm again as above with the second and third keys. Then the last result will produce ciphertext in hexa form, like: ceb25fdc56ad6e9e.

5. Conclusion

The conclusions obtained from this study are as follows:

1. The process of text encryption and decryption with the 3DES (Triple Data Encryption Standard) algorithm was done by implementing the DES algorithm three times.
2. With the cryptographic application developed based on the 3DES (Triple Data Encryption Standard) algorithm, the important data can be secured (encrypted) when sending by SMS.
3. Encrypted messages cannot be understood if they are not decrypted using the correct key. So that only eligible recipients can read it.
4. The results of this study are creating an SMS application on an Android-based Smartphone that can send and receive text messages.

References

[1] M. Aprilianto and M. Abdurohman, “Improvement Text Compression Performance Using Combination of Burrows Wheeler Transform, Move to Front, and Huffman Coding Methods,” in *Journal of Physics: Conference Series*, 2014, vol. 495, no. 1, p. 12042.

[2] R. Firdaus, R. Damanik, and D. Kurniawan, “Application of Secret Message Encryption for Shipping Sms Using Arc4 Algorithms in Mobile Technology Equipment,” 2010.

[3] A. R. Zain, “Analysis of Technical Performance and SMS Security Algorithm.”

[4] E. Melati, R. Passarella, R. Primartha, and A. Murdiansyah, “Design and Manufacture of Blood Type Detectors Using Microcontrollers,” *J. Ilmu Komput. dan Teknol. Inf. (Jurnal Generic)*, vol. 6, no. 2, pp. 48–54, 2011.

[5] A. F. Mayprana, “Utilization of Hill Cipher Algorithm and Multiprime RSA Algorithm in Hybrid Schemes on Android-Based Short Message Service (SMS) Applications,” 2018.

[6] T. Sutabri, *Analisis sistem informasi*. Penerbit Andi, 2012.

[7] R. K. Hondro, “Application of SMS Encryption and Decryption with ZIG ZAG Algorithm on Android-based Mobile Phone,” *Pelita Inform. Inf. dan Inform.*, vol. 10, no. 3, 2018.

Sms Encryption Application Using 3Des (Triple Data Encryption Standard) Algorithm Based on Android

ORIGINALITY REPORT

10%	9%	3%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	repository.unimal.ac.id Internet Source	2%
2	hdl.handle.net Internet Source	2%
3	Ratnadewi ., Benny Santoso Sugiharto, Nuning Kurniasih, Dahlan Abdullah et al. "Visual Cryptography with RSA Algorithm for Color Image", International Journal of Engineering & Technology, 2018 Publication	1%
4	ce.sharif.edu Internet Source	1%
5	link.springer.com Internet Source	1%
6	Submitted to Universitas Negeri Surabaya The State University of Surabaya Student Paper	1%
7	ojs.uho.ac.id Internet Source	1%

8	lamintang.org Internet Source	<1 %
9	Ana Grbovic, Ivana Ognjanovic, Ivan Vuckovic. "Security of AMR system in HPP Perucica", 2018 23rd International Scientific-Professional Conference on Information Technology (IT), 2018 Publication	<1 %

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		