Journal of Sisfotek Global
ISSN (Online): 2721 - 3161, ISSN (Print): 2088 – 1762
DOI: http://dx.doi.org/10.38101/sisfotek.v12i2.540
Vol. 12, No. 2, September 2022, pp. 87-93

Implementation Of Rivest Chiper 6 and Blowfish Algorithm for Mobile-Based Message Cryptography

Ari Amir Alkodri[1], Supardi[2], Risky Maulana[3], Liza Fahreni[4]

[1,2,3,4] ISB Atma Luhur, Pangkalpinang, Indonesia, 33117
e-mail: *[1]arie_a3@atmaluhur.ac.id, [2]supardi@atmaluhur.ac.id, [3]1411500049@atmaluhur.ac.id, [4]lizafahreni87@gmail.com

ARTICLE HISTORY

Received : August 29th, 2022
Revised : September 15th, 2022
Accepted : September 19th, 2022

KEYWORDS

Message Security
Encryption
Rivest Chiper 6 and Blowfish algorithms

ABSTRACT

The development of technology in recent years has been very rapid, there are still many people who use short message technology, but the security aspect is not guaranteed. People who exchange information are at risk of having information content theft during the delivery process, for that it is necessary to encrypt messages before sending and decrypt them to be read so that they are not easily misused by unauthorized people. With Rivest Cipher 6 and Blowfish cryptographic algorithms, this model is a symmetric key algorithm in the form of a block cipher that can answer message security. This method is suitable for maintaining message security. In this paper, a number of aspects of cryptography will be discussed as well as the basic concepts of cryptography. The purpose of the application is designed to be able to implement the Rivest Ciper 6 and Blowfish algorithms. Rivest Chiper 6 and Blowfish algorithms implemented on android smartphones can encrypt messages before they are sent and decrypt messages when they are received, by using two message security encryption options, users can distinguish the results of the two algorithms and become more secure. In the encryption and decryption process, a key is needed to scramble and restore the contents of the message. The key is obtained when the sender and recipient met previously can also send the key through the application but the key sent will be immediately deleted by the application so that others do not know the key to open the message.

1. Introduction

The development of technology for the past few years has been very rapid, especially in information technology, one of which is cellular telephones. The features and sophistication of cellular phones began to appear until the so-called smartphone, which has various functions such as multimedia, multiplayer games, data transfer, video streaming and others.

Smartphones have many features, but many people still use old features such as short message services or SMS (Short Message Service) via smartphones. SMS is one of the facilities provided by smartphones to send data in the form of short messages. However, with the existing SMS facility, the question begins to arise if someone wants to send confidential information through the SMS facility whether the security of the SMS can be guaranteed so that the contents of the SMS can only be read by the sender and the recipient. Along with current technological developments, there are also problems related to the level of security of these services[1]. The ease of exchanging information via SMS is abused by some people in various ways trying to steal information.

To secure SMS using Cryptography, there is an encryption and decryption process. Encryption is the process of converting plaintext (readable messages) into ciphertext (unreadable messages). The opposite of Encryption is Decryption. By encrypting the contents of the SMS, the level of information security of a message can be increased.

Research [2] with the title implementation of the rc-6 cryptographic algorithm for securing text data. RC6 is a synchronous stream cipher that can be run with a variable key and encrypts a plaintext digit by digit with a symmetric key.

Research [3] with the title analysis and implementation of double encryption and description combination of blowfish algorithm and triple des algorithm for sms on android smartphones. The results Text messages will be encrypted using the blowfish algorithm then the message will be encrypted again with the triple DES algorithm, and SMS is sent to the recipient. The blowfish algorithm

and triple DES algorithm are implemented on android smartphones which are expected to encrypt SMS before it is sent and decrypt the SMS when it is received. By using double encryption, SMS security becomes more secure and the encryption and decryption time does not take a long time and the Avalanche Effect value is good.

Research [4] based on Comparative Analysis of Rivest Code 5 Symmetrical Algorithm with Rivest Code Symmetrical Algorithm 6. For the experiments carried out on the RC5 algorithm the execution time for the generation of keys (set -up key) is very fast, which is about 9 -10 ns, a trial carried out on the RC6 algorithm execution time for the key generator (set up key) faster than 10 -11 ns. In the encryption and decryption process, the execution time depends on the size or size of the plaintext file. The larger the size of the plaintext file, the longer the execution time.

Research [5] based on A Comparative Study MD5 and SHA1 Algorithms to Encrypt REST API Authentication on Mobile-Based Application. Based on Brute Force Attack testing the SHA1 encryption algorithm has the advantage of being stronger, but the time needed for encryption is slower when compared to the MD5 algorithm. Even though it's more tethered, the difference in encryption time needed is only 37.1 ms, so that SHA1 is still considered relevant for implementing security systems and REST API authentication on a mobile application.

Based on the background of the implementation of several previous studies as the basis and comparison of the renewal of the implementation of this research, a research will be carried Implementation of Rivest Ciper 6 and Blowfish Algorithm in Mobile-Based Short Message Cryptography.

2. Research Methods

In carrying out the research, there are several stages or steps to Implementation of Rivest Ciper 6 and Blowfish Algorithm in Mobile-Based Short Message Cryptography. The research model used in this study is the waterfall model. The waterfall model has several stages that will be carried out for this research. The stages in the waterfall model [6], namely:

2.1 System Development Model

The research model used in this study is the waterfall model. The waterfall model has several stages that will be carried out for this research. The stages in the waterfall model, namely:

a. Needs analysis

The process of gathering requirements is carried out intensively to specify software requirements so that it can be understood what kind of software users need.

b. System design

Software design is a multi-step process that focuses on the design of a software program including data structures, software architecture, interface representation, and coding procedures. This stage translates software requirements from the requirements analysis stage to the design representation so that it can be implemented into a program at a later stage. The software design produced at this stage needs to be documented.

c. Program code generation

In this third stage, the design must be transformed into a form that can be understood by the machine, namely into a programming language through the coding process. This stage is the implementation of the design stage.

d. Testing

The fourth stage is the application testing process from the needs of each previous stage to ensure that there are no more errors or bugs in the application made.

e. Program implementation

The final stage in the waterfall model. Software that has been finished, run and carried out maintenance. Maintenance includes fixing errors not found in the previous step as well as application development such as adding new features [7].

The waterfall model is very suitable for user needs that are well understood and the possibility of changing requirements during software development is small. The positive thing about the waterfall model is that the structure of the system development stage is clear and a stage is executed after the previous stage is completed. This model is used because it is a practical method and quite cost-effective because all the parameters needed and the desired results can be directly modeled and simulated using a computer program (Personal Computer) in the form of software.

2.2 Object Oriented Programming Method

Object-oriented programming is used in this paper because it has many advantages in handling complex tasks. With OOP the codes that we make are more neat and structured, the process of reusing the codes that we make for almost the same project, is easy because the code we make is neat and structured. So to change or reuse code is not difficult anymore, the concept is per module. If the error is definitely easy to spot because it can be read from the function we call, it will make it easier for us to create and read our code (code efficiency). The concept of OOP also makes it easier for us to analyze the program we are going to make, this will be very pronounced if we make large and difficult programs[8].

2.3 System Development Tools

At this writing, the tools or tools used to develop the system are UML (Unified Modeling Language) tools, which consist of [9] [10]:

a. Use Case Diagrams

Use Case Diagram is a system modeling consisting of actors and then connected with use cases on the system that is made, this diagram illustrates how the connection between actors and application systems.

Through the use case diagram, it can be seen what functions are contained in this cryptography application system and short message compression.

b. Activity Diagrams

Activity Diagram describes the flow of work (work flow) or activities of a system. Activity diagrams display activities that occur in the use case, not what actors do, but activities that can be performed by the application system.

d. Class Diagrams

Class diagrams are the essence of object-oriented design and development, as well as how users and application systems can interact with each other to get the desired results.

e. Sequence Diagrams

Sequence Diagrams in this study describe the interaction between objects in the form of sending data between objects in the system that are arranged in a sequence or time series. The interaction between objects can be in the form of messages (messages), users (users), and displays (displays).

2.4 Rivest Chiper 6 (RC6) and Blowfish Algorithm

In this study, the researcher implemented an application with the Rivest Chiper 6 (RC6) and Blowfish algorithm[11]. This algorithm will be applied in the encryption and description process in the application that will be made by the researcher [12]. This algorithm is used for the process of encrypting and decrypting messages so that they are kept safe [13][14].

3. Results and Discussion

3.1 Encryption and Decryption Process

The RC6 algorithm works with four registers A, B, C, D, each of which is w-bit in size, these registers will be filled by plaintext which will then be used during the encryption process and after the encryption process ends the contents of these registers are ciphertext. The first byte of plaintext or ciphertext will be stored in the least significant byte of A and the last byte of plaintext or ciphertext will be stored in the most significant byte of D. The encryption and decryption process of the RC6 algorithm uses six basic operations:

1. a + b = summation integer modulo 2w
2. a - b = subtraction integer modulo 2w
3. a $\oplus$ b = operation bitwise exclusive-or as big w-bit words
4. a * b = multiplication integer modulo 2w
5. a<<<b = rotation of w-bit word to the left as much as the number given by the least significant lg w bit of b.
6. a>>>b = rotation of a number of w-bit words to the right by the number given by the least significant lg w bit of b.

The steps for encryption of the RC6 algorithm in detail are as follows:

1. The plaintext block is divided into 4 parts A, B, C and D, each of which has a length of w bits or the block length is divided 4. Then B and D are added up (in modulo 2w) with the internal keys S[0] and S[1].
2. Next in each round from 1 to r, do XOR and shift to the left of A with f(x) shifted to the left by lg w, where f(x) = x* (2x+1) and x = B. After that do the sum (in modulo 2w) with the internal key. The same thing is also done for C with x = D. Then swapping A B, B C, C D and D A
3. After the iteration is complete, the last step is to add (in modulo 2w) A and C with the last two internal keys. After all the blocks are divided into 4 parts put back together.

The RC6 algorithm is an iterated cipher, the main strength of this algorithm lies in the iteration it does. By doing repeated iterations using different keys, the principles of confusion and diffusion are carried out repeatedly, so security will be better.

The best attack to crack the RC6 algorithm is an attack using exhaustive search aimed at the key entered by the user or the internal key. For more complex attacks such as differential and linear cryptanalysis, it can be used to solve the RC6 algorithm that uses a small number of rotations, for the number of rotations of 20 and above, this attack cannot work well because it is difficult to find good iterative characteristics or linear estimates[15][16].

3.2 Formation of Internal Keys

To generate the internal key sequence that will be used during the encryption process, the RC6 algorithm performs a key building process that is identical to the RC5 algorithm, the only difference being in the RC6 algorithm, the number of words taken from the key entered by the user when encrypting or decrypting is more. The purpose of the key development process is to build an array S of size 2r+4 from the user input key of b bytes (0 b 255), the array will be used both in the encryption and decryption process. The process of building internal keys using two constants is called the "magic constant". The two magic constants Pw and Qw are defined as follows:

Pw= Odd((e-2)2w) ..... (1)
Qw= Odd((-1)2w) ..... (2)

Where:

E = 2.7182818284859 (the base of the natural logarithm)
=1.618022988749 (golden ratio)

Odd (x) is the closest odd integer to x, if x is even then an odd integer is taken after x.

Here is a list of magic constants at various block lengths in hexadecimal:

P16 = b7e1
Q16 = 9e37
P32 = b7e15163

Q32 = 9e3779b9
P64 = b7e151628aed2a6b
Q64 = 9e3779b97f4a7c15
The key generated by this key generation process is one-way, so this key generation process can be used as a one-way hash function.

3.3 Use Case Diagram

The following is a display of the use case diagram where the actors are the user and SMS RC6, Inbox RC6, SMS Blowfish, Inbox Blowfish and About. Can be seen in Figure 1

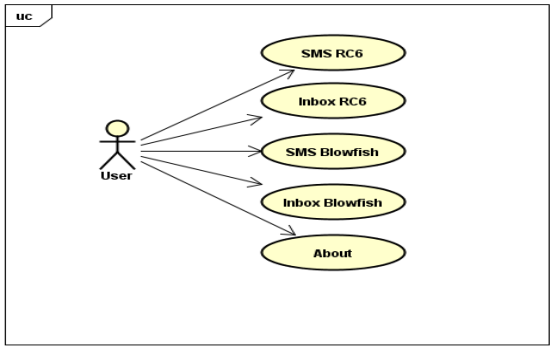

Figure 1. Application Diagram Use Case

3.4 Activity Diagram of The Application

The following is an image of the application activity diagram, which can be seen in Figure 2 below:

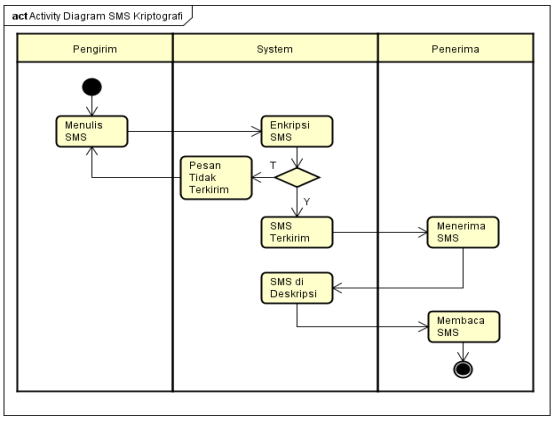

Figure 2. Application Activity Diagram

3.5 Application Diagram Sequence

The following is a display of the SMS RC6 sequence diagram and the SMS Blowfish sequence diagram can be seen in Figure 3 and Figure 4 below.

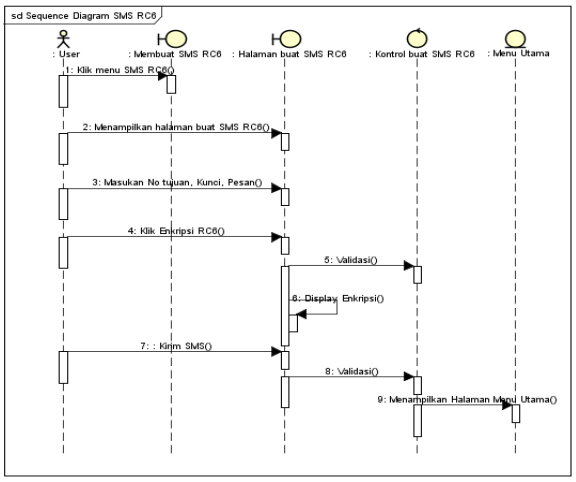

Figure 3. Application Activity Diagram

The following is a sequence diagram of SMS Blowfish.

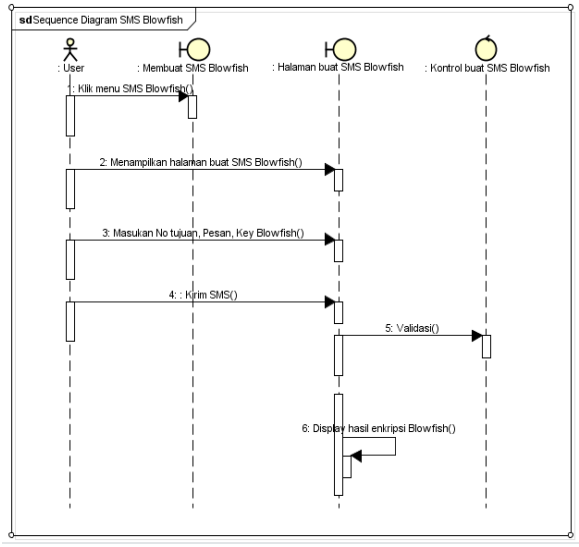

Figure 4. Application Activity Diagram

3.6 Implementation

a. Main Menu Screen Display

Screen display The main menu will appear on the smartphone screen when opening the application, there are several menus including: SMS RC6 Menu, RC6 Inbox Menu, SMS Blowfish Menu, Inbox Blowfish Menu and About can be seen in Figure 5 below

Figure 5. Main Menu Screen Display

b. RC6 SMS Screen Display

The SMS RC6 screen display will appear when pressing the SMS RC6 menu where the user when you want to send an RC6 SMS must fill in the destination number, key and message then press the RC6 encryption button to see the results of the RC6 encryption algorithm and press the send button to send SMS can be seen in Figure 6 below

Figure 6. RC6 SMS Screen Display

c. Screen Display Of RC6 SMS Reading Menu

The screen display of the RC6 SMS reading menu will appear when pressing a message in the SMS list where there is a sender number, message, key and the results of the RC6 algorithm description. that appears in the results can be seen in Figure 7 below

Figure 7. RC6 SMS Reading Menu Screen Display

d. Blowfish SMS Screenshot

The SMS Blowfish screen display will appear when pressing the SMS Blowfish menu where the user when you want to send a Blowfish SMS must fill in the destination number, message and key then press the send button then the message is encrypted by the Blowfish algorithm and sent to the destination number can be seen in Figure 8 below

Figure 8. Blowfish SMS Screenshot

e. Blowfish Inbox Screenshot

The Blowfish Inbox screen display will appear when pressing the Blowfish read button where there is a Blowfish description key and a Blowfish Search button, if the user wants to see the SMS description results the user must fill in the key according to the Blowfish encryption key then press the Blowfish Search button to see the Blowfish algorithm description results which will only appear, can be seen in Figure 9 below

Figure 9. Inbox Blowfish Screenshot

3.7 Result of implementation

In the tests carried out by sending SMS via a test delivery number with Rivest Ciper 6 with the message "how are you" with the key determination "27" then the resulting encryption AAD92CE1A8C0924A59366203 C7F50B77, while using the same SMS text as the message "how are you" with the determination of the key "27" In the Blowfish Algorithm, the qlyKe1oE0s5h5EYX7MnRgg encryption is generated.

4. Conclusions And Suggestions

Based on the results of the tests carried out as follows:

1. By using different key lengths in the encryption process carried out on the same amount of text, the processing time does not experience a big change
2 Compared to the RC6 and Blowfish algorithms, the RC6 algorithm is a simpler, faster, and more secure encryption algorithm.
3. The application of private key algorithms for SMS encryption on smartphones can increase security. An encrypted message cannot be read if it is not decrypted using the correct key.

References

[1] Arifin, Yusuf. 2015. Sistem Monitoring Keamanan Jaringan Melalui SMS Alert Dengan Snort Dan SMS Gateway. STMIK Akakom : Yogyakarta.

[2] Eko Juliansyah, 2017, Implementasi Algoritma Kriptografi RC-6 Dalam Mengamankan Data Text, Volume 16 Number 3.

[3] Guntur Tri Wibowo, R.Rumani M., Randy Erfa Saputra, 2015, Analisis Dan Implementasi Enkripsi Dan Dekripsi Ganda Kombinasi Algoritma Blowfish Dan Algoritma Triple Des Untuk Sms Pada Smartphone Android Analysis And Implementation Of Double Combination Encryption And Decryption Using Blowfish And Triple Des Algorithm For Sms On Android Smartphone, Vol.2 No.2.

[4] Rozali Toyib, Ardi Wijaya. 2018, Analisis Perbandingan Algoritma Simetris Rivest Code 5 Dengan Algoritma Simetris Rivest Code 6, Vol.2 No.2.

[5] De Rosal Ignatius Moses Setiadi et al. 2019. "A Comparative Study MD5 and SHA1 Algorithms to Encrypt REST API Authentication on Mobile-Based Application." 2019 International Conference on Information and Communications Technology, ICOIACT 2019: 206–11.

[6] Guntoro. 2020. "Metode Waterfall: Pengertian, Tahapan, Contoh, Kelebihan dan Kekurangan" https://badoystudio.com/metode-waterfall/. Diakses pada 27 Juni 2022.

[7] Roger S. Pressman, Bruce R. Maxim, 2014. Software Engineering : A Practitioner's Approach. 2 Penn Plaza, New York.

[8] D. T. Alan Dennis 2015, Barbara Haley Wixom, Analisis & Desain Sistem Pendekatan Berorientasi Objek dengan UML.

[9] H. Sensen and U. E. Unggul, 2019 "Unified Modelling Language ," Syst. Model., no. July, pp. 0–5.

[10] D. Wira, T. Putra, and R. Andriani, 2019 "Unified Modelling Language (UML) dalam Perancangan
Sistem. Informasi Permohonan Pembayaran Restitusi SPPD," vol. 7, no. 1.

[11] Deden Sukmana, Sugiarti. 2022, Prototype Penerapan Hasil Kombinasi Kriptografi Diffie-Hellman, Message-Digest 5 Dan Rivest Chiper 4 Pada Layanan Pesan Singkat Smartphone Android. JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika) Volume 07, Nomor 03 : 926–934

[12] Sebastian Suhandinata,Reyhan Achmad Rizal, Dedy OngkyWijaya, Prabhu Warren, Srinjiwi, 2019. Analisis Performa Kriptografi Hybrid Algoritma Blowfish Dan Algoritma Rsa. JURTEKSI (Journal of Information Technology and Systems) Vol. VI No. 1, hlm. 1 – 10.

[13] Yusfrizal, 2015, Penerapan Algoritma Rc6 Untuk Perancangan Aplikasi Pengamanan Sms Pada Mobile Device Berbasis Android.

[14] Dedy Abdullah, Doni Nugroho Saputro, 2016, Implementasi Algoritma Blowfish Dan Metode Least Significant Bit Insertionpada Video Mp4.

[15] Ari Amir Alkodri. 2020, Use of the Advanced Encryption Standard Algorithm for Encryption Short Message Service on Real Count Applications. 2020 8th International Conference on Cyber and IT Service Management (CITSM).

[16]Dwi Setiawan 2018, Implementasi Algoritma Rivest Chiper 6 Untuk Kriptografi Pesan Chatting Berbasis Mobile. Universitas Teknologi Yogykarta.