Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 6, Number 2, April 2022
DOI : https://doi.org/10.33395/sinkron.v7i2.11391

e-ISSN : 2541-2019
p-ISSN : 2541-044X

# Rivest Cipher 6 Algorithm Method to secure messages of Medical Record files at Perlayuan Health Center

**Aldi Rapandi Ritonga**[1)*], **Deci Irmayani**[2)] **Ali Akbar Ritonga**[3)]
[1)2)3)]Universitas Labuhanbatu, Indonesia
[1)]aldirafandi922@gmail.com, [2)]deacyirmayani@gmail.com, [3)]aliakbarritonga@gmail.com

**Submitted**: Jan 19, 2022 | **Accepted** : Jan 25, 2022 | **Published** : Apr 27, 2022

**Abstract:** This study aims to provide an effort to secure files in order to maintain important documents as assets for the Perlayuan Health Center. The Perlayuan Health Center is one of the world's health units whose role is to support health and the security of medical record files. Important factual documents that have been recorded regarding the historical history of symptoms and diseases that have been recorded such as disease or illness conditions, prevention or healing techniques that have been carried out and have been missed have previously been documented by the Health service at the Perlayuan Health Center. Medical records have or keep important records that are documented with data in the form of patient identities, examinations, treatment, actions from the facilitators of the Perlayuan Health Center. Rivest's Cipher 6 method is used to lock files. The medical record aims to be an initial benchmark to continue the action plan for drugs and treatments that will be applied. File security with At the Perlayuan Health Center there is very little security for a file because each data is not only stored on one computer and if needed the file will be copied to anyone who asks for the file. That way the file is no longer guaranteed security and confidentiality. Anyone can easily retrieve files by copying formatted encryption or data encryption. Rivest's Cipher 6 algorithm can break 128 bits blocks into 4 sets of 32 bits and this algorithm can work with 4 32 bits registers X, B, Y and D.

**Keywords:** Medical Record Files; File Protection; Perlayuan Health Center; Medical; File

## INTRODUCTION

Confidentiality and data security are very important things in communication, both for the purpose of shared security and for individual privacy, so the current development of science and technology has affected all aspects of human life. Information and data can be easily and quickly sent over the network and therefore security problems arise which are currently often ignored or even ignored, so currently it is necessary to emphasize data security in order to reduce the risk of data leakage (Juliansyah, 2017). At the Perlayuan Health Center there is still very little security for a file because every data is not only stored on one computer and if needed, the file will be copied to anyone who asks for the file. That way the file is no longer guaranteed security and confidentiality. Anyone can easily retrieve files by copying and one way is data encryption or encryption. Copying files will be very detrimental if there are parties who intentionally manipulate data in the form of important documents about medical diagnoses, medical documents, medical consultations, medical services and recordings of treatment results. Economically, the losses felt by the Perlayuan Health Center in the form of important documents that can be traded, for example, are falsification of data in the form of patient identities, examinations, treatment, and consultations. Non-material losses are felt in the form of distrust of the Public health center. Leadership to the waiters who carry out their duties so as to create conditions for the Public health center.  that are less comfortable. Events that make it necessary to secure medical record files at the Perlayuan Public Health Center are when there are cases in patients who already have an archive of Health development data that has previously been diagnosed with the type of disease with laboratory equipment, photos and clinics and there is already a medical record of the results that have been consulted but there are the crime party outside the list intentionally made a document that was not in accordance with the recording of the results of the treatment, the Perlayuan Public health center.  had the right to refuse and make a statement that the existing data was considered a crime that could harm the Public health center.

*name of corresponding author

## LITERATURE REVIEW

The RIVEST CIPHER 6 algorithm uses 44 sub-keys generated from the key and named S [0] to S [43]. Each sub key is 32 bits long. The encryption process in the RIVEST CIPHER 6 algorithm begins and ends with a whitening process that aims to disguise the first and last iterations of the encryption and decryption process. In the initial whitening process, the B value will be summed with S [0], and the D value will be added with S[i]. In each iteration of RIVEST CIPHER 6 using 2 sub keys. The sub keys in the first iteration use S [2] and S [3], while the subsequent iterations use the subsequent sub-keys. After the 20th iteration is complete, the final whitening process is carried out where the value of A is added to S [42], and the value of C is added to S [43]. Each iteration of the RIVEST CIPHER 6 algorithm follows the following rules, the value of B is entered into the function f, which is defined as f(x) =x(2x+1), then rotated left as far as lg-w or 5 bits. The results obtained in this process are assumed to be u. The value of u is then XORed with C and the result is the value of C. The value of t is also used as a reference for C to rotate the value to the left. Likewise with the value of u, it is also used as a reference for the value of A to carry out the process of turning left. Then the subkey S[2i] in the iteration is added to A, and the subkey S[2i+1] is added to C. The four parts of the block will then be exchanged following the rules, that the value of A is assigned to D, the value of B is assigned to A, the value of C is assigned to B, and the (original) value of D is assigned to C. RIVEST CIPHER 6 algorithm Decryption The ciphertext decryption process in the RIVEST CIPHER 6 algorithm is a reversal of the encryption process. In the whitening process, if the encryption process uses an addition operation, then the decryption process uses a subtraction operation. The sub key that is used in the whitening process after the last iteration is applied before the first iteration, and vice versa the sub key that is applied to the whitening process before the first iteration is used in the whitening after the last iteration. As a result, to perform decryption, all that has to be done is simply to apply the same algorithm as encryption, with each iteration using the same sub-key used during encryption, only the order of the sub-keys used is reversed. According to Denny Kurniawan (2018) Encryption is a process of converting the original message into unreadable characters. Therefore security. In recording the results of treatment at the Perlayuan Health Center, a security system is needed in encoding document files so that the document does not easily fall into the hands of unauthorized parties.

In manual calculations, the RIVEST CIPHER 6 algorithm is given a key of 16 bytes and plaintext of 128 bits (16 bytes). The key and plaintext that become the ciphertext. An example of this process is a document in the form of a file: Next, determine a key, which is as follows: Key: TODAY IS HAPPY. By adding up each decimal place in the key block, we get the sub key result. Here is the algorithm to get the S-Key:

```
Word 32 type: 32 bit (32 bit data type)

Key: String {key entered by user} I, j, c, s, v: integer
A: integer B: Integer
S: array [0.43] of word 32 L: array [0.43] of word 32 Function
ROTL (X: Word 32; y: integer) – Word 32 {function to rotate the number of bits by the second variable}
Input Algorithm (key)
S (0) – b7e15163
For I – 1 to 43 do
S[i] – s[i-1] + 9e3779b9
Endfor
A – B – I – j – 0 V – 44
If {c>v} then v – c
vv*3
For s – 1 to v do
A – S[i] – ROTL ((S[i] + A + B). 3
S – L[j] = ROTL (L[j] + A + B, A + B)
I – (i+1) mod 44 J – (j+1) mod c Endfor
```

The RIVEST CIPHER 6 algorithm that will be used in the application is built with w of 32 bits, r of 20 rounds and key lengths of more than 1 character (8 bits). So that the following results are obtained:

Table 1 Creating S-Key

| | | | |
|---|---|---|---|
| S [0]: 3650025825 | S [5]: 1216673212 | S [10]:4616673522 | S [15]:3242634689 |
| S [1]: 1216675275 | S [6]: 5216631276 | S [11]:4416273455 | S [16]:1908760767 |
| S [2]: 3003935261 | S [7]: 1616659615 | S [12]:3115435434 | S [17]:2097492399 |
| S [3]: 3414676270 | S [8]: 2286673271 | S [13]:5166752754 | S [18]:2982298321 |
| S [4]: 5216675835 | S [9]: 3213625425 | S [14]:5616678567 | S [19]:4042651233 |

*name of corresponding author

By adding up each decimal place in the key block, we get the sub key result. The RC6 algorithm that will be used in the application is built with w of 32 bits, r of 20 rounds and key lengths of more than 1 character (8 bits). Furthermore, in applying the RC6 algorithm to plaintext, the first step is to divide the plaintext into 4 blocks, namely A, B, C, D, each block consisting of 32 bits (4 characters). Plaintext: Registration and Identification (Ranmor).docx Which if converted into binary form is:

Table 2. Document Conversion Results

01010000 01000101 01001100 01001001
01010100 01000001 00100000 01001110
01010101 01010011 01000001 01001110
01010101 01010011 01000001 01001110

Change each character in each block into ASCII values, then change the ASCII values into their respective binary numbers. 8 bits long, so that each block will produce a 32-bit binary number.

Binary 1 01010000 01000101 01001100 01001001
Binary 2 01010100 01000001 00100000 01001110
Binary 3 01010101 01010011 01000001 01001110
Binary 4 01010101 01010011 01000001 01001110

Then the binary numbers in plaintext are combined again, with the rule that the first byte of plaintext is placed in the least significant bit block A. And the last byte of plaintext is placed in the most significant bit block D

Block A: 01010000010001010100110001001001

In decimal = 1346718793

Block B: 01010100010000010010000001001110

In decimal = 1413554254

Block C: 01010101010100110100000101001110

In decimal = 1431519566

Block D: 01010101010100110100000101001110

In decimal = 1431519566

After obtaining the value for each block, then proceed with the following steps:

Early Whitening

Initial whitening, by adding up B with sub key S (0), and D with sub key S (1). The sum is done in modulo 232
B = B + S (0) D = D + S (1)
B = B + S (0) mod 2^32
= 5063580079 mod 4294967296
= 768612783

D = D + S (1) mod 2^32
= 2648194841 mod 4294967296
= 2648194841

Iteration

*name of corresponding author

Iterations were carried out 20 times. Each iteration follows the following rules:
t ROTL ((X [1] *(2*X [1] + 1)), 5)
u ROTL ((X [3] * (2*X [3] + 1)), 5)
X [0] (ROTL ((X [0] XOR t), u)) + S[2*i]
X [2] (ROTL ((X [2] XOR u), t)) + S [2*i + 1]
Temp X [0] X [0] X [1]
X [1] X [2]
X [2] X [3]
X [3] Temp

The values of t and u obtained from blocks B and D are processed with the function f(x) = x(2x+1), then proceed by shifting the values of t and u to the left as far as 5 bits.
t = (B * (2*B+1))
= (768612783 * (2 * 768612783 + 1)) mod 2^32
= (768612783 * 1537225567) mod 4294967296
= 1181531221150622961 mod 4294967296
= 3082249457
t: (in binary) = 10110111101101110110010011110001
t: (shifted by 5 bits) = 11110110111011001001111000110110
t: (in decimal) = 4142702134

The value of the last 5 bits of t which is 10110, or in decimal of 22, will be used as the shift value of block C in the next process, as far as 22 bits
u = (D * (2 * D + 1) mod 2^32
= (2648194841 * (2 * 2648194841 + 1)) mod 2^32
= (2648194841 * 5296389683) mod 4294967296
= 4420872239263326213 mod 4294967296
= 4205649925
u: (in binary) = 11111010101011010010000000000101
u: (shifted by 5 bits) = 01010101101001000000000010111111
u: (in decimal) = 1436811455

The value of the last 5 bits of u which is 11111, or in decimal of 31, will be used as a shift of block A in the next process, by 31 bits. Then the values obtained are as follows:
t = 4142702134
u = 1436811455
slider t = 22 slider u = 31
The next step is to process blocks A and C with the values that have been generated.

A = (ROTL ((A XOR t), u)) + S[2*i]
A: 1346718793, in binary = 01010000010001010100110001001001
t:4142702134, in binary = 01010101101001000000000010111111
A: (xor result) = 00000101111100001010011001110110
A: (shifted 22bit) = 001111011000000010111100001010011
A: (in decimal) = 1031895123

The value of A is summed with the subkey S (2), in modulo 2^ 32: A = A + S (2) mod 2^32
= 4035830384 mod 4294967296
= 4035830384

C = (ROT ((C XOR u), t)) + S[2*i+1]
C: 1431519566, in binary = 01010101010100110100000101001110 u: 1436811455,
in binary = 01010101101001000000000010111111 C: (xor result) = 00000000111101110100000111110001
C: (shifted by 31 bits) = 00000001111011101000001111100010

C: (in decimal) = 32408546
The value of C is summed with the subkey S (3), in modulo 2^32 C = C + S (3) mod 2^32
= 3447084816 mod 4294967296

= 3447084816

Then the value of each block is obtained: A: 1031895123
B: 768612783
C: 3447084816
D: 2648194841

The next step is to exchange block values with the rules (A, B, C, D) (B, C, D, A), so that in the first iteration, the values for each block are as follows:
A: 768612783
B: 3447084816
C: 2648194841
D: 1031895123

The value of each block will be continued in the next iteration 20 times.
So that the final results in the 20th iteration are as follows:
Block A: 10101101100000101110001110111011 0
In decimal = 2911225718
Block B: 10100100100000001010000101110011 0
In decimal = 2759934694
Block C: 01111101000010000001100100100111 1
In decimal = 2097689167
Block D: 01001011001011001110001110001101
In decimal = 1261233037

Encryption Process

In the encryption process is the step which makes the original text into a new form (ciphertext).
Encryption Results:
Binary 1 = 01010000010001010100110001001001
S-Key 1 = 10101101100000101110001110111011 0
XOR 11111101110000001000101100111111
Binary 2 = 01010100010000010010000001001110
S-Key 2 = 10100100100000001010000101110011 0
XOR 11110000110000000110001010101000
Binary 3 = 01010101010100110100000101001110
S-Key 3 = 01111101000010000001100100100111 1
XOR 00101000010110110111001100000001
Binary 4 = 01010101010100110100000101001110
S-Key 4 = 01001011001011001110001110001101
XOR 00011110011111111010001011000011

Table 3. Encryption Results

| | | | |
|---|---|---|---|
| 11111101 | 11000000 | 10001011 | 00111111 |
| 11110000 | 11000000 | 01100010 | 10101000 |
| 00101000 | 01011011 | 01110011 | 00000001 |
| 00011110 | 01111111 | 10100010 | 11000011 |

So that the format of the contents of the document changes to be different from before. And the extension on the results is converted into encryption in order to know that the document is encrypted. Here are the results:
Ciphertext: Registration and Identification (Ranmor).enk

**Decryption Process**

The decryption process is the reverse step of the encryption process, which is to open the encrypted text into the original text (plaintext).

*name of corresponding author

Encryption Results:

Binary 1 = 111111011100000001000101100111111
S-Key 1 = 10101101100001011100011101110110
XOR 01010000010001010100110001001001
Binary 2 = 11110000110000000110001010101000
S-Key 2 = 10100100100000010100001011100110
XOR 01010100010000010010000001001110
Binary 3 = 00101000010110110111001100000001
S-Key 3 = 01111101000010000011001001001111
XOR 01010101010100110100000101001110
Binary 4 = 00011110011111111010001011000011

## METHOD

### *Research Stage*

The framework is a further explanation regarding the description of the process of the research framework carried out, along with the explanation.

a. Literature Review has the meaning of reviewing related libraries used especially in RC6. The literature review was carried out by making a critical analysis of the relationship between journal articles from the work of previous researchers, relating them to this research.

b. Analyzing the Problem Analysis of the problem is the problem that will be discussed in this study and the data that will be used in the system to be built, namely in designing a document security system with the **RIVEST CIPHER 6** method by changing the data into a new form.

c. Data Collection Data collection was carried out to obtain the information needed in order to achieve the research objectives. Researchers collect data that will be used in designing a system to secure data in the form of interviews and documentation.The interview was conducting a question and answer session to the admin section at the Perlayuan Health Center. The questions asked are as follows: 1. How is the process of securing medical record files at the Perlayuan Health Center and what are the obstacles? 2. Has there ever been a data leak in the form of patient identity, examination, treatment and medical documents. 3. Documentation Documentation according to Sugiyono (2015: 329) is a method used to obtain data and information in the form of books, archives, documents, written numbers and pictures in the form of reports and information that can support research.

d. Documentation is a method used to obtain data and information that the results of messages that have been encrypted are stored in files as medical records, it becomes confidential. secure data in the form of digital data, namely documents using the **RIVEST CIPHER 6** method which will later be input into the system and encrypted into ciphertext. As well as documents that have been decrypted and returned by decryption using the same key when encrypting the document.

e. The design in this research is to build a system to secure documents using the **RIVEST CIPHER 6** method.

f. Implementation is the application of the process of running the system that has been made, namely from the logic system applied in a structured computerized system (program), so that it can provide an overview to the user on how to run the program in order to produce the desired data.

### Data Analysis Method

Data analysis to secure medical record data in the form of digital data that will be entered into the system and encrypted into ciphertext. The work steps in value data security cryptography are adjusted to the data security architecture. In doing and completing this research, there are several things that are needed by the system such as system input requirements, process requirements and output requirements. Input requirements: Data to be used Process requirements: Rivest Cipher 6. Algorithm Output requirements: The output of the data used. At the analysis stage to be built, it begins with identifying, collecting literature studies regarding methods of cryptography, especially the Rivest Cipher 6 algorithm method. The literature study method is used by looking at existing research and referring to the research that has been done. In this case there are several analyzes that will be applied to the system to be built. Making applications by applying the Rivest Cipher 6 method as a data security algorithm. Rivest Cipher 6 encryption results if decrypted will match the original plaintext. The design is built using desktop-based applications. The Rivest Cipher 6 algorithm is a version equipped with several parameters, so it is written as RC6-w/r/b, where the parameter w is the word size in bits, r is a non-negative integer indicating the number of iterations during the encryption process, and b indicates encryption key size in bytes. When this algorithm is entered as an

AES candidate, the parameter values w = 32, r = 20 and b vary between 16, 24, and 32 bytes. The encryption function accepts input of 1 plaintext block which is divided into 4 registers, each of which is a w-bit word, namely A, B, C, and D. The resulting ciphertext is divided and stored in A, B, C, and D. In the encryption process S key table is required which is considered to have been obtained from the previous process. In more detail, the encryption process with Rivest Cipher 6 can be divided into several steps. In the following explanation, the notation (A, B, C, D) = (B, C, D, A) means that assignment operations are performed parallel (concurrently) for each element on the right-hand side to the corresponding left-hand side. The ciphertext decryption process in the Rivest Cipher 6 algorithm is a reversal of the encryption process. In the whitening process, if the encryption process uses an addition operation, then the decryption process uses a subtraction operation. The sub-key used in the whitening process after the last iteration is applied before the first iteration, and vice versa the sub-key that is applied to the whitening process before the first iteration is used for whitening. after the last iteration. As a result, to perform decryption, all that has to be done is simply to apply the same algorithm as encryption, with each iteration using the same sub-key used during encryption, only the order of the sub-keys used is reversed.

The following is a flowchart on the RIVEST CIPHER 6 method decryption process

```
 C = C – S [ 43]
A = A – S [ 42]
For i = 20 down to 1 do
{
(A, B, C, D) = (D, A, B, C)
u = (D x (2D + 1)) <<< 5
t = (B x (2B + 1)) <<< 5
C = ((C – S [ 2i + 1]) >>> t) u
A = ((A – S [ 2i]) >>> u) t
}
D = D – S [ 1]
B = B – S [ 0]
```

## RESULT

### System Testing or Implementation

The need for a data security system is in the form of a document by specifying the necessary equipment.

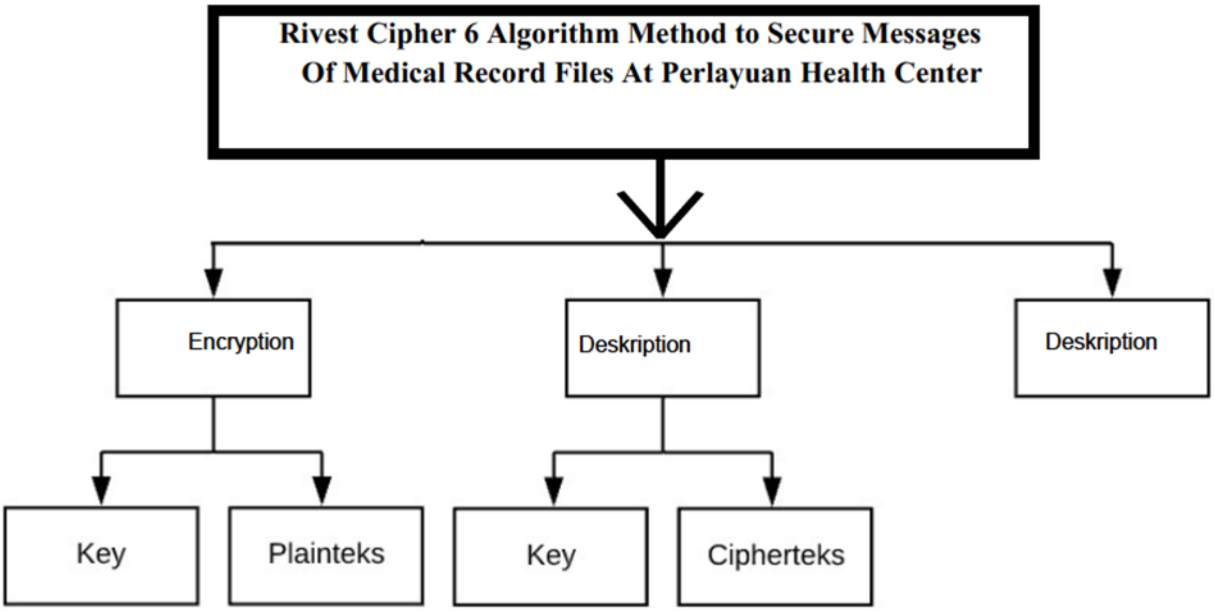
Rivest Cipher 6 Algorithm Method to Secure Messages Of Medical Record Files At Perlayuan Health Center
Encryption
Deskription
Deskription
Key
Plainteks
Key
Cipherteks

**Figure 1.** Main Menu Display

*name of corresponding author

The input design is a description of the variables or fields contained in the database tables that are used to capture data. The input design plays a very important role, because all data stored in the database table is first in the login design, specifically for admins in order to add data or update data, before the user must log in first. System design is designing or designing a good system, the contents of which are the operating steps in the data processing process and procedures to support system operations. In this implementation, it is an application in the form of steps for making the system that will be built later. In the implementation of data security using the RC6 method there are various forms of Login, Encryption, Decryption. At the stage of implementing the system, we will discuss the stages when running the system that was built. Login is a main step to enter into a system, and at the initial menu display of the program, the admin will fill in the username and password in order to enter the main menu. On this menu is to secure documents with a key as a technique in securing documents

## DISCUSSIONS

The medical record aims to be an initial benchmark to continue the action plan for drugs and treatments that will be applied. The Perlayuan Public Health Center is a community health center in serving medical consultation, medical diagnosis, medical documentation, medical services including medical records. At the Perlayuan Health Center there is very little security for a file because each data is not only stored on one computer and if needed the file will be copied to anyone who asks for the file. That way the file is no longer guaranteed security and confidentiality. Anyone can easily retrieve files by copying formatted encryption or data encryption. Rivest's Cipher 6 algorithm can break a block of 128 bits into 4 sets of 32 bits and this algorithm can work with 4 32 bit registers X, B, Y and D, so the analysis on Rivest's Cipher 5 shows that the number of rounds that occur in Rivest's Cipher 5 is not completely depending on the data contained in the block. In addition, differential cryptanalysis attacks are also proven to be able to penetrate the security offered by Rivest's Cipher 6. The security system uses cryptography in securing data using the Rivest's Cipher 6 method that was built, this application can be easily implemented because it is immediately active and easy to use. application of the Rivest's Cipher 6.  method in data or document security (*.docx) is very light to use for low-capacity laptops/computers. The results of messages that have been encrypted are saved to files in the form of medical records and medical records remain confidential

## CONCLUSION

Based The conclusion in this study is that the application of file security using the RIVEST CIPHER 6 method is quite good to use because the data that has been secured will not be easily detected by other parties because the file will change its format, with the admin key making the file difficult to hack. In the application of file security applications with the RIVEST CIPHER 6 method, it was built using the visual studio 2019 application and by using the UML design as a design medium. digital documents, namely documents using the RIVEST CIPHER 6 method which will later be entered into the system and encrypted into ciphertext. As well as documents that have been encrypted and returned by decryption using the same key when encrypting the document. The ciphertext decryption process in the RIVEST CIPHER 6 algorithm is a reversal of the encryption process. In the whitening process, if the encryption process uses an addition operation, then the decryption process uses a subtraction operation. The sub key used in the whitening process after the last iteration is applied before the first iteration, and vice versa. To perform decryption, the only thing that must be done is to apply the same algorithm as encryption, with each iteration using the same sub-key used during encryption, only the order of the sub-keys used is reversed.

## REFERENCES

T Prasetyo, R. P. (2020, Maret). Sistem Informasi Administrasi Pemerintahan Desa pada Desa Cilayung Kabupaten Kuningan. Jurnal Teknologi dan Informasi (JATI), 10.

Ardede, AMH, Sitepu, LPB, Zarlis, M., Iskandar, A., Sriadhi, S., Manurung, RT, ... & Winarno, E. (2019, November). Application of Message Security Application Using Vigenere Cipher Algorithm Utilizing One Time Pad (OTP) Algorithm as a Key Generator. In Journal of Physics: Conference Series (Vol. 1363, No. 1, p. 012080). IOP Publishing.

Toyib, R., & Wijaya, A. (2019). COMPARISON ANALYSIS OF RIVEST SYMETRIC ALGORITHM
CODE 5 WITH RIVEST SYMETRIC ALGORITHM

CODE 6) (Case Study: SMK Negeri Seluma). Upgris Journal of Informatics, 4(2), 203–209. H
Kristianto, BD, Gat, G., & Syarifudin, G. (2020). Sms Encryption Software Design Using **Rivest Cipher 6** And Rijndael

Algorithm On Smartphones. Sisfotenika, 10(1), 115.https://doi.org/10.30700/jst.v10i1.948
Budiman, A., & Paradise, P. (2019). Modification of Vigenere Algorithm and One Time Pad Using Rivest Code 6 (RC6) Key Expansion. Compilers, 8(2), 149–156.

*name of corresponding author

https://doi.org/10.28989/compiler.v8i2.481

Kurniawan, D. (2018). Planning Text Data Security Applications Using Blowfish And Rc6. Journal of Informatics Pelita, ISSN 2301-9425 (Print Media), 17(3), 254–260.

Kurniawan, RA, & Avianto, D. (2019). Design of an Encrypted Short Message Application With Web-Based Advanced Encryption Standard (Aes) Algorithm.

Laurentine. (2017). Implementation of Cryptography and Sms Compression Using the **Rivest Cipher 6** Algorithm and Android-Based Huffman Algorithm. Scientific Journal of Global Informatics, 8(1), 36–42.
Padede, AMH, Manurung, H., & Filina, D. (2017). Vigenere Cipher And Hill Cipher Algorithm In Data Security Applications In Document Files. JTIK (Journal of Informatics Engineering Kaputama), 1(1), 26-33.

Atmojo, WP, Isnanto, RR, & Kridalukmana, R. (2016).Implementation of Cryptographic Applications on Short Message Service (SMS) Using Android-Based **RIVEST CIPHER 6** Algorithm. Journal of Technology and Computer Systems, 4(3),450. https://doi.org/10.14710/jtsiskom.4.3.2016.450-453

*name of corresponding author