Journal of Sisfotek Global

Versi Online: http://journal.stmikglobal.ac.id/index.php/sisfotek
ISSN (Online): 2721 - 3161, ISSN (Print): 2088 – 1762
Vol. 11, No. 2, September 2021, pp. 115-120

RC4 Cryptography Implementation Analysis on Text Data

[1]Agung Susilo Yuda Irawan, [2]Adi Rizky Pratama, [3]Ryan Antono

[1]Universitas Singaperbangsa, Karawang, Indonesia
[2,3]Universitas Buana Perjuangan, Karawang, Indonesia
E-mail: [1]agung@unsika.ac.id, [2]adi.rizky@ubpkarawang.ac.id, [3]ryan.antono11@gmail.com.

ARTICLE HISTORY

Received : 14 September, 2021
Revised : 17 September, 2021
Accepted : 28 September, 2021

KEYWORDS

Cryptography
RC4
ASCII
Text

ABSTRACT

Security and confidentiality have become very important and continue to grow. In recent years, there have been several cases involving data security, such as the leaking of Facebook user account information. This is certainly a significant issue in the world of information technology and even the world of entrepreneurship because it involves one of the young entrepreneurs, Mark Zuckerberg. Main problem in this case is data security. who can know information and who should not know information. To overcome such things, research is made in the field of data and information security by analyzing one of the encryption and decryption techniques, namely RC4 cryptography. This study explains how RC4 cryptography works, the advantages and disadvantages of RC4 cryptography, and the effectiveness of RC4 cryptography. RC4 (River Ciper 4) is a decryption encryption technique that uses a key as a reference. The process consists of KSA, PRGA, and XOR. To find out the usefulness of RC4 cryptography, in this study, encryption and decryption were carried out on text data. There are several advantages and disadvantages to RC4 cryptography from a technical point of view. The advantage that needs to be underlined is that this RC4 cryptography uses a certain key as a reference, things like this can provide convenience to the encryption maker but can also be a threat. as a result RC4 can hide information very well while the secret key is not known by others. In addition to being used in text data, this cryptography may be used for other data such as audio and video.

1. INTRODUCTION

Entering the 4th industrial technology era, people are increasingly pampered with the easier use of technology. Technology is applied in almost all fields, such as government, business, tourism, and daily life. In addition, the use of technology today is not only used by young people but almost all ages use it, for example the use of smartphones. Ease of accessing information is one of the advantages of the development of information technology. Everyone can easily get the information or news they want. Because on the one hand, printed or conventional information dissemination media are rarely in demand by the public. Newspapers and magazines are examples of information dissemination media that have begun to be abandoned, people prefer to read news on smartphones by accessing certain sites because it is easier and more flexible. One of the media for disseminating information that is currently loved by the public is online discussion forums such as Facebook, Kaskus, Twitter, etc. With such forums, it is easier for people to get the latest information or news, just use a smartphone that is connected to the internet. However, to use it we must be registered as a user by filling in some of our information for account creation and that is one of the shortcomings that we get. Data or information contained in accounts that have been created can be stolen by irresponsible parties and can be used to commit crimes. Reporting from several information provider sites, millions of Facebook account information leaked into irresponsible hands and that is one of the crimes of the development of information technology. Data security is very necessary to keep pace with the development of information technology for the creation of data and information security. The development of algorithms or security methods must also continue to be in line with the times.

One method that can be used to secure data or information is the RC4 cryptography method. This method was first developed by Ron Rivest in 1987 at the RSA laboratory [1]. The author in this study conducted an experiment to secure data on the text using the RC4 cryptography method. By analyzing how it works, the advantages and disadvantages, and the effectiveness of using RC4 for data security.

2. METHODS

2.1. Algorithm

A cipher algorithm is an algorithm that serves to perform cryptographic purposes. The algorithm should have the power to do [2]:

Algorithms in general can be interpreted as the steps taken to solve a problem. Algorithms in the world of informatics serve as the basis of science for technology development. Algorithm is a method used by computers that consists of well-defined steps to achieve certain goals, receive input, process, and provide output [3]. An example of writing an algorithm that is widely used is the vessel content exchange algorithm. There are two vessels X and Y which contain black and white solutions, exchange the contents of the vessels so that the white solution is in vessel X and the black solution is in vessel Y. The following is a description of the algorithm above:

1) Prepare the vessel Z

2) Pour the contents of vessel X into vessel Z

3) Pour the contents of vessel Y into vessel X

4) Pour the contents of vessel Z into vessel Y

2.2. Encryption Decrypt

Encryption can be said as the process of encoding something, while decryption can be interpreted as the process of translating the results of encryption. Encryption decryption is a function that is in cryptography which is the process of encoding data or messages into cipher text (secret message), when the cipher text is received it will be converted again into an ordinary message through the decryption process so that it can be read by the recipient [4]. Decryption encryption is very useful for data security. Big companies that have great benefits should have used this concept to secure information so it doesn't leak to other parties, of course, by using technology as well. On the other hand, it is also possible if the concept of encryption and decryption is used by individuals to secure information because nowadays the world of hacking is very dangerous.

Encryption is an encoding process that converts the original text or messages that can be understood (plaintext) into text-codes or messages that cannot be understood (cipher text). Decryption is a reversal process that converts a text-code or message that cannot be understood (cipher text) into a text-original or message that can be understood (plaintext). [5]. To perform an encoding process and a reversal process using the same algorithm. A system that is used to secure data so that the confidentiality of the data is guaranteed and conveyed with maintained confidentiality, it is necessary to use cryptographic methods to secure the data to be sent. The existence of cryptography, is expected to maintain the confidentiality of data in an agency or certain circles.

2.3. Cryptography

In cryptography, there are two processes, namely encryption and description. The message to be encrypted is referred to as plaintext (plain text [6] . So called because this information can easily be read and understood by anyone. The algorithm used to encrypt and decrypt a plaintext involves the use of some form of key. The plaintext message that has been encrypted (or encoded) is known as cipher text (password text).

Cryptography is an example of the implementation of the concept of encryption and decryption. Cryptography comes from two Greek words, namely cryptos which means secret and graphing which means writing. Cryptography is a branch of science to secure messages based on the key used [7].

There are 4 basic components in cryptography, namely:

1) Plaintext, messages can be read.

2) Cipher text, messages that have been encoded.

3) Key, the key in cryptography.

4) Algorithm, how to do encryption and decryption *[8]*.

There are two techniques in doing cryptography, namely classical cryptography techniques and modern cryptography techniques [9].

The following are examples of the two cryptographic techniques: Classical cryptography:

*1) S*ubstitution, changing one or more bits in plaintext without changing the order.

2) Transposition, changing the position of the bits in the plaintext with certain rules.

Modern cryptography:

1) Symmetric cryptography, performs decryption encryption with the same key.

2) Asymmetric cryptography, performs decryption encryption with a public key and a secret key.

3) Hybrid cryptography, performs the encryption decryption process twice [10].

2.4. RC4

River Code 4 abbreviated as RC4 is an algorithm created by RSA and is in the form of a stream cipher. This algorithm was first discovered by Ronald Rivest in 1987. RC4 uses a key with a length of 1 to

256 bytes to define a table of 256 bytes. The table is used for pseudo random generation that uses XOR with plaintext to generate cipher text, each element in the table is exchanged at least once [11]. RC4 is an algorithm that is used to process input data at one time, in this way the encryption and decryption process can be carried out at variable lengths. This RC4 method is faster than the DES method, this method can process or add bytes for encryption without waiting for a certain amount of data input . There are two stages in the encryption and decryption process using the RC4 method, namely key setup and encryption. The first stage is the most difficult, namely the key setup process. This stage serves to determine the key that will be used in the next stage, namely encryption. In the first stage, it will generate encryption variables using two arrays, state and key, and a number of S (key length) as a result of the merging operation [12]. Merge operations consist of moving bytes, module operations, and other formulas. The module operation is a process that produces the remainder of the division, for example 11 divided by 4 is 2 remaining 3, the same as 7 mod 4 then the result is 3 [13].

2.5. Research methodology

The method used in this research consists of literature study, data analysis, implementation and result.

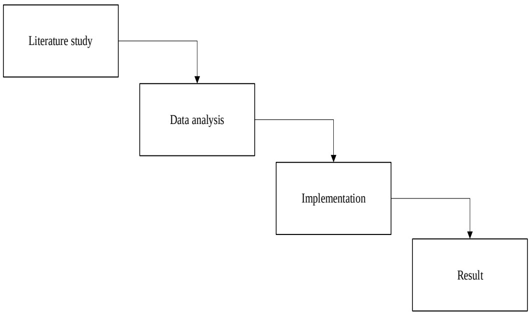

Figure 1. Research methodology

The stages of the method have their respective functions, as follows:

A. Literature study at the literature study stage, the required data were collected. The data is in the form of journals related to RC4 cryptography to be used as a reference. This journal search process is carried out using a service provided by Google, namely Google Scholar. With this service, several journals related to the research were found.

B. Data analysis after obtaining the required journals, the data analysis process was carried out. The data analysis process begins with screening the journals that have been obtained, only journals that can indeed strengthen the research arguments taken. After that, carry out the problem analysis process in accordance with the research conducted with the aim of obtaining research solutions. At this stage, researchers must understand correctly what will be discussed in the research conducted.

C. Implementation After knowing the problem and getting a research solution, the final stage is implementation. At this stage the researcher realizes between theory and practice, then analyzes and makes an assessment of the community's response to the research conductedResults And Discussion

How RC4 cryptography works on text data

In general, the algorithm for RC4 cryptography is carried out in several stages including key state array (KSA), pseudo random generation algorithm (PRGA), and XOR. In order to find out that RC4 cryptography can work at a basic level, a decryption encryption process is carried out with a 4-bit state array. This is done because if you use a 256 bit state array manually it will be difficult to do.

RUDI word encryption is performed with the key 2573. First, we perform the KSA process to obtain a block array for key determination. Then the state array S and state array K are formed as follows,

Table 1. State Arrays S and K

State array S	0	1	2	3
State array K	2	5	7	3

After getting the state array S and K, initialize i and j with 0 and then do KSA to form a random state array. The explanation is as follows:

Iteration 1

i = 0
j = (0 + S[0] + K[0]) mod 4
j = (0 + S[i] + K[i] mod 4
j = (0 + 0 + 2) mod 4 = 2
Swap (S[0], S[2])
The result of array S is
State array S 2 1 0 3

Iteration 2

i = 1
j = (2 + S[1] + K[1]) mod 4
j = (2 + 1 + 5) mod 4 = 0
Swap (S[1], S[0])
The result of array S is
State array S 1 2 0 3

Iteration 3

i = 2
j = (0 + S[2] + K[2]) mod 4
j = (0 + 0 + 7) mod 4 = 3
Swap (S[2], S[3])
The result of array S is

State array S 1 2 3 0

Iteration 4

i = 3
j = (3 + S[3] + K[3]) mod 4
j = (3 + 0 + 3) mod 4 = 2
Swap (S[3], S[2])
The result of array S is
State array S 1 2 0 3

Second, after carrying out the KSA process, the results obtained from the KSA process are carried out by the PRGA process as a key search process for each character. The pseudo-random generation algorithm (PGRA) stage aims to generate the keystream. Each round, the keystream portion of 1 byte with a value between 0 to 255 is output by PRGA based on state S [14]. Here's the explanation:

results KSA,
State array S 1 2 0 3
Re-initialize i and j as 0,
1teration 1
i = (0 + 1) mod 4 = 1
j = (0 + S[1]) mod 4
j = (0 + 2) mod 4 = 2
Swap (S[1], S[2])
The result of array S is

State array S 1 0 2 3

K1 = S[(S[1] + S[2]) mod 4]
K1 = S[2 mod 4]
KSA results,
State array S 1 2 0 3

Re-initialize i and j as 0,

1teration 1
i = (0 + 1) mod 4 = 1
j = (0 + S[1]) mod 4
j = (0 + 2) mod 4 = 2
Swap (S[1], S[2])
Hasil array S adalah

State array S 1 0 2 3

K1 = S[(S[1] + S[2]) mod 4]
K1 = S[2 mod 4]
K1 = S[2] K1 = 2
K1 = 00000010

Iteration 2
i = (1 + 1) mod 4 = 2
j = (2 + S[2] mod 4
j = (2 + 2) mod 4 = 0
Swap (S[2], S[0])
The result of array S is

State array S 2 0 1 3

K2 = S[(S[2] + S[0]) mod 4]
K2 = S[3 mod 4]
K2 = S[3] K2 = 3
K2 = 00000011

Iteration 3
i = (2 + 1) mod 4 = 3
j = (0 + S[3] mod 4
j = (0 + 3) mod 4 = 3
Swap (S[3], S[3])
The result of array S is

State array S 2 0 1 3

K3 = S[(S[3] + S[3]) mod 4]
K3 = S[6 mod 4]
K3 = S[2]
K3 = 1
K3 = 00000001

Iteration 4
i = (3 + 1) mod 4 = 0
j = (3 + S[0] mod 4
j = (3 + 1) mod 4 = 0
Swap (S[0], S[0])
The result of array S is

State array S 2 0 1 3

K4 = S[(S[0] + S[0]) mod 4]
K4 = S[4 mod 4]
K4 = S[0]
K4 = 2
K4 = 00000010

Third, after getting the key for each character (K1 to K4) then do the XOR process between the ASCII code of the word RUDI with the keys K1 to K4. Before that, we first look for the ASCII code from the word RUDI, here's an explanation :

Table 2. Ascii Code

ASCII Code For Each Plaintext Character

Letter	ASCII Code
R	01010010
U	01010101
D	01000100
I	01001001

If the ASCII code for each character has been obtained, the encryption XOR process is carried out, as follows:

Table 3. XOR encryption table

	R	U	D	I
Plaintext	01010010 (82)	01010101 (85)	01000100 (68)	01001001 (73)
Key	00000010 (2)	00000011 (3)	00000001 (1)	00000010 (2)
Chipertext	01010000 (80)	01010110 (86)	01000101 (69)	01001011 (75)

On the other hand, the description process also uses the XOR process, as follows:

Table 4. XOR Decryption Table

	R	U	D	I
Key	00000010 (2)	00000011 (3)	00000001 (1)	00000010 (2)
Chipertext	01010000 (80)	01010110 (86)	01000101 (69)	01001011 (75)
Plaintext	01010010 (82)	01010101 (85)	01000100 (68)	01001001 (73)

Jadi setelah dilakukan pengenkripsian maka kata RUDI berubah menjadi kode biner 01010000 01010110 01000101 01001011 yang dalam kode ASCII berarti PVEK

3. RESULTS AND DISCUSSION

3.1.1. Advantages and disadvantages of RC4 cryptography

There must be advantages and disadvantages in every branch of science, including RC4 cryptography. Here are some of the advantages and disadvantages of RC4 cryptography when used on text data.

1) Encryption complexity makes data hard to crack
2) Have a special key as a reference
3) Since the character length remains the same the memory size does not change

Deficiency:

1) If the key is known then the data is easy to crack
2) The same character length also gives more information

Several weaknesses in RC4 were identified. Some of these weaknesses are simple and can be solved easily, but others are critical because they can be exploited by the attackers. Two of the problems of RC4 are 1) the weakness of the KSA and 2) the weakness of relations between the S-box in different time[15].

3.1.2. Cryptographic effectiveness of RC4

To find out the effectiveness of RC4 cryptography, a survey was conducted on 20 students majoring in informatics engineering at the Singaperbangsa Karawang University, the results are as follows:

Table 5. Table of Student
Response Results Regarding the Effectiveness of
RC4 . Cryptography

	YES	NO
Ease of Rc4 Cryptography	7 people	13 people
rc4 cryptography is suitable for securing text	11 people	9 people
can be implemented in various fields	1 0 people	1 0 people
familiar in the educational environment	8 people	12 people
development in accordance with the development of information technology	11 people	9 people
Efficient	11 people	people

4. CONCLUSIONS

From the results and discussion above, several conclusions can be drawn, namely the way RC4 cryptography works is difficult in determining the key which makes the encryption process complicated.

There are several advantages and disadvantages to RC4 cryptography from a technical point of view. The advantage that needs to be underlined is that this RC4 cryptography uses a certain key as a reference, things like this can provide convenience to the encryption maker but can also be a threat.

RC4 cryptography is still not effective when used in text. In addition, this technique is still rarely used in the educational environment.

Suggestion In order to know more about the workings and uses of RC4 cryptography, the author hopes that other studies will be able to dig deeper into RC4 cryptography. In addition to being used in text data, this cryptography may be used for other data such as audio and video. In fact, we hope that for future research there will be a combination of algorithms for optimization such as combining with steganography.

REFERENCES

[1] I. Halik and Y. Prayudi, “Studi dan Analisis Algoritma Rivest Code 6 (RC6) dalam Enkripsi/Dekripsi Data,” *Snati*, vol. 6, no. D,

2005, [Online]. Available: http://journal.uii.ac.id/index.php/Snati/article/view/1402.

[2] and T. H. D. Seftyanto, M. Apriani, "No Title," 2012, [Online]. Available: https://eprints.uny.ac.id/10106/1/P - 94.pdf.

[3] H. Pertiwi, "Teori Algoritma," vol. 1, pp. 1–10, 2014.

[4] W. H. Haji and S. Mulyono, "Implementasi Rc4 Stream Cipher Untuk Keamanan Basis Data," *Semin. Nas. Apl. Teknol. Inform.*, vol. 2012, pp. 15–16, 2012.

[5] R. Munir, *Kriftografi*. Bandung: Institut Teknologi Bandung, 2006.

[6] R. K. P. Pratama and F. Latifah, "Implementasi enkripsi dekripsi pesan teks menggunakan model Julis Caesar berbasis Object Oriented Programme," *J. Techno Nusa Mandiri*, vol. XI, no. 1, pp. 17–26, 2014, [Online]. Available: http://ejournal.nusamandiri.ac.id/index.php/techno/article/view/167.

[7] J. Komputasi, "Implementasi Enkripsi Dan Deskripsi Dengan Metode," vol. 5, no. 2, pp. 38–44, 2017.

[8] P. Kriptografi and D. A. N. Pemakaianya, "2016," no. May, 2016.

[9] Suhardi, "Aplikasi Kriptografi Data Sederhana Dengan Metode Exlusive-or (Xor)," *J. Teknovasi*, vol. 03, no. 2, pp. 23–31, 2016.

[10] Karthik, Chinnasamy, and Deepalakshmi, "Hybrid cryptographic technique using OTP:RSA," *Proc. 2017 IEEE Int. Conf. Intell. Tech. Control. Optim. Signal Process. INCOS 2017*, vol. 2018-February, no. November 2020, pp. 1–4, 2018, doi: 10.1109/ITCOSP.2017.8303131.

[11] M. Edy Purnomo, W. Priyono, S. Sari, R. Ambarwati, and A. Wulandari, "Implementasi Algoritma Kriptografi RC4 Pada DSP TMS320C6713 Sebagai Pendukung Sekuritas Jaringan Komunikasi Voice Over Internet Protocol (VoIP)," *J. EECCIS*, vol. 6, no. 2, p. pp.183-188, 2012.

[12] E. L. Hakim and F. H. Utami, "Aplikasi Enkripsi Dan Deskripsi Data Menggunakan Algoritma Rc4," vol. 10, no. 1, pp. 1–7, 2014.

[13] M. Awaludin, "Penerapan Algoritma Rc4 Pada Operasi Xor Untuk Keamanan Pesan Pada Smartphone Berbasis Web," *J. Sist. Inf. Univ. Suryadarma*, vol. 4, no. 1, pp. 16–22, 2014, doi: 10.35968/jsi.v4i1.71.

[14] T. D.B.Weerasinghe, "Analysis of a Modified RC4 Algorithm," *Int. J. Comput. Appl.*, vol. 51, no. 22, pp. 12–16, 2012, doi: 10.5120/8341-1617.

[15] M. M. Hammood, K. Yoshigoe, and A. M. Sagheer, "RC4-2S: RC4 stream cipher with two state tables," *Lect. Notes Electr. Eng.*, vol. 253 LNEE, no. January, pp. 1