Implementation of Rivest Chiper Cryptography (RC6) with One Time Password (OTP) and Two Central Facilities Protocol in Complaint Service System

Muhamad Nursalman[1], Eddy Prasetyo Nugroho[2], Ferryan Reynaldi Akbar Nur[3]
{mnursalman@upi.edu[1], eddypn@upi.edu[2], ferryanreynaldi@student.upi.edu[3]}

Department of Computer Science Education, Faculty of Mathematics and Science Education
Universitas Pendidikan Indonesia[1,2,3]

Abstract. The form of assistance services is oriented towards public complaints on emergency services. In addition to the positive aspects of this service, there are also negative impacts such as sending fake data or misuse of someone's data. Therefore a Complaint Service security system is created using the Two Central Facilities Protocol, assisted by cryptographic security methods using the RC6 algorithm, which aims to find out that the reporter is actually logged in and for the reporter, report data security using the RC6 algorithm which is used when encryption and decryption of reporting data is sent to the police station or police station. From the system, obtaining the assessment of the user or user, the following are aspects of the assessment: Usability, Information Quality, and Interaction Quality from all aspects get an average value of 81%, 82.8%, and 83.1%.

Keywords: Complaint Service, RC6 Algorithm, One Time Password (OTP), Protocol Two Central Facilities, Cryptography.

1 Introduction

The form of aid services is oriented towards public complaints on emergencies, including Medical, fire, security, accidents, and natural disasters. As of mid-2013, there were 18,000 calls per day that went to 110. However, people who gave real reports were only 101 reports per day. By category, 30% of reports that enter 110 are criminal complaints, 19% traffic info, and 18% accidents. Even in this complaint service system research, security issues and validation are also the most important issues to discuss. The growth of internet users also has a trend of increasing internet crime (Cybercrime) in Indonesia and even into the top 2 origins of the world internet crime attacks and is considered as the country most at risk of information technology security attacks [1].

The difference from this system and the system with calls being called reporter data reporting will be more specific because the data obtained is from KTP when compared to making phone calls as obtained from Kompas.com news - 30/01/2013 with the title Beware, There Are Sanctions for Fadings Phone 110 [2]. The police only record data from the caller number only, so it is not guaranteed if the reporter will make the original report and get sanctions if the reporter is only playing or making false reports.

The use of the Two Central Facilities Protocol in the study was implemented for a cooperation contract monitoring system, but in Caesar Firdaus's research there was no

MSCEIS 2019, October 12, Bandung, Indonesia

DOI 10.4108/eai.12-10-2019.2296270

authentication system [3], therefore the current study using the Two Central Facilities Protocol was implemented in a complaints service system with the help of OTP for reporting authentication. authentication. authentication.

2 Related Research and Theory

This research began with conducting a literature study on theories and studies related to cryptography. The problems that occur in the research conducted by Caesar Firdaus [3] on the company monitoring system show that the file size increased from 3.785 to 4.095 times. That happens because the PDF file converted to hexadecimal results in twice the increase in file size from the original. Whereas the research carried out is about the monitoring system in the company and regarding the comparison of the RC6 algorithm with Rijndael on AES where the RC6 algorithm is code for RC6 simpler than Rijndael, but Rijndael's performance on smart cards still exceeds RC6 performance [4].

2.1 Algorithm RC6

Key Scheduling RC6. RC6 also performs the encryption process by using a different key for each rotation. The key formation in RC6 is not too different from the formation of locks on RC5. Broadly speaking, key formation is done by taking from b bytes the key entered by the user where $0 \leq b \leq 255$. A number of zero bytes is added sufficiently for the key length equal to the round number of words that are not zero. This key is then entered into an array along c where each array is filled with one byte of the key. From this key, take a number of 2r + 4 words with the length of w bits of each word and stored in an array S [0, ..., 2r + 3] [5].

```
S[ 0 ] = 0xB7E15163
for i = 1 to 43 do S[ i ] = S[ i - 1 ] + 0x9E3779B9
A = B = i = j = 0
for k = 1 to 132 do
    {
            A = S[ i ] = ( S[ i ] + A + B ) <<< 3
            B = L[ j ] = ( L[ j ] + A + B ) <<< ( A + B )
            i = ( i + 1 ) mod 44
            j = ( j + 1 ) mod c
    }
```

Encryption. RC6 operates using four registers A, B, C, D along the w bits which contain the initial input from the plaintext and can also be the end result of the ciphertext at the end of the encryption process. The first byte of plain text is entered into the least significant byte A and the last byte of plain text is entered into the most significant byte D. The next process is the result of encryption or decryption using operations on the Feistel network.

The Feistel network is a process that is carried out during one round of encryption. In RC6, the encryption process will be repeated as many as r times according to the input from the user. For the decryption process, just do the sequence on the Feistel network from bottom to top [5].

```
B = B + S[ 0 ]
D = D + S[ 1 ]
for i = 1 to 20 do
    {
        t = ( B x ( 2B + 1 )) <<< 5
        u = ( D x ( 2D + 1 )) <<< 5
        A = (( A ⊕ t ) <<< u ) + S[ 21 ]
        C = (( C ⊕ u ) <<< t ) + S[ 21 + 1 ]
        (A, B, C, D) = (B, C, D, A)
    }
A = A + S[ 42 ]
C = C + S[ 43 ]
```

Decryption. The ciphertext decryption process in the RC6 algorithm is a reversal of the encryption process. In the whitening process, if the encryption process uses a sum operation, then the decryption process uses a subtraction operation. The subkey used in the whitening process after the last iteration is applied before the first iteration, and vice versa the subkey that is applied to the whitening process before the first iteration is used in whitening after the last iteration. As a result, to decrypt, the only thing to do is to apply the same algorithm with encryption, with each iteration using the same subkey as that used in encryption, only the subkey sequence used is reversed. The following is the RC6 decryption algorithm [5]:

```
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 ]
```

2.2 One Time Password (OTP)

One Time Password (OTP) is a password that only applies to single login sessions or single transactions. In general, algorithms from OTP are made randomly. However, there are three main approaches in the OTP generate process, namely:

a. Based on "time-synchronization" between server-client authentications that provides a password (OTP will be valid if in a short period of time).
b. Based on the "mathematical algorithm" that allows the generalization of a new password based on the previous password.
c. Based on the "mathematical algorithm", the new password is based on a challenge (for example, the assignment of a password randomly will be determined by the server or transaction details) [4].

3 Method

The use of OTP and the Two Central Facilities Protocol applied to the complaints service system gets results, where the reporter will not dare to make a report because the reporter's data is obtained from original data stored at CLA, this CLA is the body that stores the reporter's original KTP also as a body that provides a validation number or OTP to the reporter. So if the reporter uses a fake NIK number or one that is not registered in the CLA the system will reject the input data and if the OTP does not match the one sent by the CLA the system will also reject the reporter. to determine the OTP number, but if the contents of the report prove false then the police can track the whereabouts of the reporter because they have to use the original data obtained from the reporter's KTP and sanctions if they are violated which are regulated in Bab IX about oaths and false statements, article 242 paragraph (1) Criminal Code or KUHP and Constitution No. 11 Years 2008 about Electronic Information and Transactions.

If the RC6 algorithm is implemented in the complaints service system, because the contents of the report are many then if the next research is added with proof of reporting, the RC6 algorithm is very suitable because if using another algorithm the file size will increase and require a long time for the encryption process and decryption. In Caesar Firdasus research using the AES algorithm resulted in several times the increase in file size from the original.

If the RC6 algorithm is implemented in the complaints service system, because the contents of the report are many then if the next research is added with proof of reporting, the RC6 algorithm is very suitable because if using another algorithm the file size will increase and require a long time for the encryption process and decryption. In Caesar Firdasus research using the AES algorithm resulted in several times the increase in file size from the original.

From **Figure 1** it can be interpreted as follows.

a. *Central Legimitazion Agency* (CLA)

CLA pada sistem layanan pengaduan yaitu untuk memberikan validasi dan menyimpan data pelapor tersebut misalnya seperti NIK, Nama, dan lain-lain.

b. *Central Tabulating Facilities* (CTF)

The CTF in the complaints service system is for the last storage of the report, and see whether the report is true or not.

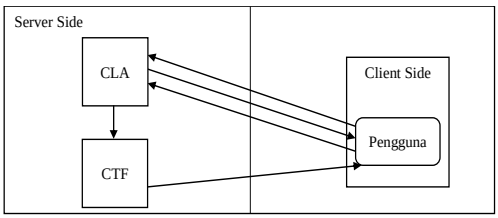

Fig. 1. Two Central Facilities Protocol Architecture.

4 Result and Discussion

4.1 Encryption Flow RC6

The flow of Encryption Algorithm RC6 stages of data encryption using the RC6 algorithm. In this section how to find out how to generate encrypted data. **Figure 2** illustrates how the process of generating ciphertexts on that data.

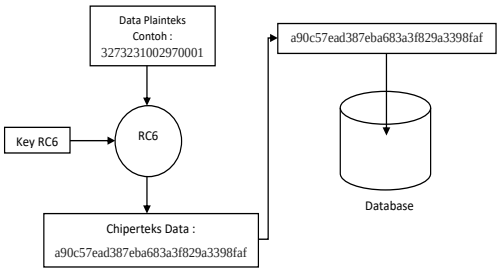

Fig. 2. Encryption Flow RC6.

4.2 Encryption Result RC6

The results of three NIK encryption that produce different ciphertexts are as shown Table 1.

Table 1. The Result Of NIK Encryption.

NO	Algorithm RC6	
	Plaintext	**Chipertext**
1	3273231002970001	a90c57ead387eba683a3f829a3398faf
2	3273231002970009	13c8e261fe85218ac96c61a749176417
3	3273231002970010	61016822b1ebfc989ad1e9dc8e19fd8f

Encryption speed testing uses the RC6 algorithm for NIK from data.

Tables 2 and 3 below show that the encryption and decryption process uses the RC 6 algorithm is very fast and quite stable because in this study encrypting a string.

Table 2. Time Encryption and Decryption of Previous Research [6].

No	File Name	File Size (KB)	Time (Second)		
			Encrypt	**Decrypt**	**Total**
1	Chen5.PDF	84	12.3	65.9	78.2
2	Dct.PDF	595	88.9	385.7	474.7
3	ChapterII.PDF	702	104.5	462.9	567.4

Table 3. RC6 Encryption and Decryption Time Result.

NIK Number	Encrypt (ms)	Decrypt (ms)
	0.1546618	0.1476011
3273231002970001	0.2026960	0.1212091
	0.4912781	0.1419761
	0.1732821	0.790485
3273231002970010	0.2443680	0.179233
	0.1232938	0.128684

From the data in Table 2 and 3 above, it can be concluded that it is true that the file size increased 3.785 to 4,095 times causing the encryption and decryption process to increase, and for Rijndael performance, it is still better than RC6 as in Table, for RC6 memory indeed has an increase if on file. However, in a study that uses a string of encryption and decryption time processes are somewhat more stable and faster even though each experiment experiences an increase due to the process of encryption and decryption the device for testing experiences a slight delay.

4.3 Result Of Validation Number OTP

The following are findings made by researchers on validation numbers that will be used for users to log in to the user dashboard, here is an example of an OTP as in Table 4.

Table 4. Result Of Validation Number OTP

Validation Number / OTP
2ee70ec3d9f93356e657320813827c18
f04b0dbc31c5ce044064226e7c32da91
b7b537c1d5d97a2dc669d1573be9e5b5

4.4 Randomness Test Data

From the results of Table 5, the below tests have very good results because the value of the test results from the Randomness Test shows a number that is not greater than the Max Value for all types of tests.

Table 5. Randomness Test

Randomness Test		Test Result	
Type	Max Value		
Frequency	3.84	0.390	Pass
Poker	14.07	4.505	Pass
Long Run	34	7	Pass
Run	9.48	1.521	Pass
Serial	5.99	0.451	Pass

4.5 Brute Force Attack

The results in Table 6 of the Brute Force Attack test on the RC6 and OTP algorithms can be categorized for quite a long time because when the key testing is entered only at the beginning and end, it results in a time of hacking of around 5,858 years.

Table 6. Brute Force Attack

Chipertext	32 EC 3C 5F 3F 05 A6 8F 6C 97 32 B3 2C 3B FA 1A 4C C4 4E 09 A5 A8 71 EB F8 42 E0 24 8E A0 DA A0
Key and Key Test	01 23 45 67 89 AB CD EF 01 12 23 34 45 56 67 78 89 9A AB BC CD DE EF F0 10 32 54 76 98 BA DC FE 01 ** FE
Brute Force Result	*5.858 Years*

4.6 WebQual Test Result

Respondents who tested the system and filled out questionnaires totaling 29 respondents, for the respondents' data attached to the appendix. The results of the questionnaire were processed using SPSS software to test the validity and reliability test.

Based on the results of testing with the WebQual method which consists of the dimensions of Usability, Information Quality, Interaction Quality and the results of testing three WebQual dimensions can be seen in Table 7.

Table 7. WebQual Test Result

No	Question	Answer Value
1	*Usability*	81%
2	*Information Quality*	82.8%
3	*Interaction Quality*	83.1%

4.7 Test of Data Confidentiality

From the results of testing Table 8 below it is stated that it has very good results because the encrypted data is not successfully decrypted using the application, it can be seen that the results of red Wireshark capture on port 443 and the RC6 ciphertext algorithm cannot be decrypted.

Table 8. Test Of Data Confidentiality

No	Source	Destination	Protocol & Port	Length	Info
1	13.107.3.128	192.168.100.12	TCP, 443	60	Red
2	52.114.32.8	192.168.100.12	TCP, 443	60	Red

4.9 Analysis of the Complaint Service Result

The difference from this system and the system with calls being called reporter data reporting will be more specific because the data obtained is from KTP when compared to making phone calls as obtained from Kompas.com news - 30/01/2013 with the title Beware, There Are Sanctions for Fadings Phone 110 [3]. The police only record data from the caller number only, so it is not guaranteed if the reporter will make the original report and get sanctions if the reporter is only playing or making false reports.

In this study, Randomness Test was analyzed by entering encrypted ciphertext data as can be seen in Table 5. Testing of ciphertext randomness uses several trials namely Frequency, Poker, Long Run, Run, and Serial tests. Tests that have been done by giving chipertext RC6 and OTP encryption results in excellent randomization results because the RC6 ciphertext algorithm and OTP test results using Randomness Test show numbers that are not greater than the Max Value for all types of tests of all test types, where Frequency produces a value 0.125000, Poker Test with a value of 3.3333, Long Run and Run Test with a value of 4.591756, 1.521, and Serial Test with a value of 0.055364.

The results obtained after testing the data encrypted by the RC6 and OTP algorithms with Randomness Test and Brute Force Attack can be seen in the Table by entering the ciphertext and Key from the encrypted data and then analyzing their randomness using the help from the CrypTool 1.4.4 application. A brute force attack test that results in the possibility of being hacked in 5,858 years that the chiptext is known to be plaintext.

In calculating the level of satisfaction using the Likert scale. From the results of testing the WebQual method in Table 7 for the system that has been built found results for the Usability dimension with the average response of the respondents 81% can dikatan points obtained are included in the category strongly agree. Then for the Information Quality dimension with the acquisition of respondents' average answers 82.8% and can get the points obtained already included in the category strongly agree. And for the Interaction Quality dimension with the average response of respondents 83.1% can be dikatan also obtained points included in the category strongly agree.

The use of the RC6 algorithm with two central facilities protocol in the complaints service system was tested using the Wireshark application from the study can be seen in Table 8 with the results of encrypted data not successfully decrypted using the application, that the results of Wireshark capture are red against sending on port 443 and the ciphertext in the RC6 algorithm cannot be decrypted.

5 Conclusions

The conclusion of the research on the implementation of Rivest Chiper cryptography (RC6) and One Time Password (OTP) in the complaints service system using the Two Central Facilities Protocol is as follows:

a. This research using the Two Central Facilities protocol has succeeded in making this system authenticated, so the reporter will feel safe that the NIK owned by the reporter can only be used by the reporter.
b. Encryption and decryption of user data by using the RC6 cryptography algorithm stored in the database with ciphertext generated from the encryption so that the data is safe and can be seen in the police station if only the admin of the police officer can

see the report data and during testing using the data Wireshark was not successfully decrypted so the data security with the RC6 algorithm was scrambled very well and getting a user rating for the system was 87.6% of several aspects of assessment including Display, Efficiency, Ease, Responsiveness, Security.

References

[1] Danuri, M., & Suharnawi, S. (2017). Trend Cyber Crime Dan Teknologi Informasi Di Indonesia. Infokam, 13(2).

[2] Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms and Source Code in C. John Wiley & Sons.

[3] Kompas, Masih Banyak Telepon Iseng, Kompas.com - 14/02/2013 13:28 WIB, https://tekno.kompas.com/read/2013/02/14/13285864/Di.110.Masih.Banyak.Telepon.Iseng

[4] Sakti, D. V. S. Y., Agani, N., & Hardjianto, M. (2015). Pengamanan Sistem Menggunakan One Time Password Dengan Pembangkit Password Hash SHA-256 dan Pseudo Random Number Generator (PRNG) Linear Congruential Generator (LCG) di Perangkat Berbasis Android.

[5] Prayudi, Y., & Halik, I. (2005). Studi dan Analisis Algoritma RIVEST CODE 6 (RC6) Dalam Enkripsi/Dekripsi Data. In Seminar Nasional Aplikasi Teknologi Informasi (SNATI).

[6] Firdaus, C., Wahyudin, W., & Nugroho, E. P. (2017). Monitoring System with Two Central Facilities Protocol. Indonesian Journal of Science and Technology, 2(1), 8-25.