Improving the Security Guarantees, Authenticity and Confidentiality in Short Message Service of Mobile Applications

[1,2]Teddy Mantoro, [2]Laurentinus
[1] Faculty Science and Technology, USBI-Sampoerna University, Jakarta, Indonesia
[2] Graduate Program, Budi Luhur University, Jakarta, Indonesia

***Abstract*- The advancement in telecommunications technology has allowed people to communicate in various ways, one of them is using mobile phone device. However, security issues such as authenticity and confidentiality of data or information are still cannot be guaranteed. Messages delivered through SMS can be easily stolen by unauthorized parties because SMS sent via BTS will be accepted by Message Service Center (SMSC), where the operator can view the message contents. There are 2 main features that specify and differentiate between RSA and RC6, they are the Time Consumed for Encryption & Decryption message and the Ability to protect the data from unauthorized parties. This study begins with a comparative analysis of performance and security of the most useful algorithms: RC6 (Rivest Cipher) and RSA (Rivest Shamirdan Adleman), Then the complexity of encryption and decryption algorithms to obtain better algorithms are discussed. As proof of concept, a prototype for encryption and decryption of SMS was developed based on Android platform. The result of this study shows that all messages can bee encrypted using a key generated before being sent to the receiver which has better security and time performance.**

Keywords: Cryptography, SMS Encryption, SMS Decryption, RSA, RC6 (Rivest Cipher), Mobile Android.

I. INTRODUCTION

Mobile phones provide a variety of features, one of them is Short Message Service (SMS). SMS is a service that allows users to communicate by sending short text messages quickly and cheaply. Security is an important aspect of data communication, but unfortunately, protection of SMS data is not secure. Therefore it is necessary for encryption and decryption applications to ensure the security and integrity of the messages from misuse.

Cryptography is a technique to hide and secure data over communication channels. Selection of the right algorithm is an important aspect, seen from the level of interest and confidentiality of data. Good algorithms that generate encryption must be unpredictable and cannot be solved using any means.

With cryptography on the application, all messages can be encrypted before sending to the receiver. The receiver needs the decryption key to decrypt the cipher text. After the analysis, design and implementation of the RC6 algorithm and the RSA algorithm tests, the test results of each algorithm's performance and security is obtain and presented on a comparison chart to show advantages and disadvantages of each algorithm in securing an SMS message.

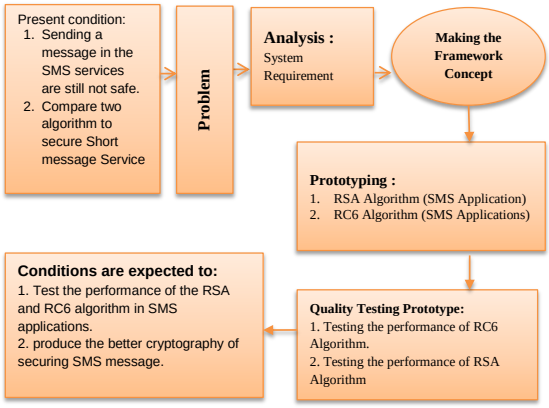

Fig. 1. Framework Concept

II. RELATED WORK

Position additional third primes to modify the RSA algorithm has been performed in [1] with an additional modifying primes, then the security level is increased because the factoring complexity of variable.

A number of SMS service studies make mobile applications as one of the future possibilities in the data communication. Implementation of the RSA algorithm in the SMS application has been discuss in [2, 3] by applying RSA algorithm based on Android application to secure SMS apps.

While the performance analysis (Execution time and Resource Utilization) of RC6, twofish and Rijndael Block Cipher Algorithms has been discussed clearly in [4].

Two different cryptography methods are applicable with SMS: the comparison between the DES Private key based Algorithm and RSA public key based algorithm [5] which discussing the encryption throughput and decryption throughput.

The public key algorithms RSA and enhanced RSA has been evaluated and compared based on execution time to enhance the security of RSA algorithm [6].

A structure proposed improvements to RC6 encryption algorithm that have the same structure of encryption and decryption. Device algorithm using simple rotation and XOR operation will be useful to the application which require same procedure of encryp data and decrypt data as light mobile device and RFIDs[11].

Implementation of the RC6 algorithm in the SMS application by applying RC6 Algorithm for encryption and decryption has successfully been used in service of sender and receiver message from Short Message Service [9].

Three different cryptography methods were compared which implemented three encryption techniques like AES, DES and RSA algorithms and compared their performance of encryption techniques based on the analysis of its stimulated time at the time of encryption and decryption [10].

III. RC6 AND RSA ALGORITHM FOR MOBILE DEVICES

RC6 algorithm is one method that uses symmetric-key encryption and serves to maintain data confidentiality. The algorithm uses the same key for encryption and decryption. RSA algorithm is an algorithm that uses an asymmetric key. RSA uses 2 keys for encryption and decryption; there is the private key and the public key by factoring very large numbers.

Phase 1: RSA Algorithm and RC6 Algorithm

a. RC6 Algorithm

RC6 algorithm (Rivest Cipher) is one candidate for the Advanced Encryption Standard (AES) submitted by RSA Security Laboratories at NIST. Designed by Ronald L Rivest, M.J.B. Robshaw, R. Sidney and Y.L. Yin. The algorithm is the development of RC5 algorithms and have fulfilled all the requirements put forward by NIST. RC6 is an algorithm that uses up to 128-bit block size, with key sizes used varied between 128, 192 and 256 bits.

RC6 algorithm is equipped with a number of parameters, so written as RC6-w / r / b. Parameter w is the word size in units of bits, the parameter r is an integer that indicates the number of iterations during the encryption process and the parameter b indicates the encryption key size in bytes. After the algorithm is included in the AES candidates, it was determined that the value of w = 32, r = 20 and b varies between 16, 24 and 32 bytes. RC6-w / r / b split the blocks of 128 bits into 4 pieces of 32-bit blocks, and follow the rules of the six basic operations as follows:

a + b :	addition operation	a - b :	reduction operation
a ⊕ b :	exclusive-OR (XOR) operation	a x b :	multiplication operation
a<<<b:	a shifted to the left as much as the second variable (b)	a>>>b:	a shifted to the right as much as the second variable (b)

b. RSA Algorithm

RSA cryptographic algorithms discovered in 1976 by researchers of MIT (Massachusetts Institute of Technology) by Ron (R)ivest, Adi (S)hamirdan, Leonard (A)dleman.
RSA algorithm is an asymmetric algorithm that uses two keys to make the process of coding data.

RSA uses prime numbers to generate public key and private key based on mathematical facts and multiplying large numbers together. It uses the block size data in which plaintext and cipher text are integers between 0 and 1 for some n values. Size of n is considered 1024 bits or 309 decimal digits. Public key is used for encryption and private key is used for decryption purpose. As sender knows encryption key and send the private key to receiver [8].

The security of RSA algorithms lies in the difficulty of factoring large numbers into prime factors. Factoring is done to obtain the private key.

Phase 2: Key Generation

a. Key Generation of RC6 Algorithm

RC6 algorithm uses 44 pieces of sub keys generated from the keys and called the S[0] to S[43]. Each sub-key length is 32 bits.

ROTL (Z:word32; Y:integer) → word32 (the function to rotate bit as much as the second variable)

```
Input(key)
S[0] ← b7e15163
For I ← 1 to 43 do
    S[i] ← S[i-1] + 9e3779b9
End for
A ← B ← i ← j ← 0
V ← 44
If (c > v) then
    v ← c
    v ← 4 * 3
For s ← 1 to v do
  A ← S[i] ← ROTL ((S[i] + A + B) .3 )
  B ← L[j] ← ROTL (L[j] +A + B, A + B)
   i ← (i+1) mod 44
   j ← (j_1) mod c
Endfor
```

b. Key Generation of RSA Algorithm

1) Choose large numbers of two primes, p and q.
2) Calculate $r = p.q$. Preferably $p \neq q$, because if $p = q$ then $r = p^2$ so p can be obtained by drawing the square root of r.
3) Calculate $\phi(r) = (p - 1)(q - 1)$.
4) Select the public key PK, which are relatively prime to $\phi(r)$.
5) Generate a secret key by using equation (5), $SK \cdot PK \equiv 1 \pmod{\phi(r)}$.

$SK \cdot PK = 1 \pmod{\phi(r)}$ is equivalent to the $SK \cdot PK = 1 + m\phi(r)$, so that SK can be calculated by:

$$SK = \frac{1 + m\phi(r)}{PK}$$

Results of the above algorithm generate a key pair: The public key is the pair (PK, r) and the private key is the pair (SK, r)

Phase 3: Encryption

a. Encryption process of RC6 Algorithm

Because RC6 algorithm breaks down into 4 pieces of 32-bit blocks, then this algorithm works with 4 pieces of 32-bit registers A, B, C, D.

The first byte of plaintext or cipher text is placed on bytes A, while the last byte is placed in byte D. In the process will be obtained (A, B, C, D) = (B, C, D, A) which means that the value that lies on the right side are from the registers on the left.

The following block diagram will explain the encryption process of RC6 algorithm:

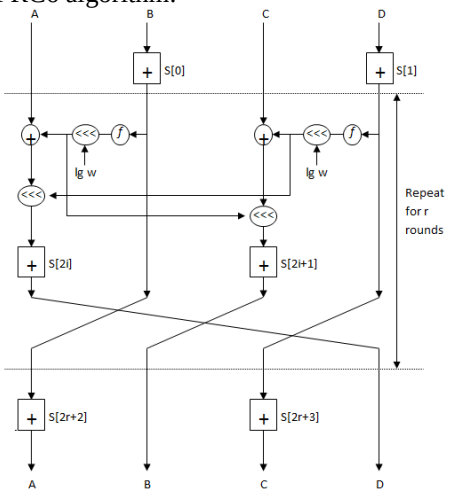

Fig. 2. Block Diagram of RC6 Algorithm

RC6 encryption process includes three things:

Dictionary :
Temp, Z, z, u, t : word32
S : Array [0.. 43]; I, Y : Integer

1) Early Whitening Algorithm
   Z[1] ← Z[1] + S[0]
   Z[3] ← Z[3] + S[1]

2) Iteration
   For I ← 1 to 20 do
   t ← ROTL ((Z[1] *(2 * Z[1] + 1)), 5)
   u ← ROTL ((Z[3] *(2 * Z[3] + 1)), 5)
   z[0] ← (ROTL((Z[0] XOR t), u)) + S[2*i]
   z[2] ← (ROTL((Z[2] XOR u), t)) + S[2*I + 1]
   temp ← Z[0]
   Z[0] ← Z[1]
   Z[1] ← Z[2]
   Z [2] ← Z[3]
   Z[3] ← Temp
   End For

3) End Whitening Algorithm
   Z[0] ← Z[0] + S[42]
   Z[2] ← Z[0] + S[43]

b. Encryption process of RSA Algorithm

Cryptography uses the encryption technique to send confidential messages through an insecure environment.

The encryption algorithm formula of RSA Algorithm :

$$C = n^e \bmod N$$

Description:

C : Chiphertext / messages that have been encrypted.
n : Plaintext / message
e : Enciphering Exponent
N : (RSA) Modulus

Phase 4: Decryption

a. Decryption process of RC6 Algorithm

Dictionary :
ROTL(Z : word32; I,Y:integer)
Temp, u, t : word32
I : Integer

Algorithm :
Z[2] ← Z[2] – S[43]
Z[0] ← Z[0] – S[42]

For I ← 20 downto 1 do
Temp ← Z[3]
Z[3] ← Z[2]
Z[2] ← Z[1]
Z[1] ← Z[0]
Z[0] ← Temp
u ← ROTL ((Z[3] * (2*Z[3] + 1)), 5)
t ← ROTL ((Z[1] * (2*Z[1] + 1)), 5)
Z[2] ← (ROTR (Z[2] – S[2*i+1]), t) XOR u)
Z[0] ← (ROTR (Z[0] – S[2*i]), u) XOR t)
End for

Z[3] ← Z[3] – S[1]
Z[1] ← Z[1] – S[0]

b. Decryption process of RSA Algorithm

To open an encrypted message, then we need the key (N, d) to decryption using the following formula :

$$n = c^d \bmod N$$

Description:

C : Chiphertext / messages that have been encrypted.
n : Plaintext / message
e : Enciphering Exponent
N : (RSA) Modulus

IV. EXPERIMENTAL

a. The Implementation of Encryption and Decryption SMS Application with RC6 Algorithm

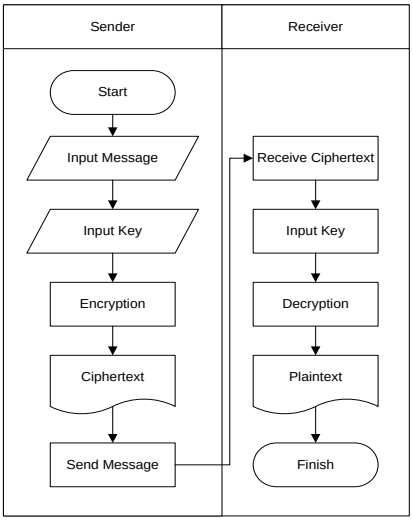

Fig. 3. Application Flowchart using RC6 Algorithm

1) Main Page

The following is the main page menu Encryption and Decryption SMS application using RC6 algorithm. Which include the menu of Write Message, Inbox, and About.

Fig. 4. Main Page of Application using RC6 Algorithm

2) Write Message Page

Write Message page contains:

No Tujuan : Receiver phone number
Kunci : Key
Pesan : Message
Hasil : Cipher text

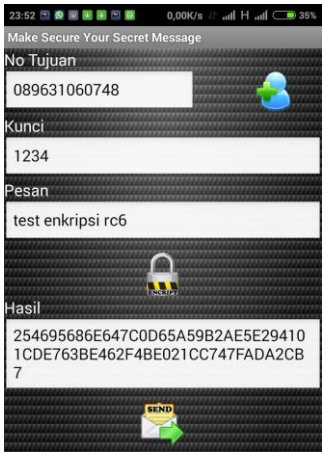

Fig. 5. Write Message Page

3) Receive Message Page

Receive SMS without using the application

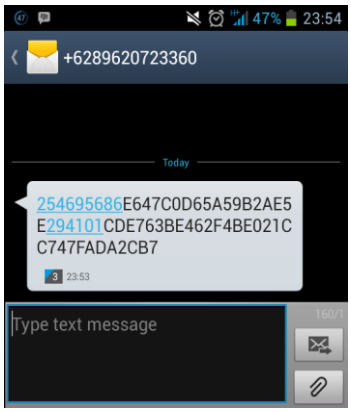

Fig. 6. Encrypted Message

The Decryption page using apps

The results message that has been decrypted using the same key with the encryption key

Fig. 7. Message Decryption with RC6 Algorithm Application

a. Implementation of Encryption and Decryption messages with RSA Algorithm

Generate Key Flowchart on RSA Algorithm :

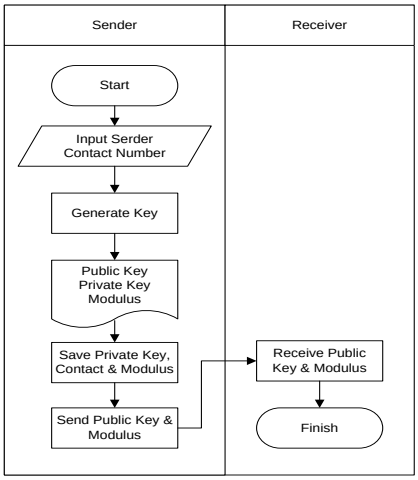

Fig. 8. The generate key flowchart using RSA Algorithm

Encryption & Decryption Flowchart on RSA Algorithm :

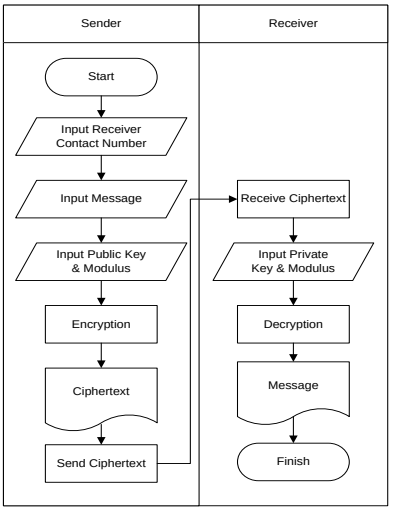

Fig. 9. The Application flowchart using the RSA Algorithm

1) Encryption Page

The Main page of Encryption and Decryption Message using RSA Algorithm.

Fig. 10. Main Page of RSA Algorithm Application

2) Create Message Page

Create a message contains:

No. tujuan : Receiver phone number
pesan : plaintext message
Private Key
Modulus
Cipher text

Fig. 11. Write Message page with RSA Applications

3) Receive Message

Message Inbox contains the contents of the list cipher text message.

Fig. 12. List Message of RSA Algorithm Application

4) Decryption Page

Decryption Message page contains :

Phone Number : Sender
Message : Cipher text
Private Key
Modulus

When the contents of Private Key D correctly then it will display the results (Message).

Fig. 13. Message Decryption with RSA Algorithm Application

V. Experimental Result

A. Performance

Performance can be determined by calculating the processing time to generate the key(s) and complete the encryption. Comparisons were made using the same key length of 128 bits.

Performance of RC6 Algorithm

RC6 algorithm uses one key for encryption, and does not depend on the length of the key. Time to generate the key is the same, although the key input is 128, 192 or 256 bits. Encryption and decryption process is also very fast and stable.

Performance of RSA Algorithm

RSA algorithm uses two keys: The public key and private key. It takes time to generate key to produce the value of N (modulus).

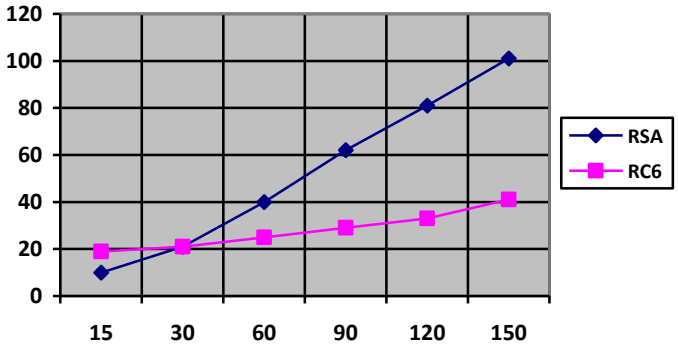

Fig. 14. Response Time (millisecond) of Encryption based on message characters

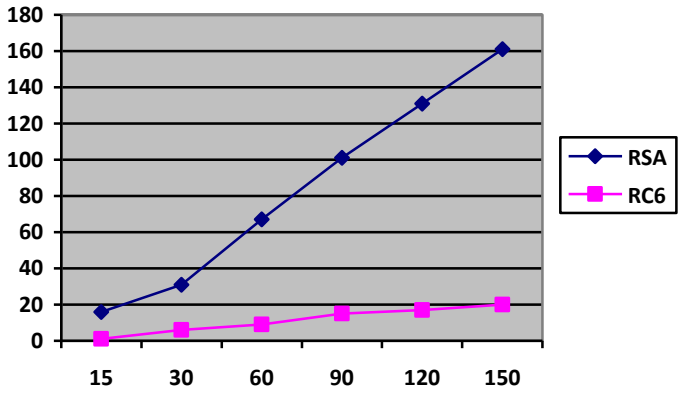

Fig. 15. Response Time (millisecond) of Decryption based on message characters

RSA Algorithm Result

The average response time in the encryption process is 0.68 milliseconds/character. The average response time in the decryption process is 1.08 milliseconds /character.

RC6 Algorithm Result

The average response time in the encryption process is 0.54 milliseconds/character. The average response time in the decryption process is 0.14 milliseconds/character.

Character of communication culture in Indonesia is a high context culture. This culture focuses on provision of very high meaning in the context or nonverbal message. For the purpose of desire, high context culture communicator always speaks convoluted. They avoid the explicit meaning of their main message and let others infer their meaning through implicit nonverbal aspects. Chit-chat cultural has become a trademark of its own to the people of Indonesia. Chit Chat has significant impact on the length of the message.

Application of Encryption on SMS applications using RSA algorithm and Algorithm RC6, affect the length of the message that was sent while the maximum length of 1 SMS message is 160 bytes. It becomes less effective and cost-efficiency.

B. Security

In the RC6 algorithm, key length and number of rounds is the most important thing in security encryption. RC6 uses data-dependent rotations that lead to the spread of bits that cannot be predicted.

At RSA, factoring problem is factoring n into two prime factors, p and q, such that n = p.q. Once successfully factored n into p and q, then φ (n) = (p-1) (q-1) can be calculated. Furthermore, because the encryption key e, then the decryption key d can be calculated from the equation e.d = 1(mod ϕ (n)).

For the value of p and q with a length 100 digits then n = p x q will measure more than 200 digits. It takes 4 billion years to find the prime factors of a 200 digit number.

RSA algorithm is much more complex than the work flow of RC6 algorithm. This is because the number of calculations and generate encryption key.

There are approaches to attack the RSA Algorithm :

1) Factoring the prime numbers .from mathematical side, we need to solve the factoring problem i.e., find the prime numbers.
2) Brute force all possible private key, but when the picked numbers are large, brute force is not

VI. CONCLUSION

This study proposed on how to increase the security guarantees, authenticity and confidentiality in Short Message Service of Mobile Applications. One way is by measuring the comparison between RSA and RC6 Algorithm. The following is the detail conclusion from this work:

First; there is significantly different time response of encryption & decryption message, the encryption & decryption time of RC6 Algorithm is faster than RSA Algorithm.

Second; apply cryptography on SMS Application impact on the length of message. The maximum length of an SMS message is 160 characters.

Third; the security of RSA Algorithm depends upon the two large prime numbers, Encryption & Decryption key, the mathematical calculation are consider strong and difficult to break.

Fourth; implementation of the RSA Algorithm and RC6 Algorithm on SMS Application is show to increase security. The cipher text cannot be read without using the correct key.

REFERENCES

[1] Al-Hamami, A. H., & Aldariseh, I. A. Enhanced Method for RSA Cryptosystem Algorithm. In Advanced Computer Science Applications and Technologies (ACSAT), 2012 International Conference on (pp. 402-408). November 2012.

[2] Dewanto, Joko and Verdy Yanto, "Pembuatan Aplikasi SMS Kriptografi RSA dengan Android", Forum Ilmiah Volume 10 No.2, Mei 2013.

[3] Alvianto, Andi Riski and Darmaji, "Pengaman Pengiriman Pesan Via SMS dengan Algoritma RSA Berbasis Android", Jurnal Sains dan Seni ITS Vol 4, No.1, 2015.

[4] Verma, Harsh Kumar and Ravindra Kumar Singh, "Performance Analysis of RC6, Twofish and Rijndael Block Cipher Algorithms", International Journal of Comuter Applications (0975 – 8887) Vol. 42 No.16, March 2012.

[5] Singh, Sombir, Sunil K Maakar,and Sudesh Kumar, "A Performance Analysis of DES and RSA Cryptography", International Journal of Emerging Trends & Technology in Computer Science Vol. 2 Issue 3, June 2013.

[6] Preetha, M. and M. Nithya, "A study and Performance Analysis of RSA Algorithm", IJCSMC Vol. 2 Pg. 126-139 , June 2013.

[7] Kahate, Atul,"Cryptography and Network Security, 2nd Ed", Tata McGraw-Hill, New Delhi, 2005

[8] Defni and Indri Rahmayun, "Enkripsi SMS (Short Message Service) Pada Telepon Selular Berbasis Android Dengan Metode RC6", Jurnal Momentum Vol.16 No.1, Februari 2014.

[9] Mahajan, Prerna and Abhishek Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web & Security, Volume 13, 2013.

[10] Safaat, N. H, "Android Pemrograman Aplikasi Mobile Smartphone dan Tablet PC Berbasis Android", Bandung: Informatika, 2012.

[11] J. N. Kim, G. Y. Cho "An improved RC6 algorithm with the same structure of encryption and decryption", Advanced Communication Technology (ICACT), International Conference on (Vol. 02).2009.