A combination of Rivest Shamir Adlemann (RSA) and Affine Cipher method on improvement of the effectiveness and security of text message

M Jannah¹,a, B Surarso² and Sutimin²
¹Magister Program of Mathematics, Departemt of Mathematics, Faculty of Science and Mathematics, Diponegoro University, Jl. Prof. Soedharto, SH, Tembalang Semarang 50275, Indonesia
²Department of Mathematics, Faculty of Science and Mathematics, Diponegoro University, Jl. Prof. Soedharto, SH, Tembalang Semarang 50275, Indonesia
È-mail: mieta.valentz@gmail.com

Abstract. Rivest Shamir Adlemann (RSA) method is one of the popular methods in the field of public key cryptography. The strength of the RSA method is based on the difficulty level of factoring of two large prime numbers. If they are factored easily, then we need to use brute force to break the system. In this present, we combined RSA method with classical method, namely Affine Cipher method to improve the level of security on text message. The process of combination RSA method and Affine Cipher method is as follow: first, text message was encryption using Affine Cipher method, then the encryption output is used as input of the RSA method. The results certified that the improvement of the security level of text message can be realized by using the combined method.

1. Introduction
The best way to secure text message is cryptography [1]. Nowadays, many methods of cryptography based on public key. Public-key cryptography can be claimed as the greatest method in the field of cryptography because it is used for both confidentiality and authentication [2, 3]. The RSA method is the most popular of public key cryptography method and asymmetric encryption. In 1977, Ron Rivest, Adi Shamir and Len Adleman developed the first major asymmetric encryption. The encryption algorithm of the RSA method is referring to one way function assumptions which is generated by modular exponential function in multiplication group ($\mathbb{Z}^*_n, x$) and multiplication group ($\mathbb{Z}^*_\varphi(n), x$) with $n = p \times q; p, q$ are prime numbers. and $\varphi(n) = (p - 1)(q - 1)$. RSA method has the strength in multiplication of two large prime numbers [6]. If the two large numbers can not to solved easily or takes a long time for solved it, so the level of algorithm effectiveness is very good. It also oppositely. If they are factored not easily, then we need to use brute force in order to break the system [3].

Many studies about the RSA method, such as: An Enhanced and Secured RSA Key Generation Scheme (ESRKGS) [3]. The study stated that the RSA method using two prime number could be calculated easily. The process and procedure of cryptography more complex in this era. So, this studies is modifying the RSA method using four prime numbers for improving the security of the RSA method. But, it can be calculated if we are factoring $n$. So, that system can be solved [4]. And also, The
combination of RSA and Block Cipher Algorithms to maintain message authentication [5]. In this study, the RSA method was combined with the Block Cipher method has a higher security than the traditional RSA method. However, the method only applies to type 1024 bits. In this present, we combined RSA method with Affine Cipher method to improve the effectiveness and secure of the system. We use the RSA method because the RSA method is one of the effective methods used to secure messages with text message types and it is still used today. And we use the Affine Cipher method because it has the same characteristics as the RSA method, which is a more effective method used for alphabetic, because the Affine Cipher method is a monoalphabetic method. And both of them use basic mathematic modulo. The process of the combined RSA method as follow: first, text message was encryption using Affine Cipher method then the encryption output is used as input of the RSA method. The output will be evaluated using the theory of factoring method.

2. Preliminaries
2.1. RSA Method
RSA is an asymmetric cryptography algorithm based on a public key cryptosystem [6]. RSA method was founded in 1977 by Rivest, Shamir & Adelman. RSA method is based on factoring problem of finding of two large prime numbers. The mathematical basic used by the RSA method is congruent equation, residue class ring, division of the residue class ring, group, multiplicative group of residue, fermat theorem. Two keys generated by RSA is a public key for encryption and private key to decryption message. RSA method consists of three steps:

2.1.1. Key generators
Step one is key generators that is used as key to encrypt and decrypt messages. There are two keys used, namely the public key and the secret key. The steps is following as:
Figure 1. Flowchart of Key Generation

The description of Fig. 1 is as follow:

1. Choose two large prime numbers for p and q. The value of p and q must be kept secret.
2. Calculate the modulus value
   \[ n = p \times q \]  \hspace{1cm} (1)
   should \( p \neq q \), because if \( p = q \) then \( n = p \times p = p^2 \), so p can be obtained by square root from \( n \) and \( n \) does not need be kept secret.
3. Calculate using the Euler function
   \[ \varphi(n) = (p - 1)(q - 1) \]  \hspace{1cm} (2)
   An integer \( n \) is called modulus.
4. Select the random integer as a public key is denoted \( e \), so that
   \[ (e, \varphi(n)) = 1, 1 < e < \varphi(n) \]  \hspace{1cm} (3)
5. By using the expended Euclid algorithm, then it will calculated inverse of \( e \), so
   \[ d \times e = 1 \pmod{\varphi(n)} \]  \hspace{1cm} (4)
   Or
   \[ d = e^{-1} \pmod{\varphi(n)} \]

Where \( k \) is the plaintext, and \( d \) is the ciphertext.

Then the result of the algorithm is obtained: the public key is the pair \((n, e)\) and the secret key is the pair \((n, d)\)

2.1.2. Encryption.
Step two is encryption. Encryption is a process carried out to change the original text message or message that can be understood to be a form of certain codes that cannot be understood. From the plaintext it is converted to ciphertext by using the formula as follows:

\[ C = M^e \mod n \]  

(5)

2.1.3. Decryption.
Step three is decryption, decryption is a process that is carried out to change messages with certain types of codes that cannot be understood to be understandable original messages. From the ciphertext it is converted to the plaintext by using the formula as follows:

\[ M = C^d \mod n \]  

(6)

2.2. Affine Cipher Method
Affine cipher is a monoalphabetic method and it is one of type of substitution ciphers and a well known encryption method [7]. Substitution techniques on Affine Cipher method use linear function \( sx + t \). In Affine Cipher, each plaintext is first mapped to the integer in the range \( 0 \sim M - 1 \) for a fixed integer \( M \) and then uses modular arithmetic to the integer into another integer namely ciphertext. The encryption function is

\[ E(x) = (sx + t) \mod M \]  

(7)

Where \( M \) is a modulo, \( s \) and \( t \) are the secret key \((s \neq 0, t \neq 0)\). The decryption function is

\[ D(x) = s^{-1}(x - t) \mod M \]  

(8)

Where \( s^{-1} \) is the modular multiplicative inverse of a modulo \( M \).

3. The Proposed Method
Cryptography is a method that can be used to secure the text message. The new proposed approach of RSA method and Affine Cipher Method has been introduced in this section. Combination of RSA method increases the level security and makes the system more efficient than the traditional RSA method and Affine Cipher method. When User A (sender) want to send a text message to the other, User B
(receiver) use combination RSA method with Affine Cipher method. The algorithm of the proposed method is as follow:

Step 1: Key Generators

This key generator is the same as the key generators in the RSA method in general.

1. Choose two large prime numbers for $p$ and $q$. The value of $p$ and $q$ must be kept secret.
2. Calculate the modulus value

   \[ n = p \times q \quad (1) \]

   should $p \neq q$, because if $p = q$ then $n = p \times p = p^2$, so $p$ can be obtained by square root from $n$ and $n$ does not need be kept secret.
3. Calculate using the Euler function

   \[ \varphi(n) = (p - 1)(q - 1) \quad (2) \]

   An integer $n$ is called modulus.
4. Select the random integer as a public key is denoted $e$, so that

   \[ (e, \varphi(n)) = 1, 1 < e < \varphi(n) \quad (3) \]
5. By using the expended Euclid algorithm, then it will calculated inverse of $e$, so

   \[ d \times e = 1 \pmod{\varphi(n)} \quad (4) \]

   Or

   \[ d = e^{-1} \pmod{\varphi(n)} \quad (5) \]

   Where $k$ is the plaintext, and $d$ is the ciphertext.

Then the result of the algorithm is obtained: the public key is the pair $(n, e)$ and the secret key is the pair $(n, d)$

Step 2: Encryption

This encryption process uses a combination of two encryption algorithms, namely the RSA algorithm and the Affine Cipher algorithm which are done sequentially. The steps are as follows:

1. Change text message to ciphertext with the encryption Affine Cipher. By using a formula:

   \[ E_1(x) = (sx + t) \pmod{M} \quad (6) \]
2. Change the first ciphertext with the encryption RSA. By using a formula:

   \[ E_2 = E_1^e \pmod{n} \quad (7) \]

By using this purposed method, the ciphertext obtained is not easy to solve. To prove it, we used the factoring method.
4. Result and Discussion

The implementation of the combination of the RSA method with the Affine Cipher method is the use of password. An example of encryption message of combination RSA algorithm is as follow:

Assume that User A wants to password “MAGMA UNDIP” to User B. Then the algorithm is as follow:

Step 1: Key Generators
User A
1. Choose two large primes
   \( p = 11 \) and \( q = 13 \)
2. Calculate the modulus value
   \( n = p \times q = 11 \times 13 = 143 \)
3. Calculate using The Euler Function
   \( \varphi(n) = (p - 1)(q - 1) = (11 - 1)(13 - 1) = 10 \times 12 = 120 \)
   \( e = 19 \)
4. Select \( d \) to satisfy \( d \times e \equiv 1 \pmod{\varphi(n)} \)
   \( d = 19 \)
   \( 19 \times 19 = 361 = 1 + 3 \times 120 \)

Step 2: Encryption
1. Suppose the message (plaintext) to be sent: MAGMA UNDIP” or in the decimal system (ASCII encoding) is 77 97 103 109 97 32 85 110 100 105 112
2. Choose \( s = 7 \) and \( t = 10 \). Because alphabet is used with 26 letters, then \( M = 26 \)
3. Change text message to ciphertext with \( E_1(x) = (sx + t) \mod M \). Then the results of ciphertext 1 in decimal system is 3 13 3 19 13 0 7 0 8 17 14
4. Change the first ciphertext with \( E_2 = E_1^e \mod n \)
the result of ciphertext 2 in decimal system is 27 37 27 19 37 0 103 0 32 113 104

So, the code (ciphertext) from of the password is ←%←‼%(none)g(none)(space)qh

From the example above it can be seen that the whole process of encryption with RSA method and Affine Cipher method produce complicated ciphertext, it forms the number of series so that the key algorithm will be difficult to solve or use brute force in order to break the system.

To prove that the plaintext cannot be solved is by using the factoring method, as follows

$$kn = x^2 - y^2 \quad (9)$$

For example:
Calculate the factor of \( n = 143 \) use Factoring Method with \( k \) is odd prime.
By using the equation of Kraitchik Method, then the result is \( p = 13 \ q = 11 \)
Plaintext can be found from ciphertext. That is by using decryption process with formula:

$$M = C^d \ mod \ n$$

Where in the example is obtained \( d = 20 \), then

$$M = 27^{20} \mod \ 143 = 1$$

1 is not the real plaintext, because the real plaintext is 77.

So, the result of combination RSA method and Affine Cipher method is ciphertext cannot be solved become the real plaintext. So, combination of RSA method and Affine Cipher can improve the effectiveness and secure of text message.

5. Conclusion
In this paper a combination of the RSA method and Affine Cipher method has been developed to secure the text message. The result shows that a combination of RSA method and Affine Cipher produces a series of number of ciphertext. The effect of ciphertext is more complicated to solve or use brute force in order to break the system. So with the combination of RSA method and Affine cipher can to improve effectiveness and the level of security of text message.

References
[1] Joshi A, Wazid M and Goudar R H 2015 Procedia Computer Science 48 360
[2] Starikovskiy A, Zhgilev A and Shevchenko 2017 Procedia Computer Science 123 457
[3] Thangavel M, Varalakshmi A, Murrali M and Nithya K 2014 Information Security and Applications 30 10004
[4] Luy M, Karatas Z and Ergin H 2016 Information Security and Applications 03 006
[5] Tarigan S Y, Ginting DS, Gaol M L and Sitompul K L 2017 IOP Conf Series: Journal of Physics Conference Series 930 012009
[6] Patil P, Narayankar P, Narayan D G and Meena S M 2016 Procedia Computer Science 78 617
[7] Zhu H, Zhao C, Zhang X and Yang L 2014 Optik 125 6672