The Combination of RSA And Block Chiper Algorithms To Maintain Message Authentication

Sepri Yanti Tarigan¹, Dewi Sartika Ginting², Melva Lumban Gaol³, Kristin Lorensi Sitompul⁴
¹,²,³,⁴Magister of Information Technology, Universitas Sumatera Utara

Email: saveyanti@gmail.com

Abstract. RSA algorithm is public key algorithm using prime number and even still used today. The strength of this algorithm lies in the exponential process, and the factorial number into 2 prime numbers which until now difficult to do factoring. The RSA scheme itself adopts the block cipher scheme, where prior to encryption, the existing plaintext is divide in several block of the same length, where the plaintext and ciphertext are integers between 1 to n, where n is typically 1024 bit, and the block length itself is smaller or equal to log(n)+1 with base 2. With the combination of RSA algorithm and block chiper it is expected that the authentication of plaintext is secure. The secured message will be encrypted with RSA algorithm first and will be encrypted again using block chiper. And conversely, the ciphertext will be decrypted with the block chiper first and decrypted again with the RSA algorithm. This paper suggests a combination of RSA algorithms and block chiper to secure data.

Keywords: RSA algorithm, Block chiper, Message authentication

1. Introduction
The security of information in this global age has become a vital necessity in some aspects of life. However, in the rapid development of information technology recently have a positive and negative impact where it becomes a convenience to everyone to get an information or a data without having to require a long process. Various ways do a lot of people to get it. Therefore, there should be a method used to secure information from unauthorized parties. One of the methods used is cryptography.

According to Request for Comments (RFC), cryptography is a mathematical science that made data incomprehensible (to hide its meaning), to prevent it from unauthorized change, or to prevent it from unauthorized use. If the transformation can be restored, cryptography means the process of converting back encrypted data into understandable form. Cryptography itself has the goal of confidentiality, data integrity, message authentication and non-repudiation. In this paper will discuss how to maintain message authentication.

One of the algorithms in cryptography is RSA. RSA algorithm is public key algorithm using prime number and even still used today. The power of this algorithm lies in the exponential process, and the number of factorials into 2 prime numbers which until now difficult to perform is known. The
RSA scheme itself adopts a block cipher scheme, where before encryption, the existing plaintext is divided into several blocks of the same length, where the plaintext and ciphertext are integers between 1 and n, where n is usually 1024 bits, and the block length itself more small or equal to \( \log(n) + 1 \) with base 2. With combination of RSA algorithm and block cipher, expected message authentication can be maintained.

2. Review Of Literature
2.1 Cryptography
Cryptography (cryptography) is derived from the Greek, kryptos means hidden and graphia means something written so that cryptography can also be called as something written in secret or hidden.

According to its terminology, cryptography is an art and a science of keeping messages safe when messages are sent from one place to another.

In cryptography, messages or information referred to plaintext or clear text. The process of transforming the original text (plaintext) into secret text (ciphertext) is called encryption. Unreadable messages are called secret text (ciphertext). The reverse process of encryption is called decryption. Decryption will return the secret text (ciphertext) to the original text (plaintext). Both encryption and decryption processes require the use of some secret information, often called keys. There are four fundamental objectives of this cryptographic science which is also an aspect of information security that is, confidentiality, data integrity, authentication and non-repudiation or non-deny.

Cryptography based on the key used in the process of encryption and decryption is divided into two parts:

a. Cryptography symmetry, this algorithm is also called classical algorithm because it use the same key for the process of encryption and decryption. Other terms of this cryptography are private key cryptography, secret-key cryptography, or conventional cryptography. In symmetry key cryptography it can be assumed that the recipient and the sender has first shared the key before the message is sent. The security of this system lies in the secrecy of the key.

b. Asymmetry Cryptography, Unlike the symmetry key cryptography, public key cryptography has two distinct keys to the encryption process and its description. Another name for this asymmetric key is key cryptography Public (public-key cryptography). The key to encryption in cryptographic asymmetry is not secret (publicly known), while the key to decryption is confidential (private key). The sender's entity will encrypt it by using the public key, while the receiving entity decrypts using the private key. Scheme of the cryptographic process this asymmetry is in the following figure.

There are two basic techniques commonly used in cryptography symmetry is a substitution technique in which the replacement of each plaintext character with other characters and transposition techniques (permutations) where this technique using character permutation. Some algorithms that use the same key (symmetry) include Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES).

There are two basic techniques commonly used in cryptography symmetry is a substitution technique in which the replacement of each plaintext character with other characters and transposition techniques (permutations) where this technique using character permutation. Some algorithms that use the same key (symmetry) include Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES).

2.1 Cryptography
Cryptography (cryptography) is derived from the Greek, kryptos means hidden and graphia means something written so that cryptography can also be called as something written in secret or hidden.

According to its terminology, cryptography is an art and a science of keeping messages safe when messages are sent from one place to another.

In cryptography, messages or information referred to plaintext or clear text. The process of transforming the original text (plaintext) into secret text (ciphertext) is called encryption. Unreadable messages are called secret text (ciphertext). The reverse process of encryption is called decryption. Decryption will return the secret text (ciphertext) to the original text (plaintext). Both encryption and decryption processes require the use of some secret information, often called keys. There are four fundamental objectives of this cryptographic science which is also an aspect of information security that is, confidentiality, data integrity, authentication and non-repudiation or non-deny.

Cryptography based on the key used in the process of encryption and decryption is divided into two parts:

a. Cryptography symmetry, this algorithm is also called classical algorithm because it use the same key for the process of encryption and decryption. Other terms of this cryptography are private key cryptography, secret-key cryptography, or conventional cryptography. In symmetry key cryptography it can be assumed that the recipient and the sender has first shared the key before the message is sent. The security of this system lies in the secrecy of the key. Scheme of the cryptographic process this asymmetry is in the following figure.

b. Asymmetry Cryptography, Unlike the symmetry key cryptography, public key cryptography has two distinct keys to the encryption process and its description. Another name for this asymmetric key is key cryptography Public (public-key cryptography). The key to encryption in cryptographic asymmetry is not secret (publicly known), while the key to decryption is confidential (private key). The sender's entity will encrypt it by using the public key, while the receiving entity decrypts using the private key. Scheme of the cryptographic process this asymmetry is in the following figure.
This asymmetry cryptography can be analogized like a locked mailbox and has a hole to insert mail. Everyone can put a letter into the mailbox, but only the owner of the letter has a key and can open the mailbox. The public key that have sent to the recipient through the same channel as the channel used to send the message, no need to fear because the unauthorized parties will not be able to decrypt the message, because it does not have a private key, or the recipient can provide the sender with the public key. Some algorithms that use different keys (asymmetry) include Digital Signature Algorithm (DSA), Rivest Shamir Adleman (RSA), Diffie-Helman (DH), Quantum Cryptography.

2.2 RSA Algorithm

The RSA algorithm comes from a combination of three names. The researchers are Ron RIvest, Adi Shamir and Leonard Adleman. This cryptographic method is classified into modern cryptography which consists of two keys, namely public key (public key) to perform encryption and privacy key (private key) to do the decryption.

Encryption converts the original data (plaintext) to the encoded data (ciphertext), while the decryption is returning the ciphertext to the plaintext.

RSA algorithm is divided into 3 steps:
1. Key Generators
   a. Select 2 large primes for p and q
   b. Calculate the modulus value
      \[ n = pxq \]  
   c. Calculate using the Euler function
      \[ \phi (n) = (p-1) x (q-1) \]  
   d. Select the random integer e as a public key, provided that it meets the Greater Common Divisor
      \[ (e, \phi (n)) = 1, 1 <e <\phi (n) \]  
   e. Calculate private key d so
      \[ dxe = 1 \ (mod \ \phi (n)) \]
2. Encryption

\[ C = M^e \mod n \] (5)

3. Decryption

\[ M = C^d \mod n \] (6)

2.3 Block Cipher

In the Cipher block, bits of plaintext is divided into blocks of the same length as 64-bits. The block cipher encryption process scheme can generally be described as follows:

![Block Cipher Diagram]

Figure 4. Encryption-Decryption of Block Chiper

Suppose the plaintext block (P) of n bits

\[ P = (p_1, p_2, \ldots, p_n) \] (1)

The ciphertext block (C) then block C is

\[ C = (c_1, c_2, \ldots, c_n) \] (2)

Key (K) then key is

\[ K = (k_1, k_2, \ldots, k_n) \] (3)

So the Encryption process is

\[ E_k (P) = C \] (4)

The decryption process is

\[ D_k (C) = P \] (5)

2.4 Message Authentication

Authentication is related to the identification/recognition, both unity of the system and the information itself. Two parties who make communication with each other should introduce each other. Information transmitted over channels must be authenticated, data, the delivery time, and so on. Data authentication problems in this cryptographic process are of primary concern. The success of the cryptographic process is greatly influenced by prime numbers on the generation of RSA keys. If there is a discrepancy of the required parameters then the process of returning the code file to the original file will not work.

3. Research Methode

The research method to obtain information and data required in this paper are as follows:

a. Library study
   Conducted by reading books related to the problem of book lending.

b. Observation
   Conducted to collect data by way of direct observation on matters relating to the library.

c. Analysis some cases, with take issues related to the discussion.
4. Analysis And Discussion
Message encryption with RSA algorithm is done using mathematical calculations, either in the process of generate keys, encrypting messages, or text decryption. RSA algorithm is based on the concept of prime numbers, modulo arithmetic, and Euler's theorem. In summary, RSA algorithm consists of three parts, namely generate keys, encryption, and decryption.

An example of encryption-decrypting a message with an RSA algorithm is: if an A wants to send a message to user B, then the first time A must send his public key to user B. After that user B will encrypt messages sent using the public key B. Then the user B perform encryption by means of $C = M^e (\mod n)$. After that user A will receive the message $C$ and decryption by means of $M = C^d (n \mod)$. Noted that the message length of $M$ must be less than $n$.

1. Choose 2 different prime numbers
   $P = 61$ and $q = 53$
2. Calculate $n = pq$
   $N = 61 \times 53 = 3233$
3. Totient Calculate $\phi(n) = (p-1) (q-1) \Phi(n) = (61-1) (53-1) = 3120$
   $E = 17$
4. Select $d$ to satisfy $ed = 1 \mod \phi(n)$
   $D = 2753$
   $17 \times 2753 = 46801 = 1 + 15 \times 3120$
5. If $m = 123$, then the encryption process is: $C = 123^{17} (\mod 3233) = 855$
6. For the decryption process are:
   $M = 855^{2753} (\mod 3233) = 123$

Suppose the message (plaintext) to be sent is "HARI INI" or in the decimal system (ASCII encoding) is 7265827332737873.

How to encrypt it is:
1. Break the $m$ into smaller blocks, for example $m$ split into six blocs that are 3 digits:
   $M_1 = 726, M_2 = 582, M_3 = 733, M_4 = 273, M_5 = 787, M_6 = 003$
   These $m$ values are still located within the interval $[0, 3337-1]$ for the transformation to be one.
2. If the public key is $e = 79$ and $n = 3337$, then the plaintext blocks can be encrypted to be:
   $C_1 = 726^{79} (\mod 3337) = 215; C_2 = 582^{79} (\mod 3337) = 776; C_3 = 733^{79} (\mod 3337) = 1743; C_4 = 273^{79} (\mod 3337) = 933; C_5 = 787^{79} (\mod 3337) = 1731; C_6 = 003^{79} (\mod 3337) = 158$. So the resulting ciphertext is $c = 215 776 1743 933 1731 158$
3. Decryption is done using private key $d = 1019$. The ciphertext blocks are decrypted to be:
   $M_1 = 215^{1019} (\mod 3337) = 726$
   $M_2 = 776^{1019} (\mod 3337) = 582$
   $M_3 = 1743^{1019} (\mod 3337) = 733$
   $M_4 = 933^{1019} (\mod 3337) = 273$
   $M_5 = 1731^{1019} (\mod 3337) = 787$
   $M_6 = 158^{1019} (\mod 3337) = 003$
4. Finally recovered the original plaintext
   $M = 7265827332737873$, which in the ASCII encoding system is $M = "HARI INI"

From the example above it can be seen that the whole process of encryption and decryption with RSA algorithm using mathematical calculation, either from key generation process, until encryption and decryption of message. In order to be calculated, the text you wish to keep a secret must be converted into numeric form first. The results of the encryption is a cipher text which is also a series of numbers.
5. Conclusions
RSA algorithm is public key algorithm using prime number and even still used today. The strength of this algorithm lies in the exponential process, and the factorial number into 2 prime numbers which until now difficult to do factoring.

The RSA scheme itself adopts the block cipher scheme, where prior to encryption, the existing plaintext is divide in several block of the same length, where the plaintext and ciphertext are integers between 1 to n, where n is typically 1024 bit, and the block length itself is smaller or equal to log(n)+1 with base 2. With the combination of RSA algorithm and block chiper it is expected that the authentication of plaintext is secure.

References
[1] Akiwate, Bahubali & Desai, Vennai. 2013. Artificial Neural Networks for Cryptanalysis of DES. International Journal of Innovations in Engineering and Technology (IJIET). Vol. 2
[2] Ashioba, N. C. & Yoro, R. E., 2014. RSA Cryptosystem using Object-Oriented Modeling Technique. International Journal of Information and Communication Technology Research. Vol. 4(2): 57-61.
[3] Goyal, Kashish & Kinger Supriya. 2013. Modified Caesar Cipher for better Security. Enhancement. International Journal of Computer Applications (0975 – 8887). Vol.73(3).
[4] Shika Mathur, Deepika Gupta, Vishal Goar, Manoj Kuri, 2017. Analysis And Design of Enhanced RSA Algorithm to Improve The Security. International Conference of Computational Intelligence & Communication Technology (CICT). Vol. 3: 1-11.
[5] Upadhyay, Sachin., Singh, Yasphal., and Jain, Kumar, Amit. 2012. “An Analysis of the Attack on RSA Sryptosystem Trhough Formal Methods”. International Journal of Soft Computing and Engineering (IJSCE). Vol(2): 2231-2307.
[6] Yan, Y Song. 2007. Cryptanalytic Attack on RSA. Springer: University of Bedfordshire, UK.