Combination of Caesar Cipher Algorithm and Rivest Shamir Adleman Algorithm for Securing Document Files and Text Messages

Indra Gunawan¹, Sumarno¹, Heru Satria Tambunan¹, Eka Irawan¹, Hendry Qurniawan¹, Dedy Hartama¹

¹STIKOM Tunas Bangsa Pematangsiantar, Medan - Indonesia
*indra@amiktunasbangsa.ac.id

Abstract. At this time, the advancement technology of computer science and telecommunications are developed highly and progressing rapidly. Data security is very important to maintain the important data content of the parties that can harm by destroying important data from the data owner. By improving data security, using a combination of algorithms, it can keep data security more secure than attacks that can harm the content of stored data, especially data in the form of document files and text messaging. The combination of algorithms used for data security used is caesare cipher algorithm and RSA algorithm. So by using a combination of caesar cipher algorithm and RSA algorithm, the security level of document files and text messages can be more awake the authenticity of the data.

1. Introducing

The problem in data security is still an important aspect in maintaining data storage, especially data stored in digital form. This is caused by the rapid progress in of computer science with the concept of open-system that has been widely used, so it can facilitate someone to do data destruction, especially data stored in digital form without having to know by the data storage. Therefore, digital data management is required by combining 2 (two) algorithms, ie Caesare Cipher Algorithm and RSA Algorithm to increase the level of security of document files and text messages.

Caesar Cipher is one of the oldest algorithms and is one of the substitution cipher types that make up the cipher by shifting all characters on plaintext with the same shift value. The weakness of the Caesar Cipher is that we used to obtain the original message by using the brute force method and the presentation of letter frequencies that most frequent appear in a sentence [1]. Caesar cipher algorithm is an algorithm by replacing the initial letter position with alphabet or called ROT3 algorithm. Transposition algorithm that is by changing the location of text message to be encoded by using certain form[10].

From the other and many public key cryptography algorithms that ever-made, the most popular algorithm is the RSA algorithm. The RSA algorithm created by Ron Rivest, Adi Shamir and Leonard Adleman in 1976 [11]. The security of the RSA algorithm lies in the difficulty of factoring a relatively larger prime number. Factoring is done to obtain private key. As long as large prime factoring numbers have not yet been found the solved algorithm, so long as the RSA algorithm will still be assured its security [2].
Cryptography arises based on communicating and exchanging information/data remotely. Communication and data exchange between region and country or continent no longer becomes a significant constraint. Along with that the security demand for the confidentiality of interchangeable information is increasing. So many users such as the defense department, a company or even individuals do not want the information conveyed by other people or competitors or other countries. Therefore, it appears that branch of science that learn about the ways of securing data or known as Cryptography [9].

2. Methodology

2.1. Cryptography
Cryptography forms a system called a cryptographic system. The cryptographic system (Cryptosystem) is a collection of encryption and decryption functions corresponding to encryption and decryption keys [3]. According to Katz, cryptography is a scientific or technical study for securing digital information, transactions and distributed computing [4]. Cryptography aims to provide security services [5].

2.2. Caesar Cipher
The first substitution in the world of data security was in the reign of Julius Caesar, so it was declared by the name of Caesar Cipher, which replaced the initial letter position of alphabet [6], caesar cipher also known as Shift Cipher.

\[
c = e(p) = (p+k) \mod 26 \ldots (1)
\]

Where \( \mod 26 \) is the number of alphabets. Equation 1 is used for the encryption process.

\[
p = d(c) = (c-k) \mod 26, \text{ (if } c-k \text{ is negative, then add 26). } \ldots (2)
\]

Where, if the result of \( c-k \) is a negative value, \( \mod 26 \) does not apply, but the result of the negative value is directly summed by 26. Equation 2 is used for the decryption process.

2.3. Algorithm of RSA
RSA is one of the Public Key Cryptosystems that often used to provide confidentiality to the authenticity of a digital data. The encryption and decryption security of this model lies in the difficulty of factoring the enormous modulus \( n \) [7].

RSA is still used extensively in electronic commerce protocols and is believed to be very secure because of its long locks and sophisticated applications [8].

2.4. Combination of Caesar Cipher and RSA Algorithm
Combination of Caesar Cipher and RSA algorithm aim to overcome the weakness of Caesar Cipher. Because the caesar cipher works only by shifting characters, it is possible to be solved by using brute
force. The Brute Force Method that most commonly used is to use the statistics of the frequency of the occurrence letters which most often appears. Example: They get the WORD message. Because the letter that most often appears is the letter A, then the shift from the letter A to the letter P which only has the frequency of occurrence 2 times, then change the letter A with the letter P, then slide back the remaining messages. Combination of caesar cipher with RSA algorithm works by encrypting the message first with caesar cipher, then the message result (ciphertext) encrypted again using RSA algorithm, so the pattern of statistical of the message can not be detected.

2.5. Calculation Combination of caesar cipher and rsa algorithm

From the theoretical base already discussed, to encrypt a data using a combination of caesar cipher and RSA algorithm, it takes several sample numbers to hold the characters, eg (c, k and p). One number is used as the object shift key (k), and two remaining are used for encryption. Example: there is a plaintext STIKOM message with a key k = 20, by mapping the alphabet A = 0 to Z = 25.

Step 1: do mapping between encryption process and plaintext, then result in modulus with 26, then result will be obtained by MNCEIG (Caesar Cipher).

Step 2: The ciphertexts that have been obtained (MNCEIG) are re-encrypted by determining the larger prime factor. Unlike the Caesar Cipher that uses only alphabetic characters, the RSA algorithm uses all types of characters.

The process of returning the message (decryption) is as follows

Step 1: decrypt the RSA algorithm, so it will generate encrypted messages to be processed in the Caesar Cipher.

Step 2 : the result of decryption with RSA algorithm will be decrypted back using Caesar Cipher, by using decryption mapping to cipher. The alphabet mapping still same, ie A = 0 to Z = 25 with the same key k = 20. So if the letter M in alphabetical order is 12, then (12-20) mod 26, since 12-20 produces a negative number (-8) then the modulus can be ignored and the number (-8) can be directly summed by 26, then the result is 18, and in alphabetical order 18 is the letter S. So ciphertexts MNCEIG after decrypted will generate STIKOM.

2.6. Pseudocode Caesar Cipher and RSA Algorithm

Pseudocode used to perform encryption and decryption with caesar cipher are:

Caesar Cipher Encryption Process
For i:=1 to lenght (s) do
Begin
C:=ord(upcase(s[i]))+indice;
If c>90 then c:=c-26;
S[i]:=chr(c);
End;

Caesar Cipher Encryption Process
For i:=1 to lenght (s) do
Begin
C:=ord(upcase(s[i])-indice;
If c<65 then c:=c+26;
S[i]:=chr(c);
End;

The RSA_scheme adopts the block of cipher_scheme itself, where prior to encryption, the existing plaintext is divided into blocks of the same length, where the plaintext and ciphertext are integers between 1 until n, where n has a size of 1024 bit, and the block length itself is smaller or equal to log (n) +1 with base 2. The encryption and decryption functions are described in the following functions:

c = m^e \mod n \ldots \text{(encryption function)}
m = c^d \mod n \ldots \text{(decryption function)}
c = \text{Ciphertexts}
\[ m = \text{Message / Plaintext} \]
\[ e = \text{public key} \]
\[ d = \text{private key} \]
\[ n = \text{modulo divider} \]

Both parties must know the value of e and value of this n, and one of the parties must have d to decrypt the encryption results by using public key e. The use of this algorithm must meet the following criteria:

- It is possible to find the value of e, d, n such that \( Med \mod n = M \) for all \( M < n \).
- It is relatively easy to calculate the value of \( Me \mod n \) and \( Cd \mod n \) for all values of \( M < n \).
- It is impossible to find d if given the value of n and e. The terms of this e and d, \( \gcd(d, e) = 1 \)

Before starting the use of this RSA, we must first have the following basic materials:

- p, q = 2 undefined primes
- n, from the result p.q
- e, with the provisions of \( \gcd(\Phi(n), e) = 1 \)
- d, e \(-1 \mod \Phi(n)\)

Example:

a. Choose 2 prime numbers, for example p = 17 and q = 11.
b. Calculate from n = pq = 17 \times 11 = 187.
c. Calculate from \( \Phi(n) = (p-1) \times (q-1) = 16 \times 10 = 160. \)
d. Select of the value e such that the relative of prime number to \( \Phi(n) = 160 \) and less than \( \Phi(n) \); we select e = 7.
e. Calculate d such that de \(-1 \mod 160\) and d < 160. The value obtained d = 23, because 23 \times 7 = 161 = (1 \times 160) + 1; d can be calculated with Extended Euclidean_AlgGORITHM.

Well, the value of e and d is what we call the Public Key (e) and Private Key (d). Couple Public Key = \{7, 187\} and Private Key = \{23, 187\}

Encryption Process:

Suppose we have M 88. For encryption process, we will calculate \[ c = 88^7 \mod 187. \]
\[ = 88^7 \mod 187 = 894,432 \mod 187 = 11. \] We get the value of C = 11.

Decryption Process:

Furthermore, this C value is sent to the recipient to be decrypted with his private key.
\[ M = Cd \mod n = 11^{23} \mod 187 = 79,720,245 \mod 187 = 88 \]

3. Results and Discussion

In this process will be generated how the steps for securing document files and messages. The document file to be secured first will be selected and then inserted a text message into the selected document file, then the document file containing the secret message will be given a key security before the document file that already contains a text message sent to the recipient.

---

**Figure 2.** The initial view of the application
In the first stage, the sender will select a document file to be inserted by a text message. The selected document file can be pdf, doc, docx, jpg, mpg.

**Figure 3.** The selection of document file to be inserted text message

Next insert a text message into the selected document file. In this case, the text message will be encrypted first using RSA algorithm and then inserted into the document file.

**Figure 4.** The Process of Insertion and Describing Text Messages

It then delivers the keywords into the encoding of text messages and document files to keep security of document files and text messages.

**Figure 5.** Keyword Giving Process

**Figure 6.** Result of Encrypted Document Files
4. Conclusion
The combination of Caesar Cipher and RSA algorithm can help improve data, when compared to using only one method. Using calculations with alphabetic structures and incorporating them by using prime numbers can improve the data security system, so that the stored data will be more awake.

References
[1] Rachmawati, Dian & Candra, Ade. 2015. Implementation of the combination of Caesar Cipher and Affine Cipher for text data security. Informatics Research and Education Journal (JEPIN), No. 2, Vol. 1
[2] Alvianto & Darmaji. 2015. Secure message delivery via SMS with the Android-based RSA Algorithm. Sains Journal and Seni ITS, No. 1, Vol. 4.
[3] Mollin. 2007. An Introduction to Cryptography. 2nd Edition. Chapman & Hall/CRC : Boca Raton, Florida.
[4] Katz & Lindell 2007. Introduction to Modern Cryptography. Chapman & Hall/CRC : United States.
[5] Paar, C. & Pelzl, J. 2010. Understanding Cryptography. Springer-Verlag: Berlin.
[6] Ariyus, D. 2008. Introduction to Cryptography: Theory, analysis and implementation. Andi: Yogyakarta.
[7] Mollin, R. A. 2007. An Introduction to Cryptography. 2nd Edition. By Tailor & Francis Group, London, New York.
[8] Zainal Arifin. 2009. Case Study: Use of the RSA Algorithm as a secure cryptographic algorithm. Samarinda.
[9] Delliana, 2014. Implementation of Hill Cipher Cryptography Algorithm in Encoding Image Data. Informatika Journal Budi Darma, Vol : VII, No. 2.
[10] Basuki, Paranita, Hidayat, 2016. Design of Layered Cryptography Applications Using Caesar Algorithms, Transpositions, Vigenere and Block Cipers Based on Mobile. National Seminar on Information and Multimedia Technology. STMIK AMIKOM Yogyakarta.
[11] Gunawan, I., Sumarno, S., Tambunan, H.S., 2018. The Function of the RSA Algorithm to Modify and Improve the Random Security of BISS. Journal of Computer Engineering, System and Science (CESS), Vol. 3, No. 2, Juli 2018.