Formosa Journal of Science and Technology (FJST)
Vol. 2, No. 1, 2023: 379-388

Implementation of the RSA Algorithm and the One Time Pad Algorithm for Text Message Security

Zulfahmi Indra[1]*, Rinjani Cyra Nabila[2]
Computer Science Study Program, Universitas Negeri Medan
Corresponding Author: Zulfahmi Indra zulfahmi.indra@unimed.ac.id

A R T I C L E I N F O

Keywords: Data Security, RSA Algorithm, One Time Pad Algorithm

Received : 03, December
Revised : 28, December
Accepted: 25, January

A B S T R A C T

Securing data is one of the things that is very important to protect the contents of the data from parties who can harm it by destroying important data from the owner. This study applies two algorithms, namely the RSA algorithm and the One Time Pad algorithm. First use the RSA algorithm first with predetermined plaintext. After finishing working on the RSA algorithm, then continue working on the same plaintext as the One Time Pad algorithm. The results of the study show that the application of the RSA and One Tome Pad algorithms, the level of security of document files and text messages can be better maintained for the authenticity of the data. So that data leakage can be minimized.

DOI: https://doi.org/10.55927/fjst.v2i1.2999
ISSN-E: 2964-6804
https://journal.formosapublisher.org/index.php/fjst

INTRODUCTION

One of the media to communicate is the media of writing. Writing serves to convey messages. Messages contained in writing may or may not contain confidential information. Confidential information can be kept confidential if it is conveyed by the sender of the message directly to the recipient of the message (Jafarudin Firdaus and Gozali 2018).

To avoid the possibility of intercepted data being directly read by eavesdroppers, the data sent is scrambled using a certain encoding method so that the messages contained in the data sent are more secure. However, only by encoding the message, it does not rule out the possibility of the message being modified by a third party.

Wiretapping cases have existed about 100 years ago. One example of a well-known wiretapping case is the case reported in 1867 by a Wall Street stockbroker working with Western Union to wiretapping telegraph operators sent to newspapers in the Middle East and then replacing the telegraph messages with fake ones (Alvianto and Darmaji 2015).

The advancement of information systems has many advantages in human life, but it also has negative aspects such as fraud, theft and so on. The fall of information into the hands of unauthorized parties can cause harm to the owner of the information, so the confidentiality aspect is required in the delivery process. One aspect of confidentiality that can be done is to encode the information into codes that cannot be understood.

Network security is one of the most important things in implementing a computer network. Computer networks caused by someone's negligence create opportunities for criminals to damage the network that is built. Therefore it is necessary to increase network security to be built (Amarudin, 2018). Own safety is very important. There are several reasons why security is very important, the first is to prevent potential material losses. The second is to reduce the risk of data/information misuse. The latter is to minimize the opportunity for criminal acts. The security benefits include:

1. Protect All Valuable Information,
2. Maintain reputation,
3. Marketing (marketing) competitive advantage
4. Save on development and support costs.

The science used to maintain the confidentiality of information is called cryptography. The importance of securing data using cryptography is because cryptography aims to maintain the confidentiality of the information contained in the data so that this information cannot be known by unauthorized parties. In maintaining data confidentiality, cryptography transforms clear data (plaintext) into unrecognizable ciphertext data. This ciphertext is then sent by the sender to the receiver. After arriving at the recipient, the ciphertext is transformed back into plaintext so that it can be recognized.

Cryptography is used in securing data because cryptography already fulfills four aspects of information security, namely aspects of Confidentiality, Data Integrity aspects, Authentication aspects and Non-Repudiation aspects. Implementation of the use of cryptography in everyday life is usually like

transactions via ATMs, Pay TV and E-commerce transactions (Hidayatullah and Insannudin 2016). Cryptography has long been used by the Spartan army in Greece as early as 400 BC (Apdilah and Swanda 2018). Cryptographic techniques are believed to be able to handle data or information security problems, because apart from using computer programming languages, cryptography also uses mathematical formulas, ranging from simple formulas to complex formulas (Hidayat and Faizin 2019).

Cryptography aims so that information that is confidential and sent through a network, such as a Local Area Network (LAN) or the internet, cannot be known and used by other people or unauthorized parties (Arief & Saputra, 2016). There are three fundamental objectives of this cryptographic science which are also aspects of information security namely: 1) Confidentiality, is a service aimed at keeping messages from being read by unauthorized parties; 2) Data integrity, is a service that guarantees the message is genuine/intact or has never been manipulated during delivery. Communicating is doing denial, that is, the sender of the message denies sending or receiving the message denies having received it (Munir, 2006); 3) Authentication is the verification of whether a person is an authorized person. Usually involves a username and password, but can include other methods of establishing identity, such as smart cards, fingerprints.

With the development of today's technology, it will be easier for everyone to obtain information or data. If the data or information obtained is not protected, it will be easy for other people to find out the data and information they have. Various ways were done to protect the data or information.

Many algorithms can be used to secure data, one of which is the RSA algorithm and the One Time Pad algorithm. The One Time Pad algorithm model is similar to the Caesar Chiper, which is a simple substitution-based classical coding system. The Caesar Ciper cipher system uses a shift operation. The shift operation is an encoding operation by substituting a letter into a letter in the alphabetical list k (Sutoyo & Murhaban, 2016).

There is also an example of a reliable cryptographic algorithm, namely RSA, where RSA is an asymmetric key encoding process (Ginting et al., 2015). The RSA algorithm is one of the most popular modern asymmetric cryptographic algorithms. This algorithm performs factoring of very large numbers, so this is the reason why RSA is considered a safe algorithm.

THEORETICAL REVIEW

Cryptography

In general, cryptography is the science and art of keeping news confidential (Bruce Schneire Applied Cryptography). In addition to these definitions, the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity and authentication (Munir, 2006). Cryptography is the science of protecting data transmission by converting it into a certain code and is only intended for people who only have a key to change the code back which functions in maintaining the confidentiality of data or messages. In

cryptography, data or messages sent over the network will be disguised in such a way (Pabokory et al., 2016). The following are terms used in the field of cryptography: 1) Plaintext (M) is a message to be sent (containing original data) that can be understood; 2) Ciphertext (C) is the encrypted (encoded) message which is the result of encryption; 3) Encryption (E) is the process of converting plaintext into ciphertext. The use of data encryption as a prevention against threats in data theft is very important and system damage, and is used to change data so that it cannot be read by unauthorized persons; 4) Decryption (D) is the opposite of encryption, namely changing the ciphertext into plaintext, so that it is the initial/original data; 5) The key (K) is an undisclosed number that is used in the encryption and decryption process (Azis, 2018).

RSA Algorithm

The RSA algorithm is an algorithm that lies in the difficulty of factoring relatively large prime numbers. This factoring is done to obtain the private key. As long as the factoring of large prime numbers has not yet found an algorithm that can solve it, then the safety of the RSA algorithm is guaranteed. RSA is an algorithm that is often used to provide confidentiality for the authenticity of digital data (Pabokory et al., 2016).

RSA is a public key cryptographic algorithm (asymmetric). First discovered in 1977 by Ron Rivest, Adi Shamir, and Len Adleman. The name RSA itself is taken from the three founders. As a public key algorithm, RSA has two keys, namely the public key and the secret key. RSA bases its encryption and description processes on the concepts of prime numbers and modulo arithmetic. Both the encryption key and the description are integers. The encryption key is not kept secret and is given to the public (so it is called a public key), but the key for decryption is secret (private key) (Ginting et al. 2015).

RSA is an algorithm for public key encryption. This algorithm was the first algorithm known to be most suitable for signing and for encryption and one of the first major discoveries in public-key cryptography. RSA is still widely used in electronic commerce protocols and is believed to be very secure because it is given long enough keys and very up-to-date applications (Zainal. 2009).

The RSA algorithm was chosen because its security lies in the difficulty of factoring prime numbers, the greater the number of primes in key generation, the more difficult it is to solve (Nagar & Alshamma. 2012). Factoring is done to obtain the key to open encrypted messages. As long as prime number factoring has not been discovered and there is no algorithm that can solve prime number factoring, the safety of the RSA algorithm will still be guaranteed (Zhao et al. 2010).

Algorithm One Time Pad

The One Time Pad (OTP) algorithm is a stream cipher that performs encryption and description one character at a time. This algorithm is an improvement over the Vernam cipher to produce perfect security. This cipher belongs to the group of symmetric cryptographic algorithms. One Time Pad (pad=paper pad) contains a sequence of randomly generated key characters. Originally, a One Time Pad is a tape (tape) that contains a row of key characters.

One pad is only used once (one time) to encrypt a message, after which the pad that has been used is destroyed so that it is not used again to encrypt other messages.

The encryption process can be expressed as the sum modulo 256 of one plaintext character with one One Time Pad key character:

Equation 2.1

$$Ci = (Pi + Ki) \bmod 256$$

Information:
Ci = Ciphertext Character
PI = Plaintext Character
Ki = Key Character

While the decryption process uses the same pad to describe the ciphertext into plaintext:

Equation 2.2

$$Ci = (Pi - Ki) \bmod 256$$

Encryption Process

The Encryption Process is:

1. Determine plaintext and convert plaintext into integers based on ASCII code
2. Determine a random key with the same key length as the plaintext to be encrypted.
3. Carry out the calculation process using equation 2.1.
4. After the encryption process is carried out, the ciphertext is obtained

Decryption Process

The process of decryption is:

1. Changing ciphertext into integer form.
2. Using the same key in the encryption process.
3. Carry out the calculation process using equation 2.2.
4. Plaintext is generated.

METHODOLOGY

In securing a text message, this study applies two algorithms, namely the RSA algorithm and the One Time Pad algorithm. first use the RSA algorithm first with predetermined plaintext. After finishing working on the RSA algorithm, then continue working on the same plaintext as the One Time Pad algorithm.

Application of the RSA Algorithm

1. Step 1: converting the specified plaintext into ascii, after that it is immediately broken into a block called m.
2. Step 2: do the mapping between the encryption process and the plaintext in each RSA algorithm and the One Time Pad algorithm. From here get the results of the encryption.
3. Step 3: carry out the description process using the private key that has been obtained, after that get the plaintext M value.

Implementation of the One Time Pad Algorithm
In this algorithm we use the same plaintext example, namely:
Plaintex: Adv Security
using key 01.
Key: 01
Converting plaintext to ASCII:
Determines plaintext and converts plaintext into integers based on ASCII code
Carry out the Encryption Process, namely:

1. Determine a random key with the same key length as the plaintext to be encrypted.
2. Perform the calculation process using the equation Ci = (Pi + Ki) mod 256
3. After the encryption process is carried out, the ciphertext is obtained

RESULTS

Application of the RSA Algorithm

In this study using the magnitudes that lie in the RSA algorithm, namely:

1. p and q prime numbers (secret)
2. n = p · q (not secret)
3. ϕ (r) = (p – 1)(q – 1) (secret)
4. PK (encryption key) (unsecret)
5. SK (decryption key) (secret)
6. X (plaintext) (secret)
7. Y (ciphertext) (not secret) (Ginting et al., 2015)

Key formation algorithm:

1. Determine that p and q are two large prime numbers, random and undisclosed, p ≠ q, p and q have the same size.
2. Calculate n = p x q, and calculate ϕ(n) = (p – 1) x (q – 1), the integer n is called (RSA) modulus.
3. Find e a random prime number that has the following conditions: 1 < e < 1(n), GCD(e, i(n)) = 1, called e relatively prime to i(n), an integer n called (RSA) enciphering component, resulting in Dd (Ee(m)) = Ee(Dd(c)) ≡ md mod n (Gunawan, 2018).

As an example given the plaintext "Adv Security", by selecting p = 47 and q = 71. From this example we get n = p × q = 3337, ϕ(n) = (p – 1)×(q – 1) = 3220. Then choose public key e = 79 (which is relatively prime with 3220 because the biggest common divisor is 1). By trying the values of k = 1, 2, 3, …, the rounded value of d is 1019 . This is the private key (for decryption).

RSA algorithm examples and solutions:
Plain text : Adv Security
In ASCII : 65 100 118 83 101 99 117 114 105 116 121
Break M into blocks that are 3 digits long

m1 = 651 m2 = 001

m3 = 188 m4 = 310

m5 = 199 m6 = 117

m7= 114 m8 = 105

m9 = 116 m10 = 121

(Note, mi still lies between 0 to n – 1 = 3337). Encrypt each block :

Encryption process:

$c_1 = 651^{79} \bmod 3337 = 1754$

$c_2 = 001^{79} \bmod 3337 = 1$

$c_3 = 188^{79} \bmod 3337 = 940$

$c_4 = 310^{79} \bmod 3337 = 2448$

$c_5 = 199^{79} \bmod 3337 = 5$

$c_6 = 117^{79} \bmod 3337 = 2289$

$c_7 = 114^{79} \bmod 3337 = 2560$

$c_8 = 105^{79} \bmod 3337 = 193$

$c_9 = 116^{79} \bmod 3337 = 1031$

$c_{10} = 121^{79} \bmod 3337 = 2798$

Result C = 1754 1 940 2448 5 2289 2560 193 1031 2798

Process description

Decrypt (using private key d=1019)

$m_1 = 1754^{1019} \bmod 3337 = 651$

$m_2 = 1^{1019} \bmod 3337 = 1$

$m_3 = 940^{1019} \bmod 3337 = 188$

$m_4 = 2448^{1019} \bmod 3337 = 310$

$m_5 = 5^{1019} \bmod 3337 = 199$

$m_6 = 2289^{1019}$ mod 3337 = 117

$m_7 = 2560^{1019}$ mod 3337 = 114

$m_8 = 193^{1019}$ mod 3337 = 105

$m_9 = 1031^{1019}$ mod 3337 = 116

$m_6 = 2798^{1019}$ mod 3337 = 121

Plainteks M = 651118831019911711410511612 1
Plaintext becomes:
651 001 188 310 199 117 114 105 116 121

Implementation of the One Time Pad Algorithm

Convert Plaintext to ASCII

Table 1. Plaintext Data Conversion into ASCII Form

A	D	v	S	e	C	u	r	i	T	y
65	100	118	83	101	99	117	114	105	116	121

Carrying out the Encryption Process, namely:

1. Determine plaintext and convert plaintext into integers based on ASCII code
2. Determine a random key with the same key length as the plaintext to be encrypted.
3. Perform the calculation process using the equation Ci = (Pi + Ki) mod 256
4. After the encryption process is carried out, the ciphertext is obtained

A = (65 + 01) mod 256 = 66

d = (100 +01) mod 256 = 101

v = (118 + 01) mod 256 = 119

S = (83 + 01) mod 256 = 84

e = (101 + 01) mod 256 = 102

c = (99 + 01) mod 256 = 100

u = (117 + 01) mod 256 = 118

r = (114 + 01) mod 256 = 115

i = (105 + 01) mod 256 = 106

t = (116 + 01) mod 256 = 117

y = (121 + 01) mod 256 = 122

Generate Ciphertext:

Table 2. Ciphertext Results

66	101	119	84	102	100	118	115	106	117	122
B	e	w	T	f	C	v	s	j	U	z

CONCLUSIONS AND RECOMMENDATIONS

The application of the RSA algorithm and the One Time Pad algorithm can help in securing text messages, when compared to only using two text methods it will be more overcome. Using calculations with the alphabetic structure in the One Time Pad algorithm and combined with using prime number factoring in RSA can make the text message security system safer and more secure. The encoding process with the RSA algorithm and the One Time Pad algorithm has been successfully used to hide messages and can restore the message to its original state. The One Time Pad algorithm is a simple but very secure algorithm because the key is only used once, and after that. Therefore, it takes a key that is the same length as the plaintext so that the longer the plaintext, the longer the key.

ADVANCED RESEARCH

Based on the implementation of the One Time Pad algorithm above, it is known that this algorithm is sufficient to fulfill the confidentiality aspect as one of the objectives of implementing cryptographic algorithms. This is because the encrypted message turns into another message that the eavesdropper cannot immediately understand because the shape is no longer the same as the original message. This algorithm is also still quite secure because the key used for each character is only used in the encryption process once. However, the implementation of this algorithm raises the key distribution problem. Where the key must be sent through a medium that is completely safe from eavesdropping and may not use the same delivery medium as sending ciphertext. Because if the media is tapped, the eavesdropper immediately has both the ciphertext and the key, so it is very easy for him to carry out the decryption process using the decryption equation.

REFERENCES

Alvianto, A. R., dan Darmaji (2015): Pengaman Pengiriman Pesan Via SMS Dengan Algoritma RSA Berbasis Android, *Jurnal Sains dan Seni ITS*, **4**(1), 1– 6.

Amarudin. (2018). Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking. *Jurnal Teknoinfo*, *12*(2), 72. https://doi.org/10.33365/jti.v12i2.121

Apdilah, D., dan Swanda, H., (2018): Penerapan Kriptografi RSA Dalam Menga-

mankan File Teks Berbasis PHP, *Jurnal Teknologi Informasi*, **2**(1), 45–52.

Arief, A., & Saputra, R. (2016). Implementasi Kriptografi Kunci Publik dengan Algoritma RSA-CRT pada Aplikasi Instant Messaging. *Scientific Journal of Informatics*, *3*(1), 46–54. https://doi.org/10.15294/sji.v3i1.6115

Azis, N. (2018). Perancangan Aplikasi Enkripsi Dekripsi Menggunakan Metode Caesar Chiper dan Operasi XOR. *Ikraith-Informatika*, *2*(1), 72–80.

Ginting, A., Isnanto, R. R., & Windasari, I. P. (2015). 144706-ID-implementasi-algoritma-kriptografi-rsa-u. *Jurnal Teknologi Dan Sistem Komputer*, *3*(2), 253–258. https://media.neliti.com/media/publications/144706-ID-implementasi-algoritma-kriptografi-rsa-u.pdf

Gunawan, I. (2018). Kombinasi Algoritma Caesar Cipher dan Algoritma RSA untuk pengamanan File Dokumen dan Pesan Teks. *InfoTekJar (Jurnal Nasional Informatika Dan Teknologi Jaringan)*, *2*(2), 124–129. https://doi.org/10.30743/infotekjar.v2i2.266

Hidayat, A., dan Faizin, A., (2019): Perbandingan Kriptografi Menggunakan Algoritma Data *Encryption Standart*(DES)dan Algoritma *Rivest Shamir Adleman*(RSA)Untuk Keamanan Data, *JASIEK*, **1**(2), 143 – 148.

Hidayatullah, A., dan Insannudin, E., (2016): Pengenalan Kriptografi dan Pemakaiannya Sehari-hari, *JurnalPengenalan Kriptografi dan Pemakaiannya Sehari- hari*, 1–6.

Jafarudin Firdaus, R. M., dan Gozali, S. M., (2018): Penyandian Pesan Menggu- nakan Kombinasi Algoritma RSA Yang Ditingkatkan dan Algoritma Elgamal, *Jurnal EurekaMatika*, **6**(1), 23–32.

Munir, R. (2006). Pengantar Kriptografi. *Bahan Kuliah IF4020*.

Nagar, S. A., & Alshamma, S. (2012). High Speed Implementation of RSA Algorithm with Modified Keys Exchange. 6th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), 639-642

Pabokory, F. N., Astuti, I. F., & Kridalaksana, A. H. (2016). Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard. *Informatika Mulawarman : Jurnal Ilmiah Ilmu Komputer*, *10*(1), 20. https://doi.org/10.30872/jim.v10i1.23

Sutoyo, M. N., & Murhaban. (2016). Kombinasi Algoritma Kriptografi Caesar Chiper dan Vigenere Chiper Untuk Keamanan Data. *Jurnal Mekanova*, *2*(2), 58–66.

Zainal Arifin. 2009. Studi Kasus : Penggunaan Algoritma RSA sebagai algoritma kriptografi yang aman. Samarinda.

Zhao, G., Yang, X., Zhou, B., & Wei, W. (2010). RSABased Digital Image Encryption Algorithm In Wireless Sensor Networks. 2nd International Conference on Signal Processing Systems ICSPS), 640-643.