Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 3, Juli 2023
DOI : https://doi.org/10.33395/sinkron.v8i3.12467
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Hybrid Cryptosystem Analysis RSA Algorithm And Triple DES Algorithm

Liana[1)*], Muhammad Zarlis[2)], Tulus[3)]
[1)] Student of Computer Science, University of North Sumatra, Medan, Indonesia,
[2)]Department of Computer Science, University of North Sumatera, Medan, Indonesia,
[3)]Department of Mathematic, University of North Sumatra, Medan, Indonesia
[1)]lianabangun@gmail.com,[2)] m.zarlis@yahoo.com,[3)] tulus@usu.ac.id

Submitted : May 27, 2023 | **Accepted** : Jun 19, 2023 | **Published** : Jul 1, 2023

Abstract: Data security is needed in terms of communication. To guarantee data security, a technique is needed to make data and information called Critography. This study aims to analyze the process of Super Encryption in symmetric and asymmetric criterias using the Triple DES Algorithm and the RSA Algorithm. This can improve data security so that data is more confidential. The method used in Triple DES which is also called the symmetric algorithm is the OFB (Output feeback) method, and the RSA Algorithm (Riverst - Shamir-Adleman) which is an asymmetric algorithm using a random number system so that when these two algorithms are combined in the Super Encryption process the more accurate the data security. Super DES Triple Encryption and RSA algorithm analysis shows that the data created by text will be encrypted into ciphertext using both methods and re-described, so that the security of the data is relatively safe. Super Encryption on the two methods Algorithm is done because the level of complexity is difficult to make Cryptanalysts to steal data and the Encryption process becomes slow but data security becomes safer and not easy to attack Cryptanalysts. The problem in this research is how to increase encryption security and speed up the encryption process by combining the RSA and Triple DES methods.

Keywords: Super Encryption Algorithm Triple DES, RSA Algorithm

INTRODUCTION

In cryptography there are several algorithms that can encode data. In the proposed hybrid encryption algorithm, Triple DES Algorithm is used for data transmission due to higher efficiency in block encryption, and RSA algorithm is used for Triple DES key encryption due to more accurate gain management in cipher keys. (Kakarla & Govind, 2012). Based on the keys used for encryption and decryption, cryptography can be divided into symmetric-key cryptography and asymmetric-key cryptography. RSA Algorithm (Rivest Shamir Adleman)

is a method in a branch of science cryptography, where RSA is a type of cryptography asymmetric which uses 2 keys, namely the key public and private. RSA cryptographic algorithm designed according to its function so that the key used for encryption that is different from that key used for description. The key for message encryption called public, while the key to decrypt. The security of the RSA algorithm lies in its difficulty

Factoring large numbers into factors prime. Factoring is done to obtain private key. During factoring large numbers prime factors have not yet been discovered efficient algorithm, so long as it is the safety of the RSA algorithm is guaranteed (Sadikin, 2012 : 249).

The received message is called private. So there is an effort to combine the two types of cryptography so as to produce a high level of security in the encryption and decryption process which

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 3, Juli 2023 e-ISSN : 2541-2019
DOI : https://doi.org/10.33395/sinkron.v8i3.12467 p-ISSN : 2541-044X

is known as the hybrid cryptosystem method. RSA (Rivest-Shamir-Adleman) is an algorithm that processes encryption and decryption on the concept of prime numbers and modulo arithmetic. OK lock

both 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).

The private key is generated from several prime numbers together with the encryption key. To find the decryption key, one must factor a non-prime number into its prime factor. In fact, factoring non-prime numbers into their prime factors is not an easy job. No effective (efficient) algorithm has yet been found for that factoring. The larger the non-prime number, the more difficult the factoring will be. The more difficult the factoring is, the more robust the RSA algorithm is.

Hybrid cryptosystem is a combination of cryptosystems that use asymmetric cryptosystems and cryptosystems that use asymmetric cryptosystems. (Schneier, 1996). In using the hybrid algorithm, the encryption technique used is symmetric and asymmetric encryption where the decryption key is the same as the encryption key. For public key cryptography, symmetric and asymmetric encryption techniques are needed where the decryption key is not the same as the encryption key.

Based on the description above, the authors are interested in conducting research by analyzing the RSA Algorithm and the Triple DES Algorithm with the cryptosystem hybrid method. The RSA algorithm is an example of Public Key cryptography and the Triple DES Algorithm, which is Symmetric and asymmetric cryptography that uses symmetric and asymmetric encryption.

LITERATURE REVIEW

Cryptography is a technique for securing and sending data in a form that is only known by those who open it, so as to secure important information both stored in storage media and transmitted via communication networks. (Ariyus, 2008). Cryptography is the process of using various techniques and/or science and art to keep messages secure. Cryptography is the science of encryption techniques where data is scrambled using an encryption key into something that is difficult to read by someone who does not have a description key. The description uses the decryption key to get the original data. The encryption process is carried out using an algorithm with several parameters. Usually the algorithm is not kept secret, even encryption that relies on the secrecy of the algorithm is considered something that is not good. The secret lies in some of the parameters used, so the key is determined by the parameters. It is the parameter that determines the decryption key that must be kept secret (the parameter being the equivalent of the key). In classical cryptography, the encryption technique used is symmetric encryption where the description key is the same as the encryption key. (Kromodimoeljo, 2010).

Cryptography (cryptography) comes from the Greek: "cryptos" which means "secret" (secret) and "graphein" which means "writing" (writing). So Cryptography is the science and art of keeping messages secure. Cryptography is a science that studies mathematical techniques related to aspects of information security such as confidentiality, data integrity, and authentication. The word "art" in the definition above comes from the historical fact that in the early days of cryptographic history, everyone might have a unique way to keep messages secret. These unique ways are different for each cryptographer so that every way of writing secret messages, messages have their own aesthetic value so that cryptography develops into an art of keeping messages secret. Cryptography has a very interesting and long history. Cryptography was used more than 4000 years ago, introduced by the Egyptians through hieroglyphs.

This type of writing is not a standard form for writing messages. Narrated in ancient Roman times, one day Julius Caesar wanted to send a secret message to a general on the battlefield. The message must be sent by a courier. Because the message contained a secret, Julius Caesar did not want the secret message to be exposed on the street. Julius Caesar then thought about how to deal with it. Then scrambled the message until it became a message that could not be understood by anyone except the General. Of course, the General had been told beforehand how to read the scrambled messages. What Julius Caesar did was change all the alphabetical arrangements from a, b, c, namely a to b, b to c and c to d and so on until the sentence could not be read by anyone.

In another sense, cryptography is the art and science of securing messages. In the world of cryptography, messages are called plaintext or cleartext. The process of disguising messages in such a way as to hide their original content is called encryption. Messages that have been encrypted are called ciphertext. The process of returning a ciphertext to plaintext is called decryption.

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 3, Juli 2023 e-ISSN : 2541-2019
DOI : https://doi.org/10.33395/sinkron.v8i3.12467 p-ISSN : 2541-044X

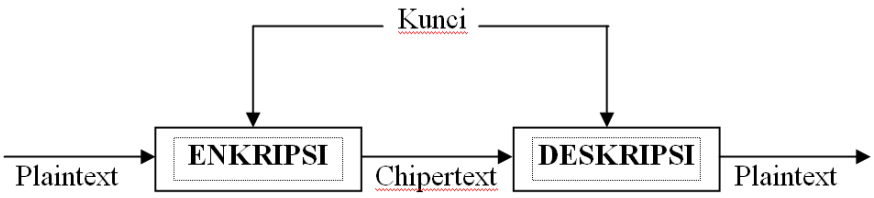


Figure 1: Basic Concepts of Encryption and Decryption

Cryptography Concept

The concept of cryptography itself has long been used by humans, for example in the Egyptian and Roman civilizations, although it is still very simple. The principles underlying cryptography are:

a. Confidentiality is a service that is intended to ensure that the contents of messages sent cannot be read by other parties (except the sender, recipient / parties who have permission). Generally this is done by encoding the message into ciphertext so that it is difficult to read and understand. For example: "LEARN CRYPTOGRAPHY" is encoded as "67652502491243237408713336866557291792646692433 4". So that the message cannot be understood by other parties, the message needs to be encoded in another form that cannot be understood. The form of the encoded message is called a ciphertext or often also called a cryptogram. Ciphertext must be able to be transformed back into the original plaintext so that the received message can be read.

b. Data integrity (data integrity), namely services that are able to guarantee that messages are original/intact or have not been manipulated during the delivery period. To maintain data integrity, the system must have the ability to detect manipulation of the message by unauthorized parties, including deleting, changing or adding unauthorized data by other parties.

c. Authentication (otentikasi) yaitu layanan yang berhubungan dengan identifikasi. Baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi maupun mengidentifikasi kebenaran sumber pesan. Dua pihak yang saling berkomunikasi harus dapat mengotentikasi satu sama lain sehingga ia dapat memastikan sumber pesan. Pesan yang di kirim melalui saluran komunikasi juga harus di otentikasi asalnya

METHOD

Development Engineering

This hybrid cryptosystem algorithm development technique uses analysis of the RSA Algorithm and the Triple DES Algorithm which are examples of symmetric cryptography and the Public Key Algorithm is an example of asymmetric cryptography.

The development flow of this hybrid cryptosystem algorithm can be seen in Figure 2. To simplify the process of encryption and decryption as well as key generation, it is divided into 4 flows:

1. Message encryption process flow
2. Message decryption process flow
3. Key encryption process flow
4. Key decryption process flow

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 3, Juli 2023
DOI : https://doi.org/10.33395/sinkron.v8i3.12467
e-ISSN : 2541-2019
p-ISSN : 2541-044X

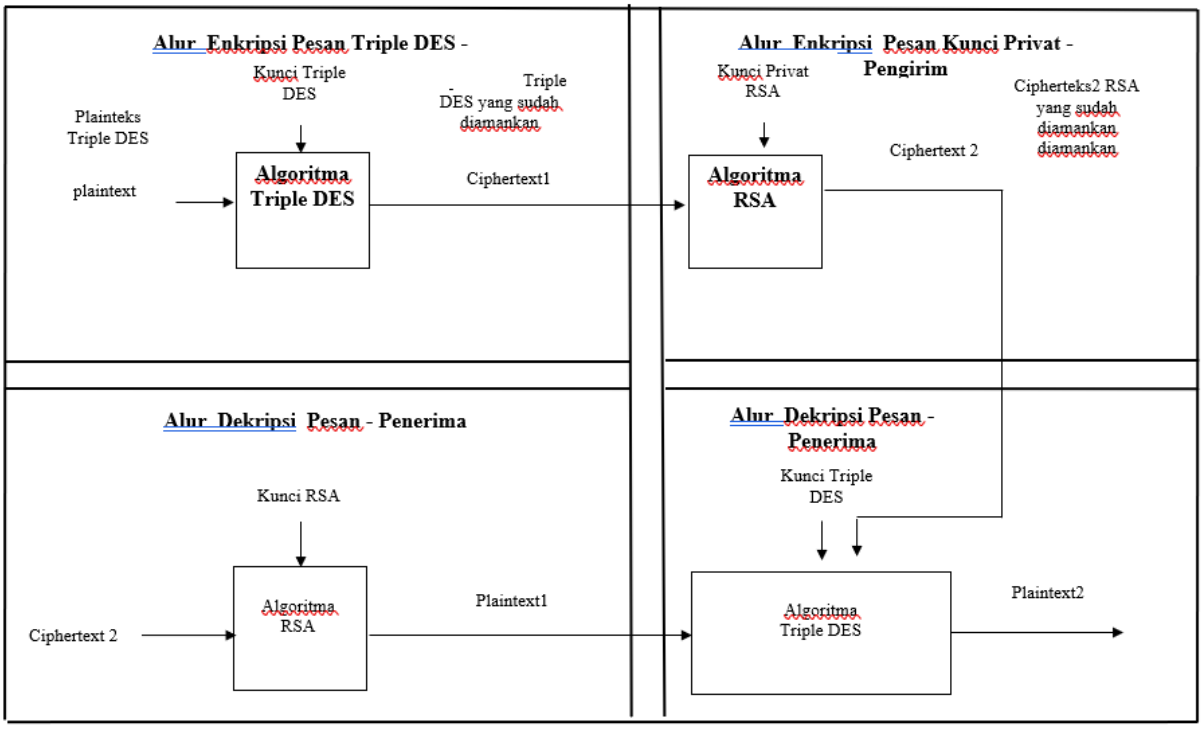


Figure 2. The development flow of the hybrid cryptosystem algorithm

Process Analysis

To add to the understanding of encryption and description in Triple DES with RSA it is carried out with many processes and is carried out in a hybrid manner, while the process can be seen below:

1. Encryption process analysis using Triple DES
   The steps in calculating the text message encryption process using Triple Des Cryptography are as follows:
   Plaintext Example: FASILKOM and change it to ASCII

F	**70**
A	**65**
S	**83**
I	**73**
L	**76**
K	**75**
O	**79**
M	**77**

2. Convert ASCII plaintext FASILKOM to be binary

70	0	1	0	0	0	1	1	0
65	0	1	0	0	0	0	0	1
83	0	1	0	1	0	0	1	1
73	0	1	0	0	1	0	0	1
76	0	1	0	0	1	1	0	0
75	0	1	0	0	1	0	1	1
79	0	1	0	0	1	1	1	1
77	0	1	0	0	1	1	0	1

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 3, Juli 2023 e-ISSN : 2541-2019
DOI : https://doi.org/10.33395/sinkron.v8i3.12467 p-ISSN : 2541-044X

3. Then Get 64 Bits Length
0100011001000001010100110100100101001100010010110100111101001101

4. Then plaintext with a length of 64 bits is divided into 32 bits
P : 01000110010000010101001101001001

01001100010010110100111101001101

5. Then enter the Key, Can be Made using alphabets or hexa numbers. As for the Triple Des key:

K	**75**
O	**79**
M	**77**
P	**80**
U	**85**
T	**84**
E	**69**
R	**82**

6. Then convert the Key to binary

75	0	1	0	0	1	0	1	1
79	0	1	0	0	1	1	1	1
77	0	1	0	0	1	1	0	1
80	0	1	0	1	0	0	0	0
85	0	1	0	1	0	1	0	1
84	0	1	0	1	0	1	0	0
69	0	1	0	0	0	1	0	1
82	0	1	0	1	0	0	1	0

7. Key Length Made to 64 Bits
0100101110100111101001101010100000101010101010100010001010101010

8. The 64 bits key is divided into 32 bits
K: 01001011010011111010011010101000

01010101010101000100010101010010

9. Then we do the OFB method from left to right

P	0	1	0	0	0	1	1	0	0	1	0	0	0	0	0	1	0	1	0	1	0	0	1	1	0	1	0	0	1	0	0	1
	0	1	0	0	1	1	0	0	0	1	0	0	1	0	1	1	0	1	0	0	1	1	1	1	0	1	0	0	1	1	0	1
K	0	1	0	0	1	0	1	1	0	1	0	0	1	1	1	1	0	1	0	0	1	1	0	1	0	1	0	1	0	0	0	0
	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	0	0	1	0	0	0	1	0	1	0	1	0	1	0	0	1	0

Round 1

P	1	0	0	0	1	1	0	0	1	0	0	0	0	0	1	0	1	0	1	0	0	1	1	0	1	0	0	1	0	0	1	0
1	1	0	0	1	1	0	0	0	1	0	0	1	0	1	1	0	1	0	0	1	1	1	1	0	1	0	0	1	1	0	1	0
K	1	0	0	1	0	1	1	0	1	0	0	1	1	1	1	0	1	0	0	1	1	0	1	0	1	0	1	0	0	0	0	0
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	0	0	1	0	0	0	1	0	1	0	1	0	1	0	0	1	0	0

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 3, Juli 2023
DOI : https://doi.org/10.33395/sinkron.v8i3.12467
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Round 2

P2	0	0	0	1	1	0	0	1	0	0	0	0	0	1	0	1	0	1	0	0	1	1	0	1	0	0	1	0	0	1	0	1
	0	0	1	1	0	0	0	1	0	0	1	0	1	1	0	1	0	0	1	1	1	1	0	1	0	0	1	1	0	1	0	1
K2	0	0	1	0	1	1	0	1	0	0	1	1	1	1	0	1	0	0	1	1	0	1	0	1	0	1	0	0	0	0	0	1
	0	1	0	1	0	1	0	1	0	1	0	1	0	0	0	1	0	0	0	1	0	1	0	1	0	1	0	0	1	0	0	1

Round 16

P16	0	1	0	1	0	0	1	1	0	1	0	0	1	0	0	1	0	1	0	0	1	1	0	0	0	1	0	0	1	0	1	1
	0	1	0	0	1	1	1	1	0	1	0	0	1	1	0	1	0	1	0	0	0	1	1	0	0	1	0	0	0	0	0	1
K16	0	1	0	0	1	1	0	1	0	1	0	1	0	0	0	0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	0
	0	1	0	0	0	1	0	1	0	1	0	1	0	0	1	0	0	1	0	0	1	0	1	1	0	1	0	0	1	1	1	1

10. Then do XOR to get the results of Q16 and K16. The above results are
00011111000011001000110010001111100001010000011010000111 0

11. After getting the results, do another 16 rounds to produce Double Des and until you get the results, then do another 16 rounds for encryption of Triple Des

RESULT

In the principle of security sending information that is secured by messages and keys. This security is carried out using a hybrid of the Triple DES algorithm with the RSA Algorithm.

Triple DES Encryption Initialization Process

To find out the results of Triple DES encryption, the first thing to do is to input the plaintext that has been determined before the sending process is carried out. Plaintext is in the form of text. And the process of replacing plaintext characters with decimals is carried out using the ASCII table and continued by changing them to binary. The process can be seen below:

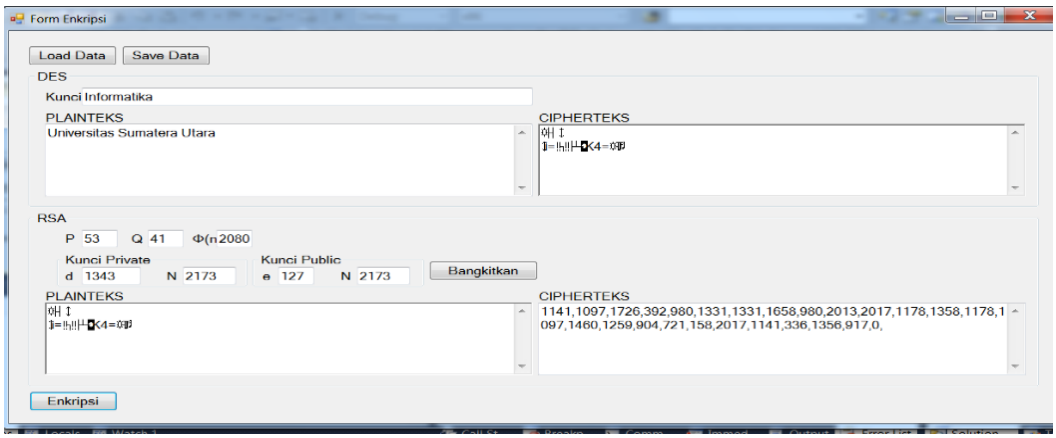


Figure 3. Encryption Process by Triple DES

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 3, Juli 2023
DOI : https://doi.org/10.33395/sinkron.v8i3.12467
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Hybrid Initialization Process of Triple DES Encryption to RSA

Find P and Q by randomly generating prime numbers if they have been obtained then do it as shown below:

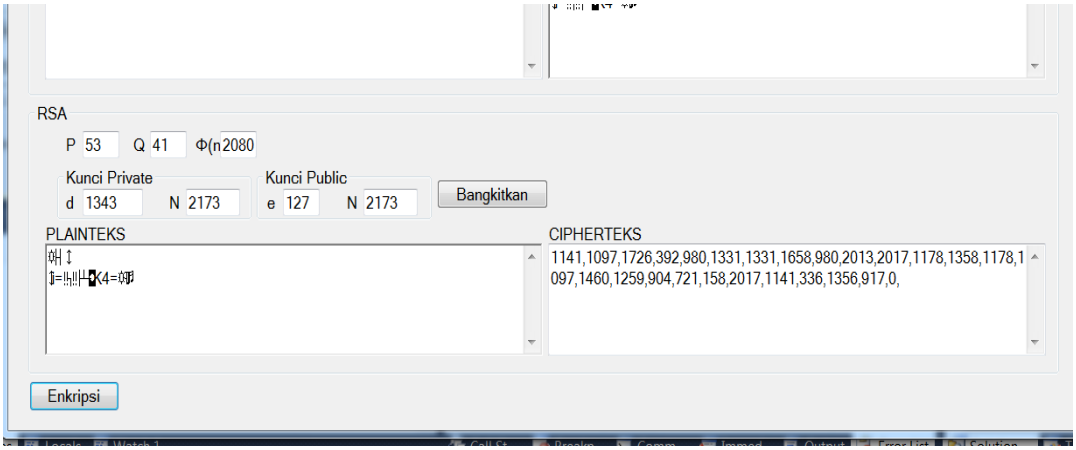


Figure 4. Encryption Process by Triple DES to RSA

Hybrid RSA Description Initialization Process Becomes Triple DES

To get plaintext, Triple DES encrypted with the RSA algorithm must be encrypted first, then the results of the description will be used to describe back to Triple DES.

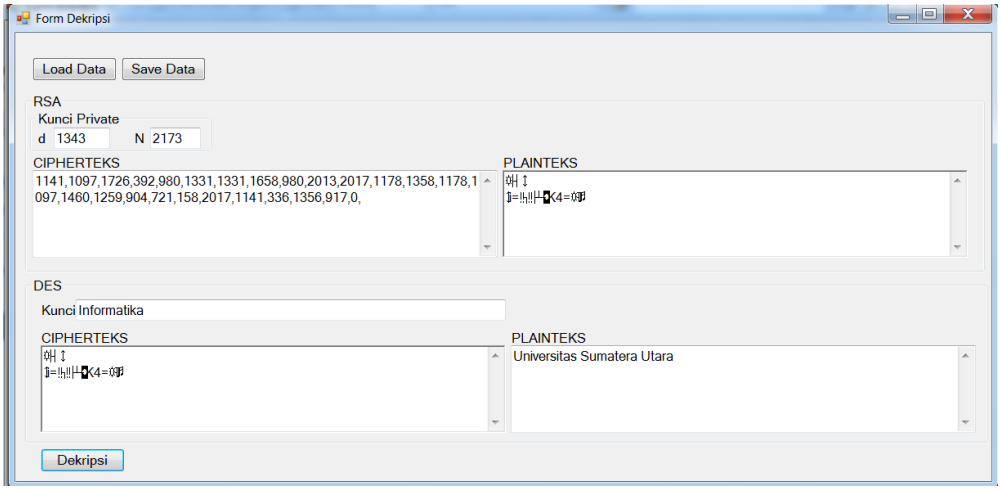


Figure 5. Process Description RSA to Triple DES

From the results of the implementation it was concluded that:

1. The encryption process that is carried out is a long process because the calculation process in the Triple Des algorithm has 16 rounds where it is not only Plaintext that is made rounds but the Key of Triple Des is done.
2. Also rotate 16 times and add XOR to get DES results and do it repeatedly. To get Double and Triple DES results 48 times.
3. The encryption process after getting Plaintext from Triple DES then proceed to RSA Encryption where in order to produce even higher security and use random primes so that it will be increasingly difficult to break because to find the e key, a random calculation of prime numbers is carried out so that the results obtained are obtained will not be easy to obtain.

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 3, Juli 2023
DOI : https://doi.org/10.33395/sinkron.v8i3.12467
e-ISSN : 2541-2019
p-ISSN : 2541-044X

4. The description process after getting the Plaintext RSA results depends on the private key so that to find the private key you have to get the P and q values and the e values, so breaking into the security will be even more complicated because the calculations are longer.
5. Description Process After getting the RSA Plaintext results, to restore in Triple DES is done by returning the Plaintext results to decimal using the ASCII table and then calculating in binary. And a predefined Key is required. So that it will be even more complicated to break into and do another round of 16 times in DES, Double and Triple Des and XOR calculations are carried out.

DISCUSSIONS

Table1. Research Results of Message Encryption Process with Triple DES Algorithm

NO	PlainText		Kunci Triple Des		ChiperTeks	
	Karakter	Bilangan Desimal	Karakter	Bilangan Desimal	Bilangan Desimal	Karakter ASCII
1	Universitas Sumatera Utara	85 110 105 118 101 114 115 116 97 115 32 83 117 109 97 116 101 114 97 32 85 116 97 114 97	Informatika	73 110 102 111 114 109 97 116 105 107 97	15 25 23 31 18 29 29 10 18 105 61 19 2 19 25 4 6 8 75 52 61 15 20 14 28 0	☼↓↕▼↕↔↔ ↕i=‼♦♠◘K4=☼'n♫z_
2	PASCA SARJANA	80 65 83 67 65 32 83 65 82 74 65 78 65	Informatika	73 110 102 111 114 109 97 116 105 107 97	53 44 51 77 50 53 59 33 32 7 47 25 47	5,3M25;! ● / ↓ /
3	Harus Bisa	72 97 114 117 115 32 66 105 115 97	Masa Depan	77 97 115 97 32 68 112 97 110	1 20 83 100 39 35 18 15 5 0	☺'nSd′#↕☼♣
4	Terima Kasih	84 101 114 105 109 97 32 75 97 115 105 104	Sampai Jumpa	83 97 109 112 97 105 32 74 117 109 112 97	31 25 12 8 0 1 20 30 25 9 7 4	▼↓♀◘ ☺'n▲↓◙●♦
5	Mohon Maaf Lahir Dan Batin	77 111 104 111 110 32 77 97 97 70 32 76 97 104 105 114 32 68 97 110 32 66 97 116 105 110	Selamat Hari Lebaran	83 101 108 97 109 97 109 97 116 32 72 97 114 105 32 76 101 98 97 114 97 110	4 14 3 65 57 65 41 7 82 37 65 36 12 16 65 54 0 0 115 15 30 10	♦♫♥A9A>●R%A$♀►A6 s☼▲

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 3, Juli 2023
DOI : https://doi.org/10.33395/sinkron.v8i3.12467
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Table 2 Results of Research on Message Encryption Process with the RSA Algorithm

NO	PlainText		RSA						ChiperTeks
	Karakter	Bilangan Desimal	P	Q	Φn	d	e	N	Bilangan Desimal
1	Universitas Sumatera Utara	85 110 105 118 101 114 115 116 97 115 32 83 117 109 97 116 101 114 97 32 85 116 97 114 97	53	41	2080	57	73	2173	1274 1744 1589 1396 26 1836 1045 2144 1552 1045 1221 83 1951 1790 1552 1552 26 1836 1552 1221 1274 1552 1836 1552
2	PASCA SARJANA	80 65 83 67 65 32 83 65 82 74 65 78 65	37	83	2952	1597	61	3071	2522 206 830 1224 206 2460 830 206 82 2960 206 2694 206
3	Harus Bisa	72 97 114 117 115 32 66 105 115 97	97	47	4416	2729	89	4559	1748 1746 4263 2671 1340 820 1018 962 1340 1746
4	Terima Kasih	84 101 114 105 109 97 32 75 97 115 105 104	67	53	3432	1733	101	3551	3371 251 2276 3179 2122 3388 2192 1611 3388 2645 3179 1570
5	Mohon Maaf Lahir Dan Batin	77 111 104 111 110 32 77 97 97 70 32 76 97 104 105 114 32 68 97 110 32 66 97 116 105 110	43	97	4032	989	53	4171	261 3048 3660 3048 702 968 261 3977 3977 2146 968 3666 3977 3660 1534 1775 968 984 3977 20 1534 702

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 3, Juli 2023
DOI : https://doi.org/10.33395/sinkron.v8i3.12467
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Table 3 Results of Hybrid Process Research of the Triple Des Algorithm and the RSA Algorithm

NO	PlainText		Kunci Triple Des		ChiperTeks	
	Karakter	Bilangan Desimal	Karakter	Bilangan Desimal	Bilangan Desimal	Karakter ASCII
1	Universitas Sumatera Utara	85 110 105 118 101 114 115 116 97 115 32 83 117 109 97 116 101 114 97 32 85 116 97 114 97	Informatika	73 110 102 111 114 109 97 116 105 107 97	15 25 23 31 18 29 29 10 18 105 61 19 2 19 25 4 6 8 75 52 61 15 20 14 28 0	☼↓↕▼↕↔↔ ↕i=‼♦♠◘K4=☼'n♫z_
2	PASCA SARJANA	80 65 83 67 65 32 83 65 82 74 65 78 65	Informatika	73 110 102 111 114 109 97 116 105 107 97	53 44 51 77 50 53 59 33 32 7 47 25 47	5,3M25;! ● / ↓ /
3	Harus Bisa	72 97 114 117 115 32 66 105 115 97	Masa Depan	77 97 115 97 32 68 112 97 110	1 20 83 100 39 35 18 15 5 0	☺'nSd'#↕☼♣
4	Terima Kasih	84 101 114 105 109 97 32 75 97 115 105 104	Sampai Jumpa	83 97 109 112 97 105 32 74 117 109 112 97	31 25 12 8 0 1 20 30 25 9 7 4	▼↓♀◘ ☺'n▲↓◙●♦
5	Mohon Maaf Lahir Dan Batin	77 111 104 111 110 32 77 97 97 70 32 76 97 104 105 114 32 68 97 110 32 66 97 116 105 110	Selamat Hari Lebaran	83 101 108 97 109 97 109 97 116 32 72 97 114 105 32 76 101 98 97 114 97 110	4 14 3 65 57 65 41 7 82 37 65 36 12 16 65 54 0 0 115 15 30 10	♦♫♥A9A>●R%A$♀►A6 s☼▲

NO	ChiperTeks Triple DES			RSA						ChiperTeks RSA	
	Karakter	Bilangan Desimal	Karakter ASCII	P	Q	Φn	d	E	n	Rumus	Hasil
1	Universitas Sumatera Utara	15 25 23 31 18 29 29 10 18 105 61 19 2 19 25 4 6 8 75 52 61 15 20 14 28 0	☼↓↕▼↕↔↔ ↕i=‼♦♠◘K4=☼'n♫_	53	41	2080	57	73	2173	C ^ e mod 2173	2167,2054,1507, 1911,2142,2104, 2104,713,2142, 1589,405,1133,525, 1133,2054,1827,1862, 882,1693,1059,405, 2167,569,1121,1815,0,
2	PASCA SARJANA	53 44 51 77 50 53 59 33 32 7 47 25 47	5,3M25;! ● / ↓ /	37	83	2952	1597	61	3071	C ^ e mod 3071	1085,1255,2271,559, 190,1085,1256,1968, 2460,441, 1342,1693,1342,
3	Harus Bisa	1 20 83 100 39 35 18 15 5 0	☺'nSd'#↕☼♣	97	47	4416	2729	89	4559	C ^ e mod 4559	1, 2477, 4255, 2533, 3920, 3393,953, 1060, 890, 0
4	Terima Kasih	31 25 12 8 0 1 20 30 25 9 7 4	▼↓♀◘ ☺'n▲↓◙●♦	67	53	3432	1733	101	3551	C ^ e mod 2551	2523,1362,1330, 3018,0,1,2950,507, 1362,1488,2296,2361,
5	Mohon Maaf Lahir Dan Batin	4 14 3 65 57 65 41 7 82 37 65 36 12 16 65 54 0 0 115 15 30 10	♦♫♥A9A>●R%A$♀►A6 s☼▲	43	97	4032	989	53	4171	C ^ e mod 4171	3352, 526, 1019, 2330, 10 2330, 3800, 3563, 2969, 179, 2330, 3360, 3810, 3401, 2330, 2429, 0 ,0 1366, 1493, 149, 3111

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 3, Juli 2023
DOI : https://doi.org/10.33395/sinkron.v8i3.12467
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Table 4 Research Results of Character Length and Speed of Time in the Hybrid Process of the Triple Des Algorithm and the RSA Algorithm

No	Panjang Karakter	Waktu
1	1197	00:00:00:06
2	2350	00:00:00:21
3	8379	00:00:03:11
4	2295	00:00:00:20
5	2016	00:00:00:18
6	2394	00:00:00:24
7	16758	00:00:14:48
8	1521	00:00:00:12
9	1360	00:00:00:07
10	2836	00:00:00:28

Character Length Graph With Process Time in Triple DES and RSA Algorithms

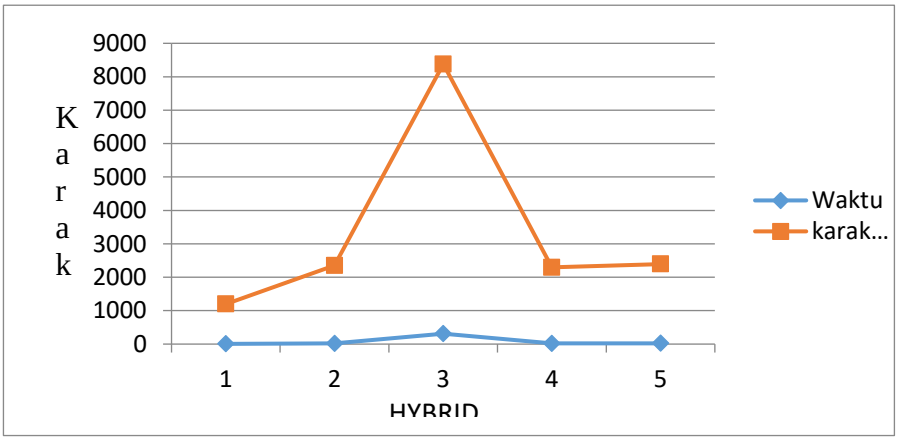
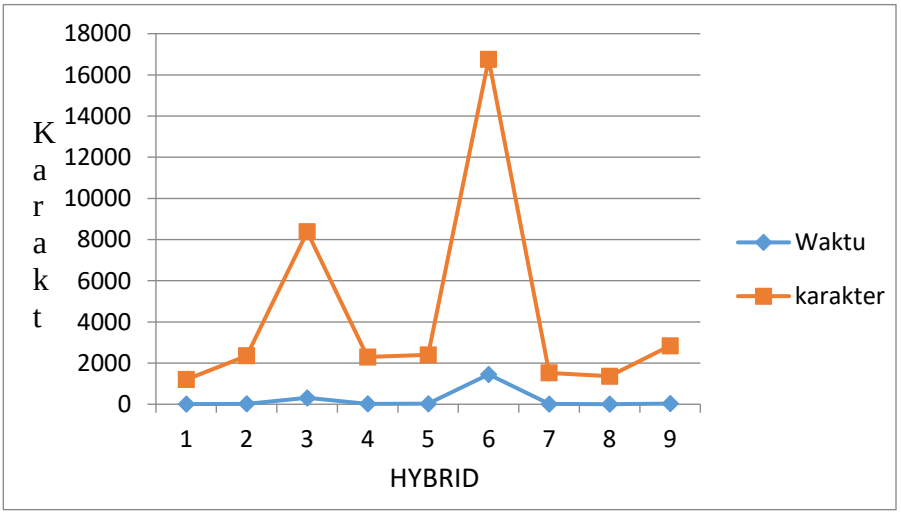


Figure 6. Graph of Character Length with Time Process in Triple DES and RSA Algorithms with 5 Data



*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 7, Number 3, Juli 2023
DOI : https://doi.org/10.33395/sinkron.v8i3.12467
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Figure 7. Graph of Character Length with Process Time in Triple DES and RSA Algorithms with 10 Data

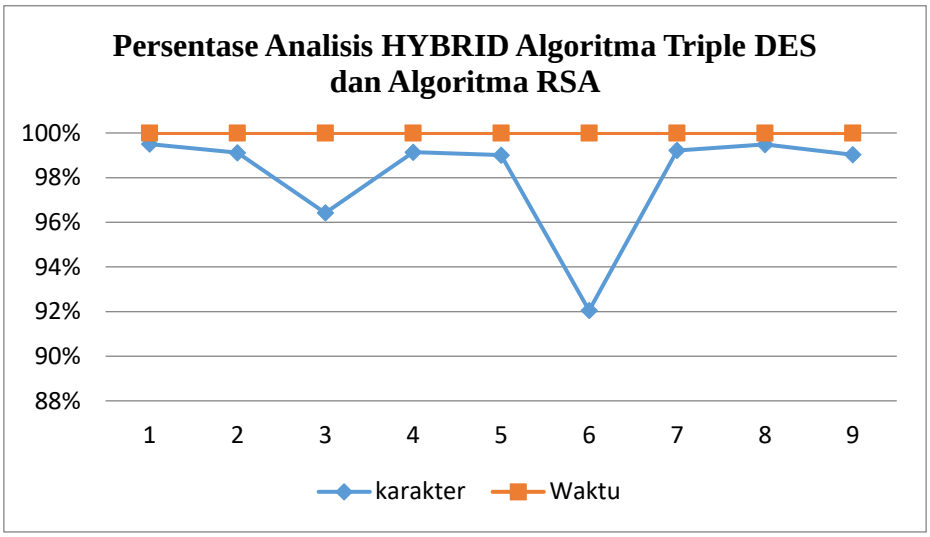


Figure 8. Graph of Hybrid Analysis Percentage in the Triple DES Algorithm and the RSA Algorithm

CONCLUSION

Based on the results of the research and discussion, the conclusions can be written as follows:

1. Based on the tests conducted, it was concluded that the cryptosystem hybrid Triple DES Algorithm and the RSA Algorithm complement each other in plaintext security so that they are not easily attacked by using this connection method.
2. The more random the prime numbers in the RSA algorithm, the more difficult it is to break into its security because it is difficult to find the value of d or the private key.
3. The bigger the p and q in the RSA algorithm, the bigger the key will be.
4. The longer the character you want to encrypt, the longer the process, so the percentage of speed decreases.
5. The advantages of the Triple DES algorithm hybrid cryptosystem with the RSA algorithm produce long keys that make it difficult for security to be solved easily.
6. Message security using hybrid cryptosystem Triple DES Algorithm and RSA Algorithm is better because the key used for encryption and description is different. In addition, it is very difficult to guess the key because the RSA private key must be found using random prime numbers. And the results are never the same.

REFERENCES

Ariyus, Dony. 2008. Pengantar Ilmu Kriptografi: Teori, Analisis dan Implementasi. Penerbit Andi: Yogyakarta.

Ariyus, Dony. 2006. Computer Security. Penerbit Andi: Yogyakarta.

Chan, Sasmita, Adhytio & Ginting Muthe, Permana 2014. Perancangan Aplikasi Pengamanan File dengan Memanfaatkan USB Flashdisk Sebagai Kunci Menggunan Algoritma Triple DES. *ISSN*: 2301-9425

Chmielowiec, D. 2010. Fixed Point Of The RSA Encrytion ALgorithm. *Elvesier Theoretical Computer Science*: 411: 288-292

Karkarla, Veenannand & Govind, N.S. 2012. FPGA Implementation of Hybird Encryption Algorithm Based on triple DES and RSA in Bluetooth Communication. *International Journal of Applied Research & Studies*: 2278-9480

*name of corresponding author

Kim, S. & Lee, G. 2006. Secure Verifiable Non- interactive Oblivious Transfer Protocol Using RSA and Bit Commitment On Distributed Envirotment, Elsevier

Kromodimoeljo, Sentot. 2010. *Teori & Aplikasi Kriptografi,* SPK IT Consulting

Kurniawan, Yusuf. 2004. Kriptografi. Keamanan Internet dan jaringan Komunikasi. Penerbit Informatika. Bandung.

Madhur, Kapil., Yadav, Singh, Jitendra. & Vijay, Ashish. 2012. Modified Elgamal over RSA Digital Signature Algorithm (MERDSA). *International Journal of Advanced Research in Computer Science and Software Engeneering*(1): 2277-128X

Mahajan, Sonam & Sigh, Maninder. 2014. Performance Analysis of Efficient RSA Text Encrytion Using NVIDIA Cude – C and Open CL. *Proceeding of the 2014 International Conference on interdisciplinary Adveances in Applied Computing – ICONIAAC* '14 31:1-6.

Mollin, Richard. 2007. *An Introduction to Cryptography*, Taylor & Francis Group

Munir, Rinaldi. 2006. *Kriptografi*. Penerbit informatika, Bandung

Narula, Sigh, Mandeep & Singh, Simarpreet. 2014. Implementation of Triple Data Encrytion Standart using verilog. *International Journal of Advanced Research in Computer Science and Software Engeneering*(1): 2277-128X

Parsi K.2012. Data Security in cloud computing using RSA Algorithm. International Journal of Research in computer & Communication Technology,1(4) : 143-146

PuCha, ZHONG & WanSu, BAO, 2012. Quantum menhanical meet-in-the-middle search algorithm for Triple DES. *Chinese Science Bulletin*(3): 321-325

Pratama, Aditya. 2011. Pembangkit Bilangan Acak Semu. *Kriptografi:* **IF3058**

Sadikin, Rifki. 2012. *Kriptografi untuk keamanan jaringan*, CV Andi Offset, Yogyakarta

Talbot, Jhon dan Dominic Welsh. 2006. *Complexity and Crytography*. USA : Cambridge University Press.

Thao. 2014. A Visualization Tool For The RSA Cipher. *Proceeding of the ACM National Science Foundation under grants DUE-1140512, DUE-1245310 and IIS=1319363*: Departement of Computer Science Michigan Technological Universitas Houghton, MI.USA.

Wang, H., Song, Z., Niu, X. & Ding, Q. 2013. Key Generation Research of RSA Public Crytosystem and Matlab Imp[lement. *International Conference on sensor Network Security Technology and Privacy Communication System (SNS & PCS)*: 18 : 125 – 129.

Zainal, 2009. Studi Kasus Penggunaan Algoritma RSA sebagai Algoritma Kritografi yang aman. Jurnal Informatika Mulawarman. (3 September 2009).

*name of corresponding author