International Journal of Information System & Technology
Akreditasi No. 36/E/KPT/2019 | Vol. 4, No. 1, (2020), pp. 471-481

Implementation of Combination Vigenere Cipher and RSA in Hybrid Cryptosystem for Text Security

Jamaludin, Romindo

Politeknik Ganesha Medan

jamaludinmedan@gmail.com, romindo4@gmail.com

Abstract

According to the key used, cryptography can be divided into two, namely: symmetric cryptography and asymmetric cryptography, each of which has advantages and disadvantages. The selection of a symmetric cryptographic algorithm can perform the encryption process in a short time, but the key security is less secure so it must be changed frequently. While asymmetric cryptography is the opposite, the security of key distribution can be overcome but the data encryption process is slower. The coding process in this study uses two cryptographic algorithms, namely the Vigenere Cipher algorithm as an example of the symmetric algorithm and the RSA (Rivest Shamir Adleman) algorithm which is an example of an asymmetric algorithm. The purpose of this research is to calculate and implement so that it can be applied to overcome the weaknesses that occur from the two types of cryptography. The hybrid cryptosystem coding method is always used to overcome the weaknesses of the two cryptographs. The results show that there is an increase in security in encryption because there will be two encodings, namely message encoding with the Vigenere Cipher cryptographic algorithm and key coding with the RSA cryptographic algorithm. Besides, there is an increase in the time in the encryption and decryption process. From the results of the research, it takes 424 milliseconds in the encryption process and 335 milliseconds for the decryption process with 59,400 characters. A hybrid cryptosystem coding method using a combination of Vigenere Cipher and RSA can be implemented to increase text security and increase speed in the encryption process.

Keywords: *Cryptography, Hybrid Cryptosystem, Vegenere Cipher, RSA*

1. Introduction

There are several arts of securing data through a channel, one of which is cryptography. Cryptography is a technique of securing and guaranteeing the authenticity of data which consists of two processes, namely encryption and decryption [1]. In cryptography, highly confidential data will be encrypted in such a way that even if the data is stolen by unauthorized parties, they cannot find out the real data, because the data they steal is data that has been encrypted. The original data to be sent and in cryptography as plaintext, and the data that has been encoded is called ciphertext

Cryptography aims to maintain the confidentiality of the information contained in the data so that unauthorized parties cannot find out the information. Cryptographic algorithm designers are called cryptographers [2].

Based on the keys used for encryption and decryption, cryptography can be divided into symmetric-key cryptography and asymmetric-key cryptography. Each of them has its advantages and disadvantages. Symmetric cryptographic algorithm is designed so that the encryption process requires a short time. The weakness is that the security of the lock is less secure and the key must be changed frequently. While asymmetric cryptography is on the contrary, security issues in key distribution can be overcome, but the encryption and decryption process of data is generally slower because encryption and decryption use

ISSN : 2580-7250

large numbers and involve large power operations and the size of the ciphertext is larger than plaintext [3].

To overcome the weaknesses of the two types of cryptography, a hybrid cyptosystem coding method is used. Hybrid cryptosystem is a technique that uses several different ciphers to take advantage of their respective advantages. A hybrid cryptosystem is built using two divider cryptosystems, namely the public key and the symmetric key[4]. In a hybrid cryptosystem, files are secured using a symmetric algorithm and symmetric keys are secured using an asymmetric algorithm [1].

The reasons for overcoming the weaknesses of the two types of key cryptography are weak data security and the slow encryption decryption process, so research is needed by combining the Vigenere Cipher algorithm, one example of symmetric key cryptography and RSA, one example of symmetric key cryptography with the hybrid cryptosystem method, so that from a combination of the two types of cryptographic algorithms It is hoped that this will result in a high level of security but fast in the encryption and decryption process [5].

2. Literature Review

The purpose of this research is to analyze through the results of calculations and implement the results of these calculations to overcome the weaknesses that occur from the two types of cryptography. The hybrid cryptosystem coding method is always used to overcome the weaknesses of the two cryptographs. Hybrid cryptography is often used because it takes advantage of the advantages of data processing speed by a symmetric algorithm and the ease of key transfer using an asymmetric algorithm. This results in increased speed without compromising comfort and safety.

Hybrid cryptographic algorithms are algorithms that utilize two levels of keys, namely the secret key (symmetrical) - also known as the session key - for data encryption and the secret key pair - the public key for digital signatures and protecting the symmetrical key [6].

The coding process in this study uses two cryptographic algorithms, namely the Vigenere Cipher algorithm as an example of the symmetric algorithm and the RSA (Rivest Shamir Adleman) algorithm which is an example of an asymmetric algorithm.

The choice of Vigenère Cipher is based on the fact that the Vigenère Cipher is the best example of a compound-alphabet cipher and is very well known for being easy to understand and implement [3]. However, the Vigenère Cipher cryptography is no longer secure, several methods of attacking the Vigenère Cipher cipher have revealed this code weakness. The cipher analysis proposed by Friedrich Kasiski called the Kasiski test in 1963 against the Vigenère Cipher cipher could unravel the key length and subsequently unravel the key value of the Vigenère Cipher key [7]. While the selection of the RSA algorithm as an asymmetric key cryptography is because of the many public-key cryptographic algorithms that have been made, the most popular algorithm is the RSA algorithm. This algorithm performs factoring of very large numbers. For these reasons RSA is considered safe. To generate two keys, two large random prime numbers are selected[6]. The weakness of RSA is seen when a small encryption exponent is used to send the same message to different recipients [8].

To enrich the material to be discussed, references to previous research are needed. Previous research serves to analyze and enrich the discussion of research, and to differentiate it from the research that is currently being carried out. In this case, two previous national research journals related to the author's research are included, these journals include :

1. Research entitled **"Implementation of Rivest Shamir Adleman (RSA) Cryptographic Algorithms and Vigenere Cipher on 8 Bit Bitmap Images",** was investigated by Andro Alif Rakhman and Achmad Wahid Kurniawan in the national journal TechnoCom Vol. 14, No. 2, May 2015: 122-134, describes security using two

types of cryptographic combination symmetric and asymmetric types. The method used in this study is to combine the Rivest Shamir Adleman (RSA) and Vigenere Cipher cryptographic algorithms on the color index value of each pixel. using a combination of the Rivest Shamir Adleman (RSA) and Vigenere Cipher algorithms to secure the image. The image to be used is a bitmap file with a pixel depth of 8 bits. The image will be processed by encrypting the RGB color index value on each pixel using the RSA cryptographic algorithm first, then continued by using the Vigenere Cipher algorithm. Meanwhile, the decryption stage is carried out using the Vigenere Cipher algorithm first and then using the RSA cryptographic algorithm [9].

The advantage of this journal heme is that security is used on images and has been proven by software. The weakness of the coding process does not use schematic diagrams so that it is difficult to understand the series of work, especially for readers who do not understand cryptography. The research equation that the authors do is both using two types of cryptography of the symmetric and asymmetric types, only the difference is that the author uses a different method, namely Hybrid Cryptosystem, there is an encryption and message decryption process in Vegenare Ciphter cryptography and the encryption and key decryption process in key cryptography occurs in cryptography RSA.

2. The research entitled **"Combination of Caesar Cipher Algorithm and RSA Algorithm for Securing Document Files and Text Messages",** was investigated by Indra Gunawan at the National Journal of InfoTekJar Vol. 2, No. 2, March 2018: 124-129, describes security using two types of symmetric cryptographic combinations, namely Caesar and asymmetric, namely RSA. The combination of the Caesar cipher with the RSA algorithm works by encrypting the message first with the Caesar cipher, then the results of the message (ciphertext) are re-encrypted using the RSA algorithm, so that the statistical appearance of the message cannot be detected [10].

   The advantages of this journal theme are security used on files and have been proven by software. The weakness of the coding process does not use schematic diagrams so that it is difficult to understand the series of work, especially for readers who do not understand cryptography. The research equation that the authors do is both using two types of cryptography of the symmetric and asymmetric types, only the difference is that the author uses a different method, namely Hybrid Cryptosystem, there is an encryption and message decryption process in Vegenare Ciphter cryptography and the encryption and key decryption process in key cryptography occurs in cryptography. RSA.

3. Research Methodology

The coding method used in this study uses a Hybrid Cryptosystem using a combination of the Vigenere Cipher Algorithm which is an example of symmetric cryptography and the RSA Algorithm which is an example of asymmetric cryptography

The scheme for the development of the Hybrid Cryptosystem algorithm before the calculation process can be seen in the following figure:

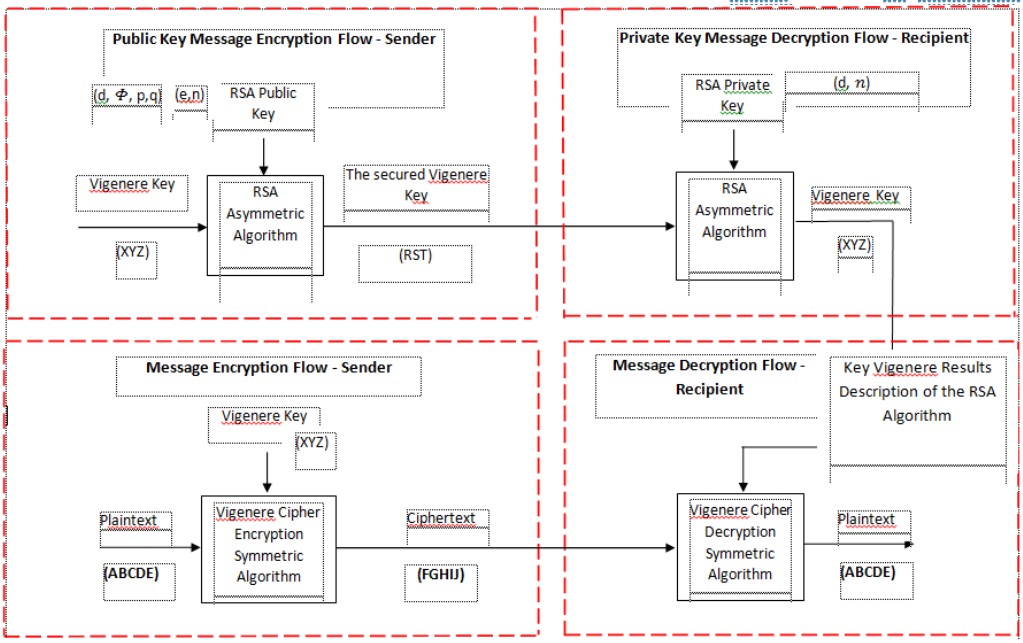

Figure 1. Schematic Diagram of The Combination of Vigenère Cipher and RSA Using the Hybrid Crytosystem Method

To simplify the encryption and decryption process in the Hybrid Cryptosystem algorithm development and key generation, it is divided into 4 streams:

1. Message encryption process flow - sender
2. Message-recipient decryption process flow
3. The flow of the public key encryption process - sender
4. Private key decryption process flow – recipient

3.1. Message Encryption Process Flow – Sender

In the message encryption process, the readable text (plaintext) ABCDE is encrypted by the Vigenere Cipher Symmetric Algorithm using the XYZ key, the result is in the form of FGHIJ ciphertext encoded text which will be sent to the recipient later.

The flow of the message-sender encryption process can be seen in Figure 2.

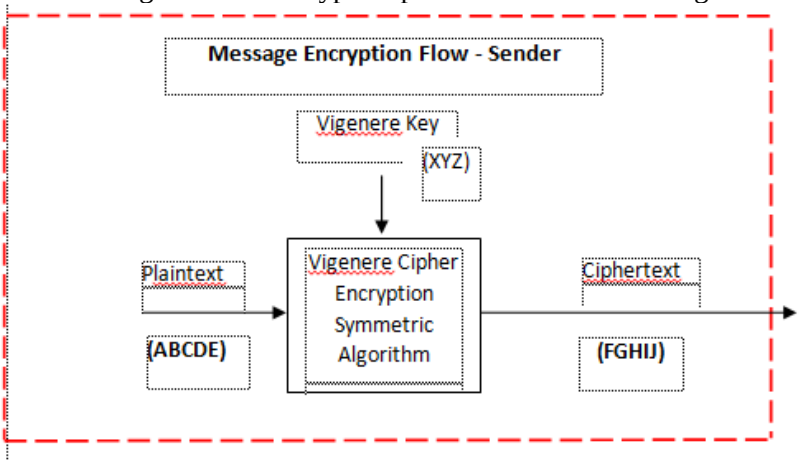

Figure 2. The Process of Encrypting The Sender's Message

3.2. Message-Recipient Decryption Process Flow

The FGHIJ ciphertext is the result of encryption by the Vigenere Cipher Encryption Algorithm, then decrypted by the Vigenere Decryption Symmetric Algorithm using the XYZ key, the result of the RSA algorithm key description results in ABCDE plaintext

that can be read by the recipient. The process flow of the recipient's message decryption can be seen in Figure 3.

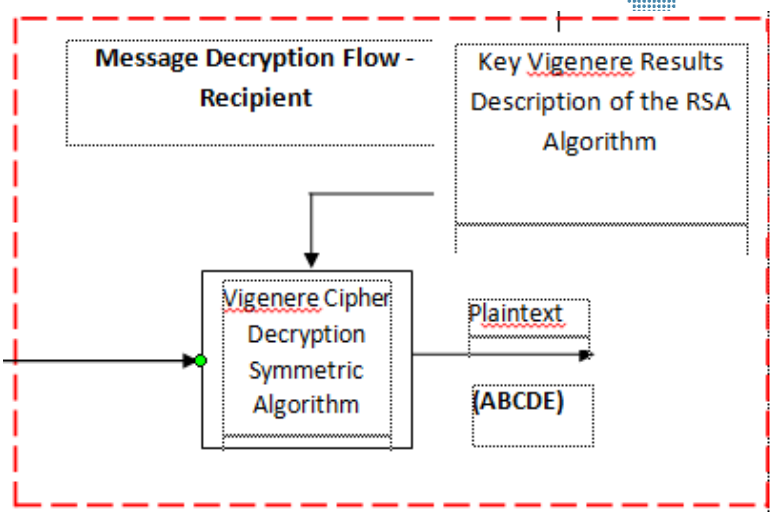

Figure 3. Recipient Message Decryption Process

3. 3. The Flow Of The Public Key Encryption Process – Sender

The XYZ key is encrypted using the RSA Asymmetric Algorithm with the RSA public key generating an RST key which will later be sent to the recipient.

The flow of the RSA public key encryption process can be seen in Figure 4.:

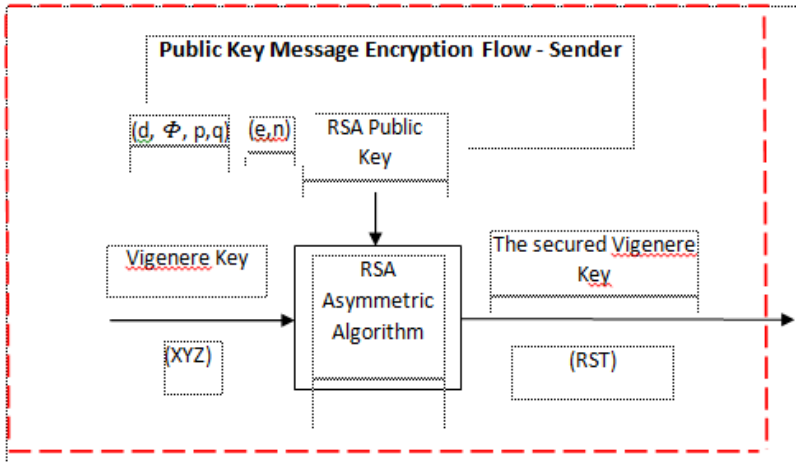

Figure 4. The Process of Encrypting The Sender's Public Key

3.4. Private Key Decryption Process Flow – Recipient

The Vigenere key has been secured encrypted using the RSA Asymmetric Algorithm with the RSA private key generating the Vigenere key. Then the key is decrypted using a private RSA key, then the Vignere key is generated which is used to generate the Vigenere Cipher Decryption Symmetric Algorithm. The process flow of the recipient's private key decryption can be seen in Figure 5.

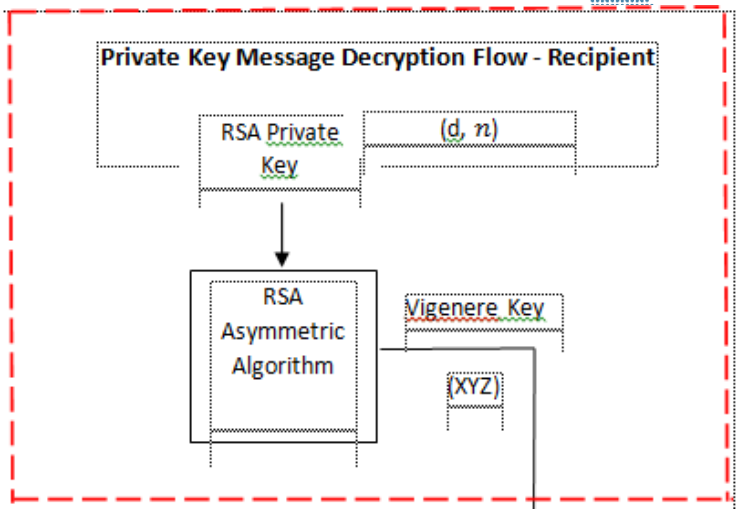

Figure 5. The Process of Decrypting The Recipient's Private Key

To prove the correctness of the method used, an analysis of the combination of the two types of cryptography Vigenere Cipher and RSA is carried out, then the calculation is carried out until finally the results of the calculations performed show that the message and key sent must be the same as the message and key received. Figure 6. shows a schematic image of the correct calculation results, so that the method used can be implemented in programming form.

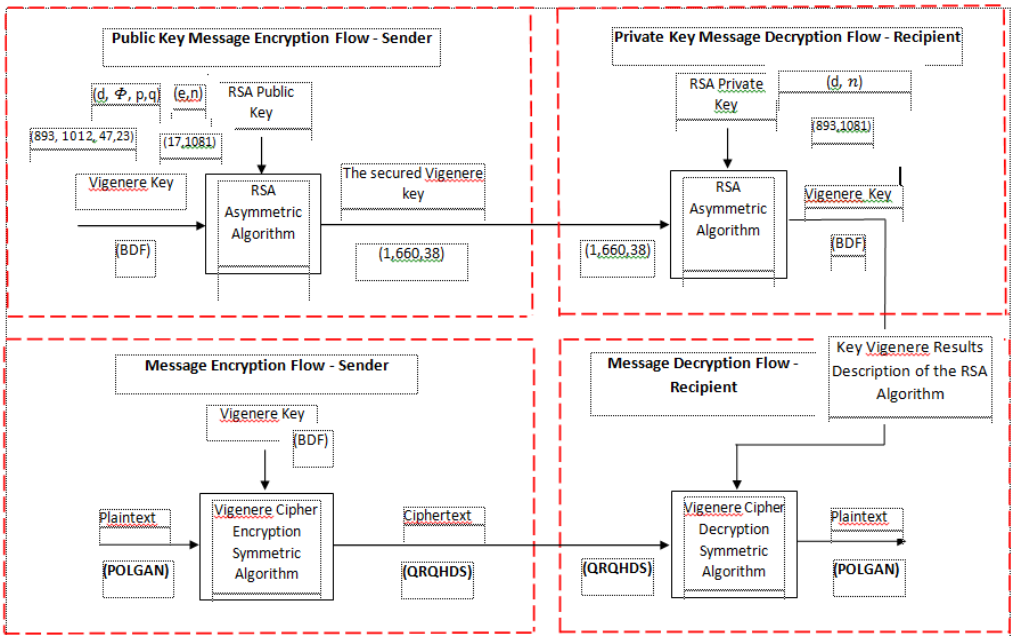

Figure 6. Schematic Diagram of The Combination of Vigenère Cipher and RSA Using The Hybrid Crytosystem Method

4. Result and Discussion

4.1. Finding

In this discussion, the calculation results of the coding process from the combination of the Vigenère Cipher and RSA algorithms will be implemented in software, with the software being easier to test the coding results. Because a laptop device is used to affect the speed of the encryption process, the specifications of the laptop are as follows:

a) Using the Windows 7 Operating System and VB.Net Ver Programming Software. 2010.
b) Supporting hardware: Laptop Toshiba Satellite L645 Core I3 processor with a speed of 2.3 GHz, 2 GB RAM memory, 160 GB hard disk.

The following is a display of the output of a combination of the Vigenère Cipher and RSA algorithms. After the program is run, the main form will appear as shown in Figure 7. Then in the main form we can choose to process the encryption there is an Encryption form as shown in Figure 8. and the decryption process as shown in Figure 9.

Figure 7. Main Form Display

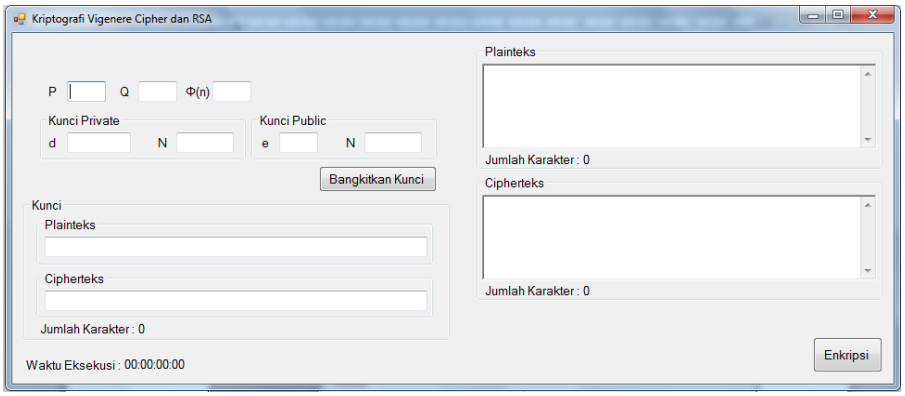

Figure 8. Display Encryption Process Form

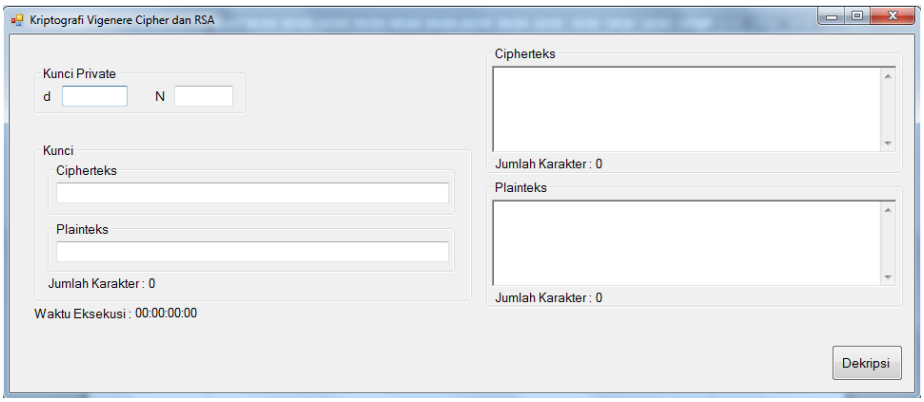

Figure 9. Display Decryption Process Form

Then we will test the results of the calculations we have done before, by implementing them in the software. To perform the encryption process on the main menu select **Encryption**, then we enter 2 prime numbers **P = 47** and **Q = 23** and $\varphi_{(n)}$ = **1012** then enter the **Private Key d = 893, N = 1081** and the **Public Key e = 17 and N = 1081**. Then enter a text message on the **Plaintext: POLGAN** tab and enter the key in **Plaintext: BDF**. To perform the encryption process, select the Encrypt button, you will see the results of the **QRQHDS** ciphert text for the text and the ciphert text **1,660,38,** the key, as shown in Figure 10.

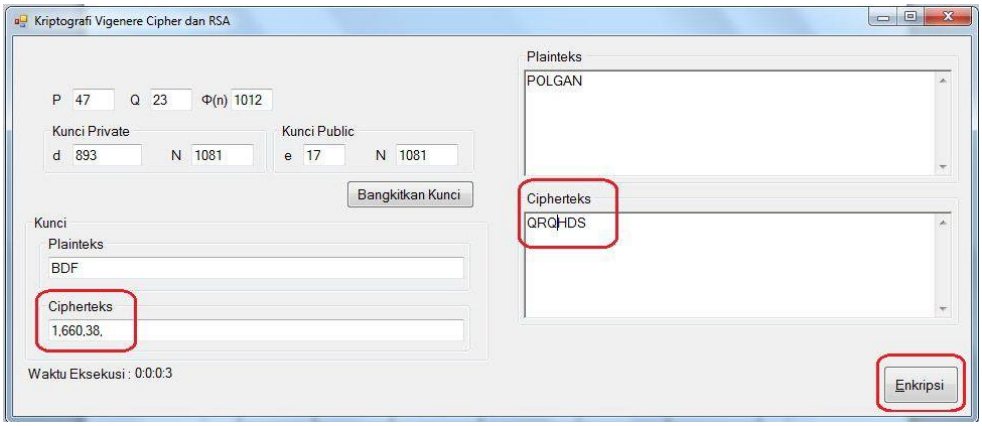

Figure 10. Text Message Encryption Process and Key

Then to do the decryption process, select the Decryption tab on the main menu. Enter the **Private Key d = 893** and **N = 1081**, then enter the **QRQHDS** ciphert text for text and ciphert text 1,660,38, key, finally select Decryption, the text message will return to the **POLGAN** plaint text and **BDF** key, as shown in Figure 11.

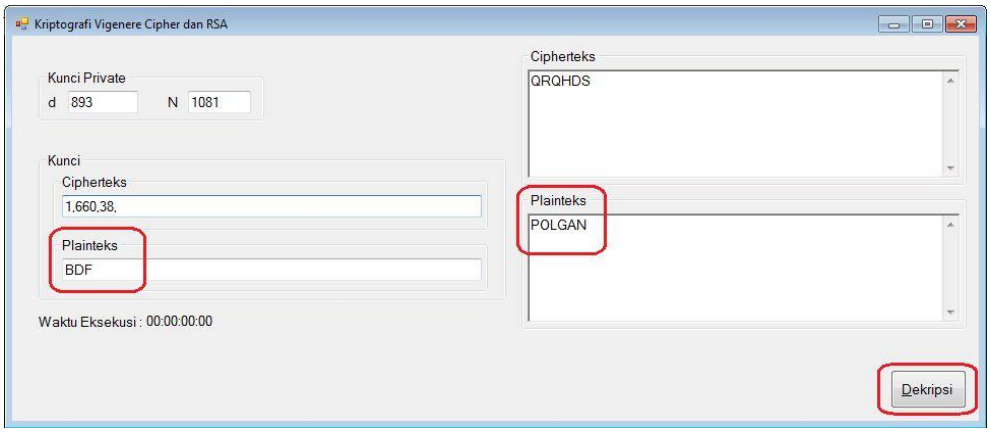

Figure 11. Text Message Decryption Process and Key

The result of the implementation is correct if the message text and the key in the plaint text when encrypted will then be encrypted and will be decrypted again, then the result must be the same as the previous text message and key.

4.2. Discussion

In this discussion, we will simulate some text messages and keys to get a graph for the time required for encryption and decryption.

In this research, it is practiced that the key given with the **POLGAN** character and the length of the text message character is different from the lowest to the highest, it will be

seen. the time it takes to perform the encryption and decryption process varies with character length, see table 1

Table 1. Encryption and Decryption Processing Time with the Same Key but Different Text Messages Total Characters

PROSES ENKRIPSI-DEKRIPSI	KUNCI (POLGAN)	PESAN (KARAKTER)	WAKTU (milidetik)	
			ENKRIPSI	DEKRIPSI
1	6	1.058	1	1
2	6	2.906	2	2
3	6	4.236	3	3
4	6	8.448	8	6
5	6	11.880	18	13
6	6	23.760	56	46
7	6	31.920	97	88
8	6	37.620	153	120
9	6	47.520	251	196
10	6	59.400	424	335

If we want to see the graph from table 1. above, a graph will be generated with the time required for the encryption and decryption process as shown in Figure 12. and 13.

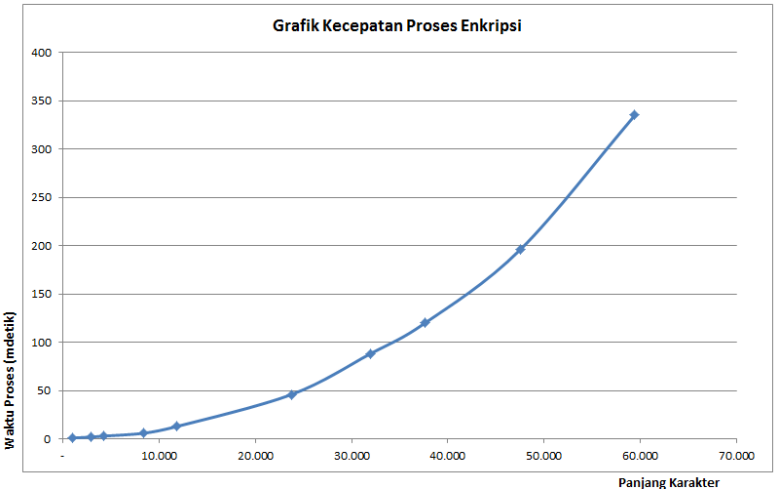

Figure 12. Graph of Time Required in the Process of Encrypting Text Messages and Keys

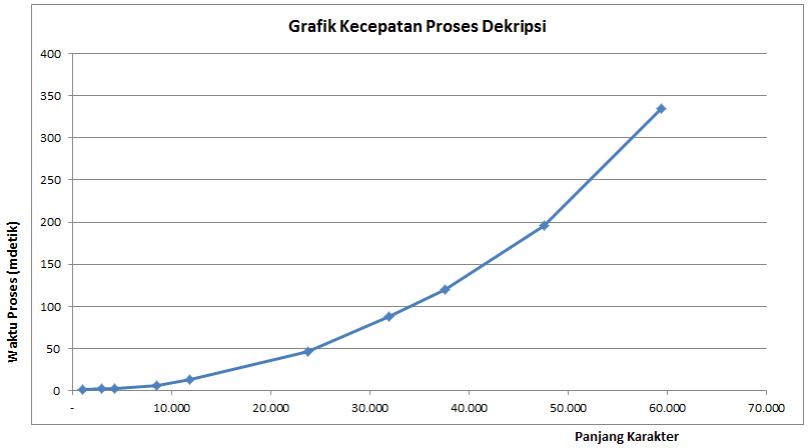

Figure 13. Graph of Time Required in the Process of Text Message Decryption and Key

In the graphs in Figures 12 and 13. We can see that the time required for the encryption and decryption process depends on the variety of text messages given, the greater the number of text characters given, the greater the time required for the encryption and decryption process. Then the time required for the encryption process is longer than the decryption process. Then in this research it is also practiced with a different case where the length of the text message characters is the same as many as 54,400 characters, while the key given is different by taking the example of a simulated GANESHA key from the smallest letter to the largest letter, see table 2.

Table 2. The Encryption and Decryption Processing Time with Both Keys Varies But Text Messages are Same Length

KUNCI VIGENER (Jumlah Karakter)		PESAN (Jumlah Karakter)	WAKTU (milidetik)	
			ENKRIPSI	DEKRIPSI
G	1	59.400	463	468
GA	2	59.400	459	478
GAN	3	59.400	433	391
GANE	4	59.400	454	420
GANES	5	59.400	420	384
GANESH	6	59.400	449	421
GANESHA	7	59.400	439	401

If we want to see the graph from table 2. above, you will see a graph with the time required for the encryption and decryption process as shown in Figure 14. and 15.

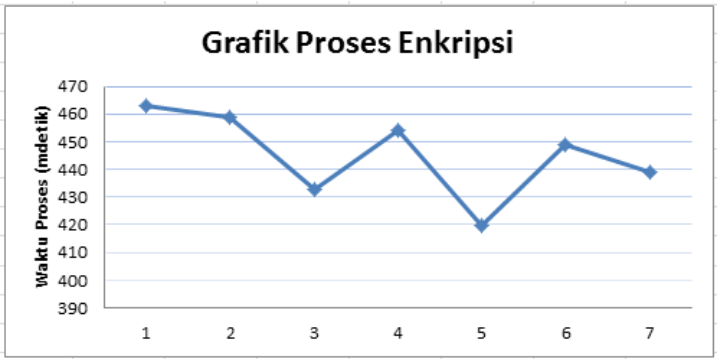

Figure 14. Graph of Time Required in the Process of Encrypting Text Messages and Keys

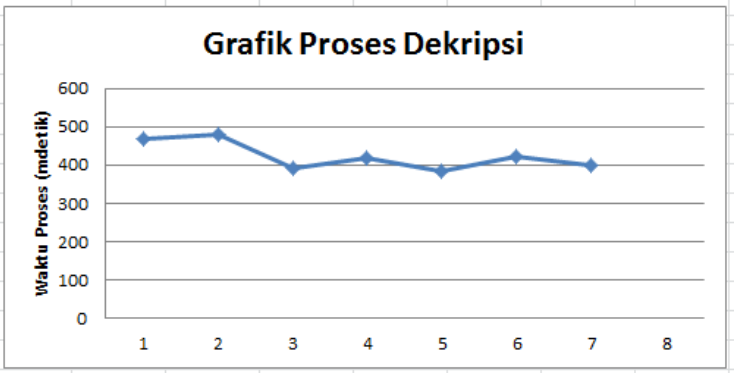

Figure 15. Graph of Time Required in the Process of Text Message Decryption and Key

In the graphs in Figures 14 and 15. We can see that the time required to perform the encryption and decryption process varies, it will produce varying speeds in the encryption process and in the decryption process with varying times the increase is unstable.

5. Conclusion

Based on the discussion and calculation process in the analysis above, the following conclusions can be drawn:

a) Text message processing time is affected by the character length of the key and text message. The longer the key given, the longer the encryption process takes place.
b) Data security includes being on the side of the lock, the longer the key character the longer it takes to crack it.
c) The encryption process time takes longer when compared to the time of the decryption process, this is because in the encryption process there is a key formation process in the Vigenera Cipher and RSA as well as the encryption process both in Vigenere Cipher, Vigenère Cipher and RSA, all of which require a fairly complex calculation. Different from the decryption process which focuses only on the decryption,
d) The hybrid crtptosystem method by combining the Vigenere Cipher algorithm and RSA can speed up the encryption and decryption process and increase better security on text messages.

References

[1] D. Rachmawati, A. Sharif, Jaysilen, dan M. A. Budiman, "Hybrid Cryptosystem Using Tiny Encryption Algorithm and LUC Algorithm," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 300, no. 1, 2018.
[2] R. Romindo dan J. Jamaludin, "Sistem Pendukung Keputusan Menggunakan Metode ANP Untuk Pemilihan Toko Daring Terbaik di Politeknik Ganesha," *REMIK (Riset dan E-Jurnal Manaj. Inform. Komputer)*, vol. 4, no. 1, hal. 83, 2019.
[3] M. Rinaldi, *Kriptografi*. Bandung: Informatika, 2006.
[4] R. K. Gupta dan P. Singh, "A New Way to Design and Implementation of Hybrid Crypto System for Security of the Information in Public Network," vol. 3, no. 8, hal. 108–115, 2013.
[5] Jamaludin, "Rancang Bangun Kombinasi Chaisar Cipher dan Vigenere Cipher Dalam Pengembangan Algoritma Kriptografi Klasik," *Semin. Nas. Teknol. Inf.*, no. The Future of Computer Vision, hal. 234–243, 2017.
[6] D. Ariyus, *Pengantar ilmu kriptografi: teori analisis & implementasi*. Yogyakarta: Penerbit ANDI, 2008.
[7] Rifki Sadikin, *Kriptografi untuk keamanan jaringan*. Yogyakarta: Penerbit ANDI, 2012.
[8] L. B. Rivera, J. A. Bay, E. R. Arboleda, M. R. Pereña, dan R. M. Dellosa, "Hybrid Cryptosystem Using RSA , DSA , Elgamal , And AES," vol. 8, no. 10, hal. 1777–1781, 2019.
[9] A. A. Rakhman dan A. W. Kurniawan, "Implementasi Algoritma Kriptografi Rivest Shamir Adleman (Rsa) Dan Vigenere Cipher Pada Gambar Bitmap 8 Bit," *Techno.COM*, vol. 14, no. 2, hal. 122–134, ISSN:2356-2579, 2015.
[10] J. Herdyka, "Peranan Pemerintan dan Ikatan Profesi dalam Keselamatan Kerja," Universitas Gunadarma, 2018.