Available online at: http://proceeding.rsfpress.com/index.php/ic-smart/index
Proceeding on International Conference of Science Management Art Research Technology (IC-SMART)
Volume 1 Number 1 (2020): 89-100

Hybrid Cryptosystem Analysis by Using The Combination of Vigenere Cipher and RSA for Text Security

Jamaludin, Romindo

Information Technology, Politeknik Ganesha Medan, Indonesia;
E-mail address jamaludinmedan@gmail.com; E-mail address romindo4@gmail.com

Abstract

The development of Information and Communication Technology (ICT) brought many benefits to the needs of human life, especially the needs for the information which is increasingly obtained easily. This is in line with the need for information security from parties who want to get important data so that it can harm the owner of the source data. One of the data safeguards used is cryptography. Once the importance of data security, almost all activities of human life cannot be separated from cryptography. According to the key used, cryptography can be divided into two, namely: symmetric cryptography and asymmetric cryptography, which has its own advantages and disadvantages. The objective of this research is to analyze through the calculation results so that they 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 coding process in this research uses two cryptographic algorithms. They are the Vigenere Cipher algorithm as an example of a symmetrical algorithm and the RSA (Rivest Shamir Adleman) algorithm, which is an example of an asymmetric algorithm. The result of the research on the calculation shows that there is increased security in the encryption because there will be two encodings, namely the coding of the messages by the Vigenere Cipher cryptographic algorithm and key coding by the RSA cryptographic algorithm

Keywords: Cryptography, Hybrid Cryptosystem, Vegenere Cipher, RSA

I. INTRODUCTION

There are several arts of securing data through a channel, one of which is cryptography. 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 protect the confidentiality of the information contained in the data so that unauthorized parties cannot find out the information. Cryptographic algorithm designers are called cryptographers. (Romindo, 2018)

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. A 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 resolved, but the encryption and decryption process of data is generally slower because encryption and decryption use large numbers and involve large power operations and the ciphertext size is larger than plaintext. (Rinaldi, 2006)

To overcome the weaknesses of these two types of cryptography, a hybrid cryptosystem coding method is used. A 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.(Gupta dan Singh, 2013)

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 it will produce a high level of security but fast in the encryption and decryption process.(Jamaludin, 2019)

II. LITERATURE REVIEW

The purpose of this research is to analyze through the calculation results 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. Hybrid cryptography is often used because it takes advantage of the advantages of speed of data processing by symmetric algorithms and the ease of key transfer using an asymmetric algorithm. This results in increased speed without compromising comfort or safety.

The hybrid cryptographic algorithm is an algorithm that utilizes 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 symmetrical keys. (Ariyus, 2008)

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 the 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(Rinaldi, 2006). However, Vigenère Cipher cryptography is no longer secure now. Several methods to attack the Vigenère Cipher cipher have revealed this code weakness. The cipher analysis proposed by Friedrich Kasiski, called the Kasiski test in 1963 of the Vigenère Cipher cipher, could unravel the length of the key and further unravel the key value of the Vigenère Cipher.(Rifki Sadikin, 2012). While the selection of the RSA algorithm as 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 chords, two large random prime numbers are selected. (Ariyus, 2008)

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 distinguish it from the research that is

being carried out. In this case, two previous national research journals related to the author's research are included. These journals include:

1. The research entitled "Implementation of Rivest Shamir Adleman (RSA) and Vigenere Cipher Cryptographic Algorithms in 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 cryptography 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 images. 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 of each pixel using the RSA cryptographic algorithm first, then followed by using the Vigenere Cipher algorithm. Whereas the decryption stage is carried out using the VigenereCipher algorithm first then using the RSA cryptographic algorithm..(Rakhman dan Kurniawan, 2015)

The advantage of this journal theme 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 Cipher cryptography, and the encryption and key decryption process in key cryptography occur in cryptography.

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. (Gunawan, 2018)

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 Cipher cryptography, and the encryption and key decryption process in key cryptography occurs in cryptography RSA.

III. RESEARCH METHODOLOGY

The encryption 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 can be seen in figure 3.1.

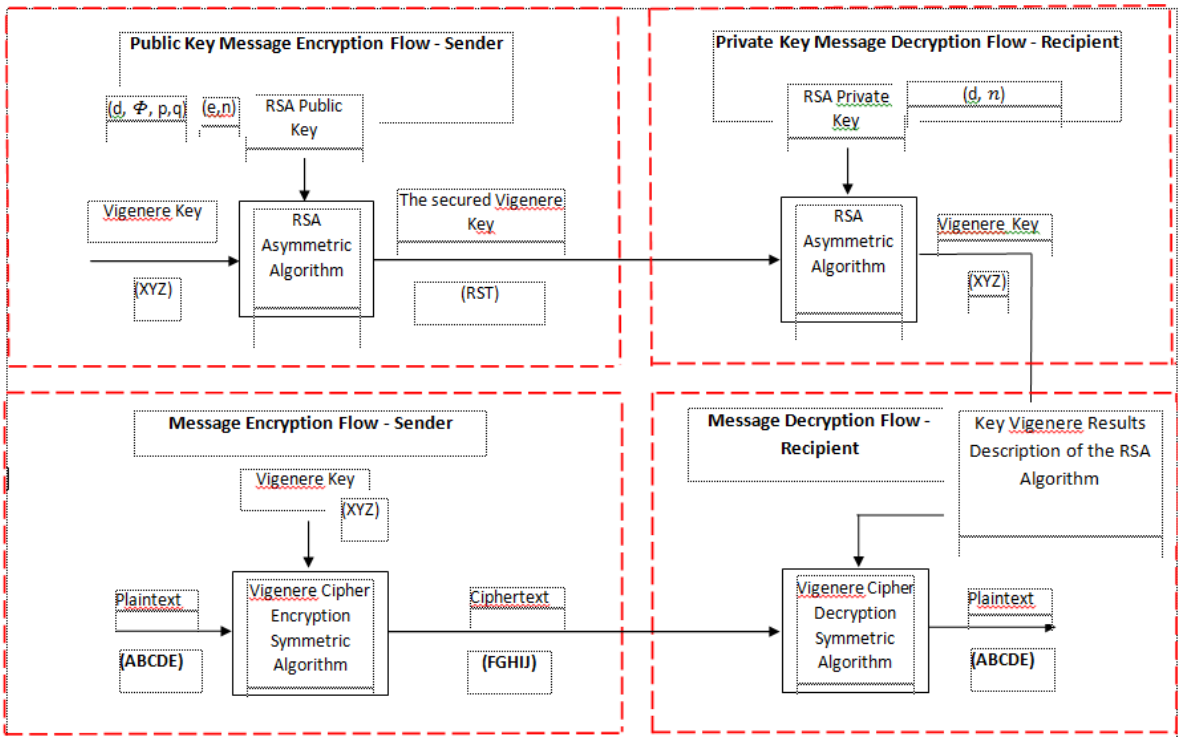

Figure 3.1. Schematic diagram of the combination of Vigenère Cipher and RSA using the Hybrid Cryptosystem method

To simplify the encryption and decryption process in the Hybrid Cryptosystem algorithm development and key generation, it is divided into four 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 3.2.

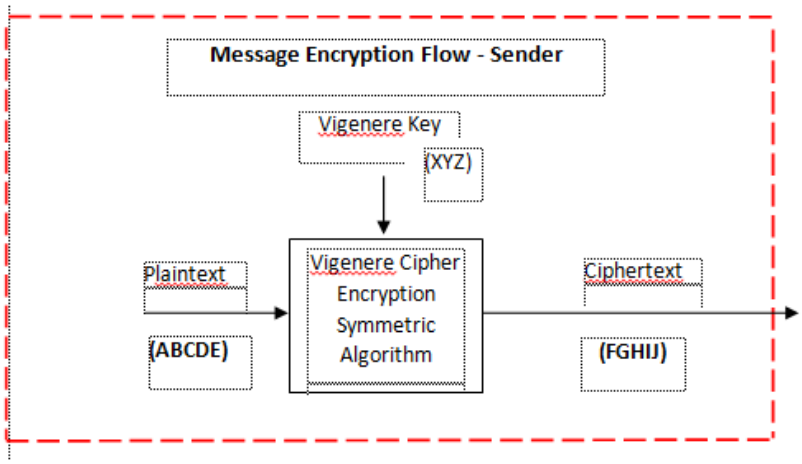

Figure 3.2. The process of encrypting the sender's message

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 3.3.

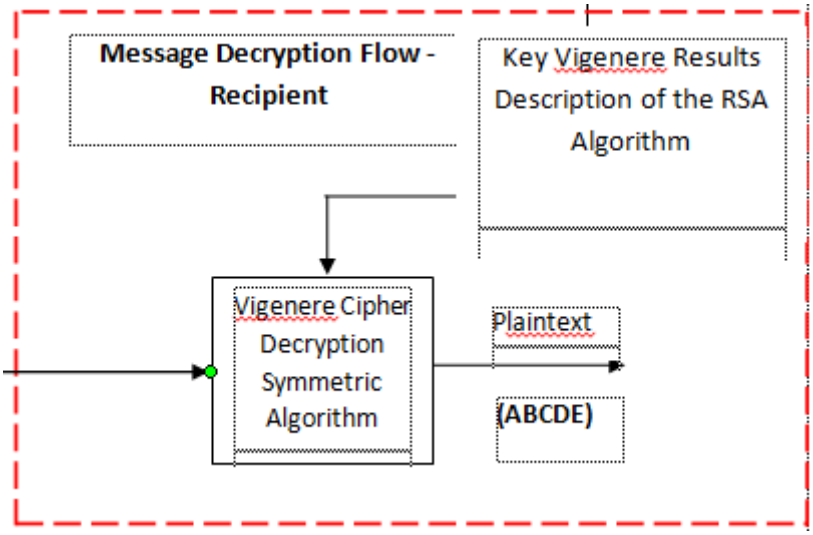

Figure 3.3. Recipient message decryption process

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

he 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 3.4 .:

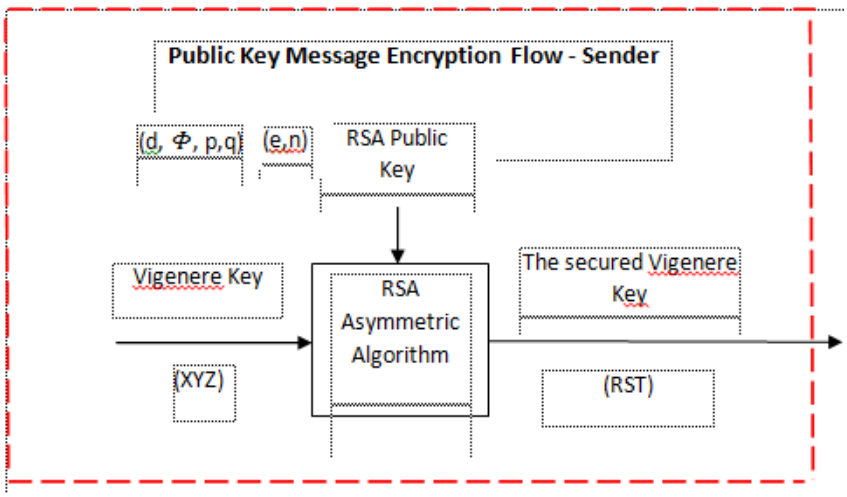

Figure 3.4. The process of encrypting the sender's public key

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, and 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 3.5.

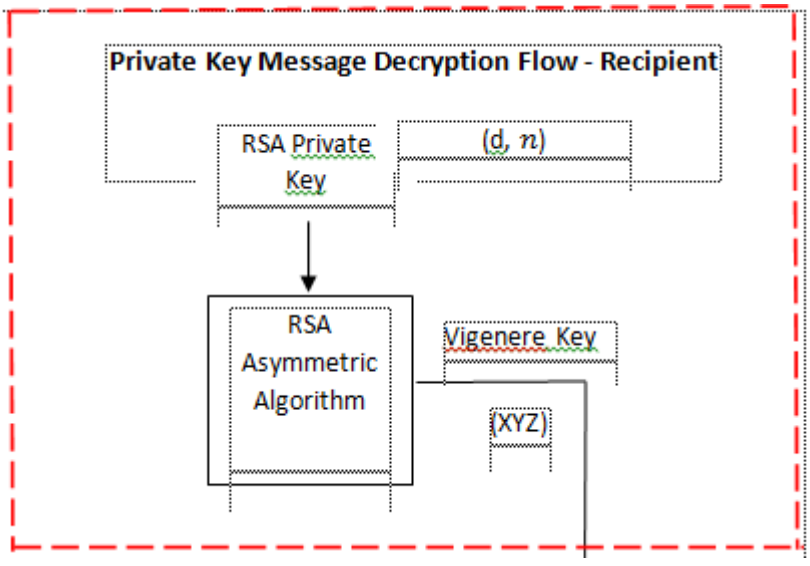

Figure 3.5. The process of decrypting the recipient's private key

.

IV. FINDING AND DISCUSSION

In this discussion, it is necessary to calculate the encryption and decryption process of the combination of the Vigenère Cipher and RSA algorithms. The results of the correct calculations form the basis for creating software programs.
For example, the word POLGAN is used for plaintext, and the key used is BDF. The results of this calculation are correct. When the message in the plain text is encrypted, it will be encoded and will be decrypted again, like plaint text. Also, the key will be encrypted and will be re-decrypted as in the previous message encryption and decryption process.

4.1. Text Message Encryption Process - Sender Using Vegenere Cipher Cryptography

The steps in the calculation of the text message encryption process - the sender using the Vegenére Cipher Cryptography are as follows:

1. Plaint Text: **POLGAN**

P	O	L	G	A	N
15	14	11	6	0	13
P_1	P_2	P_3	P_4	P_5	P_6

2. Vigenère Key : **BDF**

K_1	K_2	K_3	K_4	K_5	K_6
B	D	F	B	D	F
1	3	5	1	3	5

C1 = (P1. + K1) mod 26
= (15 + 1) mod 26
= 16 mod 26 = 16 = **Q**

C2 = (P.2. + K2) mod 26
= (14 + 3) mod 26
= 17 mod 26 = 17 = **R**

C3 = (P3. + K3) mod 26
= (11 + 5) mod 26
= 16 mod 26 = 16 = **Q**

C4 = (P4. + K4) mod 26
= (6 + 1) mod 26
= 7 mod 26 = 7 = **H**

C5 = (P5. + K5) mod 26
= (0 + 3) mod 26
= 3 mod 26 = 3 = **D**

C6 = (P6. + K6) mod 26
= (13 + 5) mod 26
= 18 mod 26 = 18 = **S**

So result of the ciphertext encryption :

Q	R	Q	H	D	S
16	17	16	7	3	18
$C_{1.}$	$C_{2.}$	$C_{3.}$	$C_{4.}$	$C_{5.}$	$C_{6.}$

So the result of Vigenère Chipper algorithm's message-encryption is ciphertext2 = **QRQHDS**

4.2. Decryption Process Text Message - Recipient Using Cryptography Vegenére Cipher

The steps in the calculation of the text message decryption process - the recipient using the Vegenére Cipher Cryptography are as follows:

1. Ciphertext: **QRQHDS**

Q	R	Q	H	D	S
16	17	16	7	3	18
C_1	$C_{2.}$	C_3	$C_{4.}$	$C_{5.}$	$C_{6.}$

2. Vigenère Key: **BDF**

K_1	K_2	K_3	K_4	K_5	K_6
B	D	F	B	D	F
1	3.	5.	1.	3.	5.

D1 = (C1. - K1) mod 26
= (16 - 1) mod 26
= 15 mod 26 = 15 = **P**

D2 = (C.2. - K2) mod 26
= (17 - 3) mod 26
= 14 mod 26 = 14 = **O**

D3 = (C3. - K3) mod 26
= (16 - 5) mod 26
= 11 mod 26 = 11 = **L**

D4 = (C4 - K4) mod 26
= (7 - 1) mod 26
= 6 mod 26 = 6 = **G**

D5 = (C5. - K5) mod 26

= (3 - 3) mod 26
= 0 mod 26 = 0 = **A**

D6 = (C6. - K6) mod 26
= (18 - 5) mod 26
= 13 mod 26 = 13 = **N**

So the results of the plaint text decryption process :

P	O	L	G	A	N
15	14	11	6	0	13
D_1	D_2	D_3	D_4	D_5	D_6

So the message decryption of Vigenère's algorithm is ciphertext1 = **POLGAN**

4.3. Key Encryption Process - Sender Using RSA Cryptography

The steps in the calculation of the key message decryption process - the sender using RSA cryptography are as follows:

1. Take two very large prime numbers p and q
   For example : P = **47** and Q = **23**

2. Count N = P * Q
   N = 47 * 23
   N = 1081
3. Count Φ (n) = (P-1) (Q-1)
   Φ (n) = (47-1) (23-1)
   Φ (n) = 1012
4. Randomly retrieve the encryption key e with the following conditions
   - $1 < e < \Phi(n)$
   - e relatively prime to Φ (n), so GCD(e, Φ (n))=1

   An example that satisfies e = 17

   GCD(e, Φ (n)) = 1
   GCD(17,1012) = 1

   1012 mod 17 = 9
   17 mod 9 = 8
   9 mod 8 = 1
   8 mod 1 = 0
   So that e = 17 fulfills the requirement above

5 Calculate the decryption key d :

$$e * d \bmod \Phi(n) = 1$$

d	e. d mod $\Phi(n)$ = 1 17.d. mod 1012 = 1
1	17.1.mod 1012 = 17

2	17.2. mod 1012 = 34
3	17.3. mod 1012 = 51
. . .	. . .
893	17.893 mod 1012 = 1

After calculated that meets the requirements e * d mod Φ (n) = 1, when d counts to 893, so d = 893

6. Publish the public key pair = (e, N)
   Publish the public key pair = **(17, 1081)**
7. Save private key pair = (d, N)
   Save private key pair = **(893,1081)**

Sender:

8. Obtain the recipient's public key pair
   Public key = (e,N)= (17,1081)
9. Determine the key to be encrypted, in the case that will be encrypted is the BDF Vigenere Cipher key, which is the input for the RSA Asymmetric Algorithm

Vegenere cipher key encryption : BDF (1,3,5)

10. Encrypt the Vigenere key with the formula: C = me mod N, so that

m=1 C = m^e mod N
= 117 mod 1081 = **1**

m=3; C = m^e mod N
= 317 mod 1081 = **660**

m=5; C = me mod N
= 517 mod 1081 = **38**

So the results of the Vegenere Cipher key encryption: (**1,660, 38**)

11. Send the Vegenere Cipher C key to the recipient
12. Receive the Vegenere Cipher C key from the sender

4.4. Key Decryption Process - Receiver Using RSA Cryptography

Vegenere Cipher key decryption

13. Decrypt the results of the Vegenere Cipher key encryption with the formula: **$m = C^d$ mod N**, so that

m = C^d mon N
= 1^{893} mod 1081 = **1**
m = C^d mon N
= 660^{893} mod 1081 = **3**
m = C^d mon N
= 38^{893} mod 1081 = **5**

So the decryption of the RSA receiver key is (**1,3,5**) when converted the same as **BDF.**

So that after calculating the encryption and decryption process, the combination of the Vegenere Cipher Algorithm and RSA can be mapped to the schematic diagram as shown in figure 4.1.

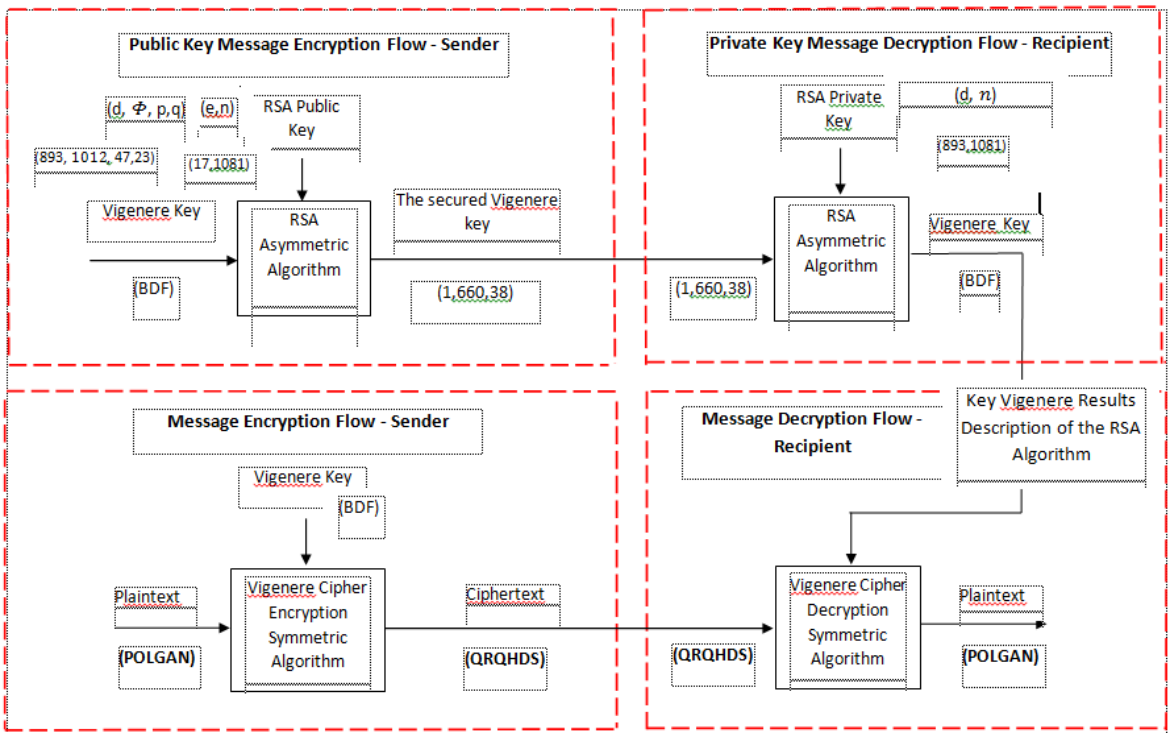

Figure 4.1.Schematic diagram of the combination of Vigenère Cipher and RSA using the Hybrid Cryptosystem method

V. CONCLUSION AND FURTHER RESEARCH

Based on the discussion and calculation process in the analysis above, the following conclusions can be drawn: The Vigenère Cipher and RSA algorithms can be combined so that later the combination will produce an algorithm that has a high level of data security and is fast in the encryption process, both encryption and decryption. Then, the results of this research can be applied in software programs so that they can be used to strengthen text security.

REFERENCES

Ariyus, D. (2008) Pengantar ilmu kriptografi: teori analisis & implementasi. Yogyakarta: ANDI. Retrieved at: https://books.google.co.id/books?id=3SSTJONEmX0C&printsec=frontcover&hl=id#v=onepage&q&f=false.

Gunawan, I. (2018) "Kombinasi algoritma Caesar cipher dan algoritma RSA untuk pengamanan file dokumen dan pesan teks," Infotekjar, 2(1), pp. 124–129.

Gupta, R. K. dan Singh, P. (2013) "A New Way to Design and Implementation of Hybrid Crypto System for Security of the Information in Public Network," 3(8), pp. 108–115.

Jamaludin (2019) "Rancang Bangun Kombinasi Hill Cipher dan RSA Menggunakan Metode Hybrid Cryptosystem," Sinkron, 2(April 2018). Retrieved at: https://jurnal.polgan.ac.id/index.php/sinkron/article/view/139.

Rakhman, A. A. dan Kurniawan, A. W. (2015) "Implementasi Algoritma Kriptografi Rivest Shamir Adleman (Rsa) Dan Vigenere Cipher Pada Gambar Bitmap 8 Bit," Techno.COM, 14(2), pp. 122–134, ISSN:2356-2579. Retrieved at: http://publikasi.dinus.ac.id/index.php/technoc/article/view/886/657.

Rifki Sadikin (2012) Kriptografi untuk keamanan jaringan. Yogyakarta: Penerbit ANDI.

Rinaldi, M. (2006) Kriptografi. Bandung: Informatika. Retrieved at: https://scholar.google.com/scholar?hl=th&as_sdt=0,5&cluster=16551445928354209324.

Romindo, R. (2018) "Analisa Perbandingan Algoritma Monoalphabetic Cipher Dengan Algoritma One Time Pad Sebagai Pengamanan Pesan Teks," Sinkron, 2(April 2018). Retrieved at: http://jurnal.polgan.ac.id/index.php/sinkron/article/view/123..