Collaboration of RSA Algorithm Using EM2B Key with Word Auto Key Encryption Cryptography Method in Encryption of SQL Plaintext Database

Elwin Yunith Purba¹, Syahril Efendi¹, Pahala Sirait², Poltak Sihombing¹
¹Department of Informatics Engineering, Universitas Sumatera Utara, Medan Indonesia
²Department of Informatics Engineering, Mikroskil, Medan Indonesia.

E-mail: elwinpurba.manorsa@gmail.com

Abstract. RSA algorithm is a modern cryptographic algorithm and is often used for data security, and until now no one has been able to solve it. This algorithm uses two keys, public key and private key, the degree of difficulty of this algorithm lies in the factorization of large prime numbers. EM2B key algorithm function is to change the primary key become a new key into ASCII characters. This algorithm has the increament key algorithm function to change the length of the key characters are same as the plaintext. The Wake method is a stream cipher algorithm uses a 128 bit key and a 256 X 32 bit table. The strength of the RSA algorithm is the bit length used, and the strength of the WAKE method also lies in the bit length used and many rotation that occur. While the strength of the EM2B key algorithm lies in the increament key. After testing, the combination of three algorithms consists of the RSA algorithm using the EM2B key and WAKE method and a combination of two algorithms with WAKE method using the EM2B key, the encryption results are better and safer than using only one WAKE algorithm.

1. Introduction

The progress of information technology cannot be prevented anymore, and the development of information technology progress has changed human life. The important data is very important to maintain the confidentiality of the information, especially information that contains confidential data that should not be known by unauthorized people [1]. The capabilities possessed by a computer device today are undoubted, this is evidenced by the high speed accuracy in completing a job. Besides the advantages that can be obtained from the use of computers, the most important thing to consider is part of its security, if the information / data stored on the computer is damaged due to interference from hackers, it can result in heavy losses as well. Encryption is a standard method that is always used to scramble information data, so that information cannot be read by other people who are not authorized [2].

In J D Howard's book, "An Analysis of security incidents on the internet" stated that Computer security is an action to prevent attacks from people who are not entitled to a data or who wants to access the network by someone who is not responsible [14]. In 2016 data hacking occurred such as Ransomware and was considered a cyber threat to the business world, and many countries were affected by Ransomware such as Britain, Singapore and others. After that there was a DDoS attack the
data on the server in the United States, and there were 412 million user accounts hacked by the DDoS attack [3]. If condition of a computer that is not properly secured, especially its database, will be a great opportunity for hackers to get into computer access and steal all the data they want [4].

The security of an information or data is very important always to be secured, in order to reduce the risk that occurs and add to the benefits obtained from our hard working [11]. Database threats often occur, such as personal data or company data and must be given special attention to secure the database, because many others try to steal even damage our data or company so that it can be damaged by other people even be taken and used our data, business data or organization data for something that is not good. Therefore, the database must be secured from people who are not entitled to our data. To secure the database there are many models to be developed for database security [12].

In determining a cryptographic algorithm that is used for data system security against the threat of Cryptoanist attacks, speed problems also need to be considered. In this sophisticated era there are many kinds of algorithms regarding asymmetry and symmetry cryptography. If a cryptographic algorithm is considered to be a strong level of security, but the encoding process in implementing the application turns out to be slow, then cryptography will not be an option for cryptographic users. Consideration of the ability and reliability of an algorithm must be prioritized when it comes to computer networks, especially when using client-server-architecture [13].

In this paper I will review how the data encryption process by applying a combination of three algorithm that consist of RSA algorithm uses the EM2B key with WAKE (Word Auto Encryption) cryptography method, and applying a combination of two algorithm that consist of WAKE (Word Auto Encryption) cryptography method uses EM2B key to secure data as much as possible.

2. Literature Review
2.1. Cryptography

The word cryptography comes from the word Cryptos, which means hidden words and Graphen which have the meaning of writing, so the word cryptography can be interpreted as an art or science that examines how data is converted into certain forms that are more specific and difficult to understand by others. Cryptography has the purpose of being able to maintain the confidentiality of information or data that must not be known by others who have no interest in the information or data [5].

The security of a cryptographic algorithm depends on the performance of an algorithm, therefore such algorithms are called limited algorithms. And a limited algorithm is an algorithm used by a certain group of people to guarantee the information or data sent to other people to arrive safely and not be damaged or taken by someone who is not entitled to that information or data [6].

2.2. RSA algorithm

RSA is one of the modern cryptographic algorithms and is still widely developed by researchers in this world. The RSA algorithm was made by three researchers from MIT (Massachusetts Institute of Technology) in 1976. The name RSA stands for the names of the three inventors Rivest, Shamir, and Adleman. The RSA algorithm factoring very large numbers into prime factors. Factoring is done to obtain the private key [7].

The ingredients to state the RSA scheme are the following [6]:

- \( p \) and \( q \) are two prime numbers (Private, chosen)
- \( n = pq \) (Public, calculated)
- \( \varphi(n) = (p - 1)(q - 1) \) (Public, calculated)
- \( e \) (Encryption key), with \( \gcd(\varphi(n), e) = 1; 1 < e < \varphi(n) \) (Public, chosen)
- \( d \) (Decryption key), \( d \) calculated from \( d \equiv e^{-1} \mod \varphi(n) \) (Private, calculated)

The keys were generated as follows:

- Select two prime numbers, \( p \) and \( q \), \( p \neq q \)
- Calculate the product \( n = pq \), The value of \( n \) no need to be kept secret.
Calculate \( \varphi(n) = (p - 1)(q - 1) \).

Select an integer for the public key, say its name \( e \), with \( \gcd(\varphi(n), e) = 1; 1 < e < \varphi(n) \).

Calculate the decryption key, \( d \) through \( ed \equiv 1 \pmod{m} \) or \( d \equiv e^{-1} \mod{\varphi(n)} \).

Public key is consist of \((e, n)\), \(PU = \{e, n\} \).

Private key is consist of \((d, n)\), \(PR = \{d, n\} \).

Plaintext were encrypted as follows:

- Plaintext: \( M < n \)
- Chipertext: \( C \equiv M^e \mod{n} \)

Chipertext were decrypted as follows:

- Chipertext: \( C \)
- Plaintext: \( M \equiv C^d \mod{n} \)

2.3. EM2B Key Algorithm

The EM2B key algorithm is an algorithm that functions to convert the main key into a new key that is converted into ASCII characters. Key algorithm EM2B develop a simple key generator algorithm to encrypt plaintext. The modulus system of adding plaintext with keys becomes an advantage in the speed of the encryption process. The EM2B algorithm also has an increment key algorithm that works when the length of the key is smaller than the length of plaintext, so the Increment key is a method for adding key character length by summing the two previous key characters and modulated with 256 ASCII-based letters. EM2B is the abbreviation name of the inventors of this algorithm, E Mendrova, E Manorsa, and B Yako found in 2017.

This EM2B key algorithm has the following equation [3]:

\[
K_{f} = K_{i} \mod{26} \tag{1}
\]

\[
K_{i[new]} = (K_{i} + K_{f}) \mod{256} \tag{2}
\]

Explanation:

a. \( K_{i} \) = The Main Key,

b. \( K_{f} \) = The Main Key do mod with 26 \( (K_{i} \mod{26}) \),

c. \( K_{i[new]} \) = New Key Generated.

The scheme to explain the process of the EM2B Key and Increment Key algorithms can be seen in the following Figure 1:

![Figure 1. Process of the EM2B Key Algorithm (Source: E Mendrova  E Manorsa and B Yako 2017).](image-url)
And for the Increment Key algorithm process:

\[ IncK_i = \left( K_{i[\text{max}]} + K_{i[\text{max-1}]} \right) \mod 256 \]  (3)

Explanation:

- \( IncK_i \) = Increment Key,
- \( K_{i[\text{max}]} \) = The last Key index in ASCII,
- \( K_{i[\text{max-1}]} \) = Previous Key Index in the key.

Figure 2. Increment Key Process (Source: E Mendrova E Manorsa and B Yako 2017).

Another supporting algorithm is Vigenere Cipher. This type of encryption algorithm is well known for being easy to understand and implement. Techniques to produce ciphertext can be done using the substitution of numbers and square vigenère [9]. Character letters used in vigenere cipher are A, B, C, ..., Z and equated with the numbers 0, 1, 2, ..., 25. The encryption process is done by writing the key repeatedly. Key writing is done repeatedly and be held until each character in the message has a pair of characters from the key. Then the characters in the message are encrypting using the Caesar cipher algorithm with the paired key value [8]. The encryption process can be calculated by the following equation [10]:

\[ E_i = (P_i + K_i) \mod 26 \]  (4)

where \( E_i \), \( P_i \) and \( K_i \) are encrypted characters, Data characters and key characters. While the decryption process can use the following equation:

\[ D_i = (C_i - K_i) \mod 26 \]  (5)

with \( D_i \) is a decrypted character, \( C_i \) is a ciphertext or password character, \( K_i \) is a key character.

2.4 WAKE (Word Auto Key Encryption) Method

The WAKE method is one of the stream cipher algorithms where it has been used commercially for a long time. WAKE stands for Word Auto Key Encryption. This method was invented by D J Wheeler in 1993. The WAKE method uses a 128 bit key and a 256 x 32 bit table. In this WAKE algorithm, this method uses OR, AND, XOR and Shift Right operations. Dr. Solomon has used this WAKE method on his latest Anti Virus.

The main process of WAKE consists of [10]:

- Key formation process.
- The process of forming an S-Box table (Substitution Box).
The Process of encryption and decryption.

The core of the WAKE method lies in the key formation process by uses 128 bit key and the formation of an S-Box table. The S-Box table of the WAKE method is flexible and varies with each round, if more rounds, the data security is getting better [10].

3. Methodology

In designing a cryptographic algorithm, a maximum accuracy is required. The level of security is the key to the success of the cryptographic algorithm itself. Time efficiency also needs to be considered because if the encryption and decryption process takes a long time, it will be bad for encrypting data on a large scale [15]. Broadly speaking the process of encryption and decryption on the implementation of the RSA algorithm with the EM2B Key and the WAKE (Word Auto Key Encryption) method in encrypting data can be seen through the following blog diagram.

![Encryption and Decryption Process With RSA + EM2B + WAKE](image)

**Figure 3.** Encryption and Decryption Process With RSA + EM2B + WAKE.

In this research, the RSA Algorithm uses the EM2B Key and the WAKE method cryptographic algorithm to improve the security of encrypted data. It is hoped that the EM2B key and the ability of the RSA algorithm, can be a combination of algorithms to encrypt keys and collaborate with WAKE methods in encrypting plaintext will make the data very difficult to solve. Therefore it is necessary to analyze each algorithm among others are the RSA algorithm, the EM2B key algorithm and the WAKE method used to encrypt data.

Analysis of the RSA Algorithm can be seen as follows:

A. Take randomly two large and different primes, but the size of both or the number of digits in the base of numbers used should be the same.

B. Calculate the modulus and Euler’s Totient function $\varphi(n)$ by the formula: $n = pq$

   \[
   \varphi(n) = (p - 1)(q - 1)
   \]

   with:

   $n$ modulus (public key)
   $p$ and $q$ = Two primes generated randomly.

C. Select an integer $e$ such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$ where:

   $l$ = Integer number,
   $e$ = Public Key (Encryption Key),
   $gcd$ = Greatest common divisor.

D. Calculate the integer value $d$ where $1 < d < \varphi(n)$ such as:
\[ d = e - 1 \mod \phi(n) \text{ or } ed = 1 \mod \phi(n) \],
where:
\[ d = \text{Private Key (Decryption Key)}. \]

E. Create a table to present each character.

F. The plaintext (encrypted text) is encrypted with numbers corresponding to the table formed by process of \( e \) and \( M \) will be obtained which is a collection of numbers from the plaintext, then the set of numbers is blocked every 4 numbers into \( m_1, m_2, m_3, \ldots m_n \). The encryption process is done per block and each block of the encryption formula is:
\[ c_1 = m_1 e \pmod{n}, c_2 = m_2 e \pmod{n}, \ldots, c_n = m_n e \pmod{n}, \]
where \( c_1, c_2, c_3, \ldots c_n \).

G. The decryption process is done by using logic like step F by performing an inverse calculation, ie:
\[ m_1 = c_1 d \pmod{n}, m_2 = c_2 d \pmod{n}, \ldots, m_n = c_n d \pmod{n}, \]

To improve the security of RSA algorithm, then specified security key in the form of private key password, public key and modulo generated from two prime numbers. This key will continue to be used by the sender and recipient of the data in encrypting and decrypting the data. If the security key password by the system owner is deemed to be insecure, then both parties immediately inform it to be changed altogether. This security key view consists of:

Analysis of EM2B algorithm as follows:
A. Specify some words used as the primary key for encrypting datas. Key is given a symbol with \( K_i \)
where \( K_i = K_1, K_2, K_3, \ldots K_n \).

B. The key is converted into decimal ASCII numbers.

C. Determine the modulus value of 26 of each key character that has been converted into decimal places, \( K_i = K_i \mod 26 \).

D. Add \( K_i \) with \( K_j \) then modulated with 256 and generate a new key \( K_{i[new]} \) which is converted in decimal ASCII characters.

In the EM2B Key algorithm, the key we choose does not must have the same character length as plaintext. Plaintext may consist of several sentences and even paragraphs. The key will adjust the length of its character with plaintext by using the increment key algorithm already stored in it. The performance analysis of the increment key algorithm can be seen below:
A. The maximum character index is summed with the previous character index \( K_{i[\max]} + K_{i[\max-1]} \),
and generate a new key character index \( K_{i[new]} \).

B. The new key index \( K_{i[new]} \) becomes the maximum key index, then added again to the previous key index.

C. This looping step will stop if the maximum index of the key is equal to the plaintext maximum index \( K_{i[\max]} = P_{i[\max]} \).

The analysis of the WAKE method cryptographic algorithm is as follows:
1. Determine yourself or generate key formation that is as many as n-rotation.
   Use function \( M(X,Y) = (X + Y) \gg 8 \text{ XOR } T[ (X + Y) \text{ AND } 255 ] \).
2. The input key will be divided into 4 parts and set to the initial values of variables \( A_0, B_0, C_0 \) and \( D_0 \).
3. The above variable values will be processed through the following steps [10]:
   a. \( A_{i+1} = M(A_i, D_i) \)
   b. \( B_{i+1} = M(B_i, A_{i+1}) \)
   c. \( C_{i+1} = M(C_i, B_{i+1}) \)
   d. \( D_{i+1} = M(D_i, C_{i+1}) \)
The value of $D_i$ is the value of the $K_i$ key.
- Enter the above process into Functions $M(X, Y) = (X + Y) \gg 8 \times O R T[(X + Y) \text{ AND } 255]$. 

4. Form an S-Box table with the following steps:

a. Initialize value $TT[0] \ldots TT[7]$:
   - $TT[0] : 726a8f3b (\text{in hexadecimal})$
   - $TT[1] : e69a3b5c (\text{in hexadecimal})$
   - $TT[2] : d3c71fe5 (\text{in hexadecimal})$
   - $TT[3] : ab3c73d2 (\text{in hexadecimal})$
   - $TT[4] : 4d3a8eb3 (\text{in hexadecimal})$
   - $TT[5] : 0396d6e8 (\text{in hexadecimal})$
   - $TT[6] : 3d4c2f7a (\text{in hexadecimal})$
   - $TT[7] : 9ee27cf3 (\text{in hexadecimal})$

b. Initialize initial values for $TT[0] \ldots TT[3] :$
   - $TT[0] = K[0]$
   - $TT[1] = K[1]$
   - $TT[2] = K[2]$
   - $TT[3] = K[3]$

   generated from keys which are broken into 4 equal parts.

c. For $T[4] \ldots T[255]$, do the following process:
   - $T[n] = T[n - 4] + T[n - 1]$
   - $T[n] = X \gg 3 \times O R T[(X \text{ AND } 7)]$

   generated from keys which are broken into 4 equal parts.

d. For $T[0] \ldots T[22]$, do the following process:
   - $T[n] = T[n + 89]$

The process of implementing the RSA algorithm using the EM2B key with the WAKE method in encrypting messages can be explained by the following steps:

A. A data or plaintext is encrypted using a main key.
B. First the key created is the public key and the private key with the RSA algorithm with the WAKE (Word Auto Key Encryption) method.
C. When the RSA algorithm process with WAKE method is done, the value of the primary key is put together into one block and then separated into several blocks. The value of each block is not greater than the value of $n$ in the RSA key generator.
D. After the block process is done then it is encrypted using the RSA algorithm.
E. Then the encryption results from the RSA algorithm with the WAKE method are ciphertext ($C_i$), and the key encryption result ($E_k$), then is changed by the EM2B key to produce a new ASCII character, by formula:
   - $K_{i[\text{new}]} = (K_i + K_f) \mod 256$
   - $K_f = K_i \mod 26$.
F. If the key length is still smaller than the plaintext length, then the key is processed by the increment key with the formula:
   - $\text{Inc}K_i = (K_i + K_f) \mod 256$.
G. Next do the encryption again, where each ciphertext is added with the key that was encrypted before, after that modulated with 256 to produce a new ciphertext. $C_i = (P_i + K_f) \mod 256$.
H. The process ciphertext from the RSA algorithm with the EM2B key will be XORed using the WAKE method, and the resulting ciphertext is the end result of encryption.
I. To decrypt, do the process from step A to step F, but with a note, step A through step F has been stored in temporary, while in step G to generate plaintext again use the formula $D_i = (C_i - K_f) \mod 256$ and in step 8 XOR returns to produce the same plaintext as the original.
4. Results and Discussion
To explain the methodology above, the author did an experiment on the plaintext sql database consist of 60 databases, but only a few plaintext databases are displayed as a consideration in writing this paper. This research the author did with Visual Basic tools to analyze the process and the results of the combined algorithms, performed by the author are displayed in the table. The results of these experiments can be seen at the applications and tables below:

![Figure 4](image1.png)

**Figure 4.** New Key Formation with RSA + WAKE.

![Figure 5](image2.png)

**Figure 5.** New Key Formation Process.

![Figure 6](image3.png)

**Figure 6.** The Results of forming a new key

![Figure 7](image4.png)

**Figure 7.** S-Box Table Formation Process

![Figure 8](image5.png)

**Figure 8.** Encryption results of 3 combined algorithms

![Figure 9](image6.png)

**Figure 9.** Decryption Results Of 3 Combined Algorithms
In Figure 4, first is done the process of forming a new key by using the RSA algorithm with the WAKE (Word Auto Key Encryption) method, and the process of the algorithm already explained in the methodology chapter. And in Figure 5, it happens the process of forming a new key and the results are in Figure 6. In Figure 7, the S-BOX table process is performed and processed by a combination of the RSA algorithm with the WAKE method. In figure 8 is the result of encryption from the database plaintext by using a combination of three algorithms consists of RSA algorithm using EM2B Key with WAKE method cryptographic algorithm, and in figure 9 is decryption results from a combination of algorithms after the process in figures 4, 5, 6 and 7 are done. The results of all this research process can be seen in the following tables and graphs:

Table 1. Differences between encryption results of RSA + EM2B Key + WAKE and WAKE.

| File Name       | Key Length | Number Of Rotation | Number of characters before encryption | Number of characters after encryption | Character differences between 3 combined algorithms with WAKE |
|-----------------|------------|--------------------|----------------------------------------|--------------------------------------|------------------------------------------------------------|
| wood.sql        | 8          | 25                 | 46.479                                 | 41.612                               | 0.89 %                                                     |
| gedger.sql      | 8          | 30                 | 122.752                                | 117.046                              | 0.42 %                                                     |
| bengkel.sql     | 9          | 45                 | 31.248                                 | 28.045                               | 1.720 %                                                    |
| kewalram.sql    | 9          | 30                 | 106.733                                | 98.491                               | 0.60 %                                                     |
| rezekiakumar.sql| 10         | 7                  | 28.590                                 | 25.685                               | 1.06 %                                                     |
| db_simpeg.sql   | 10         | 54                 | 65.532                                 | 59.007                               | 0.56 %                                                     |
| ascentiutax.sql | 11         | 26                 | 40.587                                 | 37.603                               | 0.94 %                                                     |
| capticu_database.sql | 11      | 24                 | 36.391                                 | 33.276                               | 0.69 %                                                     |
| emoney.sql      | 12         | 46                 | 77.345                                 | 68.648                               | 0.62 %                                                     |
| cp.sql          | 12         | 13                 | 67.731                                 | 60.716                               | 0.25 %                                                     |
| gandhiinn_book.sql | 13  | 30                 | 73.957                                 | 65.511                               | 0.47 %                                                     |
| md5.sql         | 13         | 10                 | 1.314                                  | 1.214                                | 0.14 %                                                     |
| travel.sql      | 14         | 19                 | 8.609                                  | 7.821                                | 0.26 %                                                     |
| stocksummary.sql| 14         | 29                 | 1.878                                  | 1.712                                | 0.67 %                                                     |
| medis.sql       | 15         | 38                 | 7.719                                  | 6.899                                | 0.56 %                                                     |
| scango.sql      | 15         | 42                 | 279.795                                | 250.385                              | 0.94 %                                                     |
| regettacancor2.sql | 16    | 34                 | 201.847                                | 179.649                              | 0.42 %                                                     |
| iss-wp.sql      | 16         | 48                 | 181.439                                | 170.556                              | 0.25 %                                                     |

In Table 1 above is a combination of three algorithms to produce the number of ciphertext after encryption, compared to the number of ciphertexts of encryption results that only use one algorithm with the WAKE (Word Auto Key Encryption) method cryptographic algorithm. Difference in number of characters ciphertext resulting from a combination of three algorithms and one algorithm in this research is 0.42%. In research with a combination of these three algorithms produce a Chipertext character more than just using one WAKE method cryptographic algorithm. This shows that encryption results from a combination of three algorithms, the results of the Chipertexts are more randomly and certainly safer and it will be difficult to hack or taken by someone who is not entitled to our data. Besides that the main key has been encrypted several times among others, first the primary key is encrypted with the RSA algorithm and the WAKE method algorithm, after that it is regenerated with the EM2B Key algorithm use Increment Key, so that the key length are same as the plaintext length, and finally the ciphertext are XORed by the WAKE method algorithm for the end of encryption. Therefore even the new key produced it will be difficult for others to guess. From the table above a graph can be made as shown below:
In this paper, the author also do research on a combination of two algorithms between the WAKE algorithm using the EM2B key with one cryptographic algorithm by WAKE method. The author's goal is to know are there a difference between a combination of three algorithms and a combination of two algorithms when compared against one algorithm that is a WAKE method cryptographic algorithm. The author gets results like the table below.

Table 2. Difference Table Encryption Results with WAKE + EM2B Key and WAKE Method.

| Files Name         | Key Length | Number Of Rotation | Number Of Characters before encryption | Number Of Characters after encryption | Number Of Characters before decryption | Number Of Characters after decryption | Character differences between 2 combined algorithms with WAKE |
|--------------------|------------|--------------------|----------------------------------------|--------------------------------------|---------------------------------------|---------------------------------------|-------------------------------------------------------------|
| griyagaya.sql      | 8          | 26                 | 60.089                                 | 55.683                                | 60.089                                | 55.683                                | 2.88%                                                        |
| gedger.sql         | 8          | 30                 | 122.752                                | 118.837                               | 106.733                               | 101.094                               | 1.51%                                                        |
| kewalram.sql       | 9          | 22                 | 23.015                                 | 20.953                                | 23.015                                | 20.953                                | 1.37%                                                        |
| rezekimakmur.sql   | 10         | 7                  | 28.590                                 | 26.259                                | 28.590                                | 26.259                                | 2.19%                                                        |
| random.sql         | 10         | 22                 | 30.840                                 | 27.281                                | 30.840                                | 27.281                                | 0.39%                                                        |
| ascientitax.sql    | 11         | 26                 | 40.587                                 | 37.663                                | 40.587                                | 37.663                                | 2.33%                                                        |
| captius. database.sql | 11    | 24                 | 36.391                                 | 33.276                                | 36.391                                | 33.276                                | 0.32%                                                        |
| emoney.sql         | 12         | 46                 | 77.345                                 | 74.684                                | 77.345                                | 74.684                                | 4.66%                                                        |
| snapnap.sql        | 12         | 47                 | 7.560                                  | 6.833                                 | 7.560                                  | 6.833                                 | 1.27%                                                        |
| gandhiin_book.sql  | 13         | 30                 | 73.957                                 | 66.511                                | 73.957                                 | 66.511                                | 0.87%                                                        |
| gmltestari.sql     | 13         | 44                 | 252.356                                | 237.621                               | 252.356                                | 237.621                               | 1.05%                                                        |
| stocksummary.sql   | 14         | 29                 | 1.878                                  | 1.712                                 | 1.878                                  | 1.712                                 | 2.56%                                                        |
| medis.sql          | 15         | 38                 | 7.067                                  | 6.989                                 | 7.067                                  | 6.989                                 | 0.61%                                                        |
| scanguard.sql      | 15         | 42                 | 279.795                                | 279.795                               | 279.795                                | 279.795                               | 0.52%                                                        |
| access.sql         | 16         | 29                 | 27.612                                 | 24.858                                | 27.612                                 | 24.858                                | 0.04%                                                        |
| iss-wp.sql         | 16         | 48                 | 181.439                                | 170.556                               | 181.439                                | 170.556                               | 0.41%                                                        |

| Total Characters   | 70.098     | 69.170              | 1.04%                                  |                                      |                                       |                                       |                                                              |

In Table 2 above there are differences number of characters the result of encryption with the WAKE method cryptographic algorithm uses EM2B key when compared to using only the WAKE cryptographic algorithm. And the difference in the number of characters the average is 1.04%, this signifies that result of encryption in the form of ciphertext which produced from combined cryptographic algorithm with the WAKE method using the EM2B key, the ciphertext is more and more random compared to the number of characters the result of encryption cryptographic algorithms using the WAKE method only. And the results of encryption from the combination of the two algorithms are more difficult to guess and the data is safer compared if only using one algorithm, that is WAKE method cryptographic algorithm. Because the main key has been generated with the EM2B Key algorithm using the Increment Key, so that the length main key must be the same as plaintext.
length which will be encrypted, therefore a new key is generated it will be difficult to guess by unauthorized people get the secret key (private key).

During the author's research, that the number of plaintext characters before being encrypted are always more than the number of ciphertext characters after encrypted by a combination of three algorithms or with two algorithms, this is caused by the WAKE cryptographic algorithm with processes that have been explained in the methodology in chapter 3 about the analysis of the cryptographic algorithm WAKE method, and the process of the WAKE algorithm is to speed up the encryption process. And after decryption the number of files is the same as the number of files after being encrypted or before decryption.

Although there are some results of the ciphertext on a combination of three algorithms, there are a number of Chipertext characters less than the ciphertext results of the WAKE method cryptographic algorithm are written in red text, but the result of encryption generated by encryption a combination of three algorithms are more random than using only one algorithm, and the encryption results are safer than one algorithm. This is caused by the RSA algorithm using the EM2B Key with the WAKE method algorithm, which has also been explained in the implementation of the RSA algorithm using the EM2B key with the WAKE method in encrypting the plaintext database in chapter 3 namely the methodology process. To make encryption results safer from hacker attacks, if the length of the main key is getting longer, the results of encryption, will be safer and will be difficult to steal by other people who want to try to retrieve our data. From the table above a graph can be made as shown below:

![Graph of Differences in Encryption Results with WAKE + EM2B Key and WAKE Method](image)

**Figure 11.** Graph of Differences in Encryption Results with WAKE + EM2B Key and WAKE Method

5. Conclusion

a. As long as the author conducts this research the number of ciphertext from a combination of three algorithms or two algorithms produces chipertext which is more dominant random when compared to using only one algorithm.

b. A combination of three ortwo algorithms will be better and safer than just using one algorithm to encrypt plaintext of sql database.

c. The longer the main key, the encryption results produce ciphertext after being encrypted the better and safer from hacker attacks who want our data, and more difficult to guess, this is caused by the RSA algorithm where the algorithm has not been resolved until now, especially if combined with three or two other algorithms as examined by the author, that is RSA algorithm uses the EM2B Key with the WAKE method cryptographic algorithm. Or a combination of the WAKE method cryptographic algorithm using the EM2B key.

d. Number of files before encryption and after encryption or after decryption are same.
References

[1] Heri N, Robin R, Ansari S A, Muhammad S, Muhammad D and Herlina A 2017 Secure a Transaction Activity with Base64 Algorithm and Word Auto Key Encryption Algorithm 2nd International Conference on Statistics, Mathematics, Teaching, and Research IOP Conf. Series: Journal of Physics: Conf. Series 1028 (2018) 012053

[2] Dahlan A, Robin R, Andi, syahputra U S, Ananda F U, Zahratul F, Malahayati M and Harun H 2017 Super-Encryption Cryptography with IDEA and WAKE Algorithm 1st International Conference on Statistics, Mathematics, Teaching, and Research IOP Conf. Series: Journal of Physics: Conf. Series 1019 (2018) 012039

[3] Elwinus H A M, Elwin Y P, Boy Y S and Rahmat W S 2017 Collaborative Encryption Algorithm Between Vigenere Cipher, Rotation of Matrix (ROM), and One Time Pad (OTP) Algorithm, 2nd International Conference of Computer, Environment, Social Science, Health Science, Agriculture & Technology (ICEST) 2017 5-7 May 2017, ISSN: 2415-6698

[4] Basri 2016 Symmetrical And Asymmetric Cryptography In Data Security Perspectives And Computational Complexity. Journal of Computer Science Vol. 2 September, (P) ISSN: 2442-4512, (O) ISSN: 2503-3832

[5] Bruce S 1996 Applied Cryptography 2nd edition Source Code in C John Wiley & Sons

[6] William S Cryptography and Network Security: Principles& Practices, Fifth edition, Prentice Hall, ISBN-13: 978-0136097044, 2010

[7] Muhammad A, Fitriyani and Nurul I RSA Cryptography in Client-Server Based File Transfer Applications, Information Technology Technological Journal Applied Volume I, No 3, 10 August 2015, ISSN: 2407 – 3911

[8] Katz J and Lindell Y 2015 Introduction to Modern Cryptography 2nd ed. CRC Press. Boca Raton

[9] Ahmad R 2012 Department of Electrical Engineering, Diponegoro University Semarang, Implementation of AES Cryptographic Algorithms for Email Encryption and Decryption, Transient, vol. 1, no. 3, September 2012, ISSN: 2302-9927.64

[10] Wheeler D J 1993 A bulk data encryption algorithm Cambridge Security Workshop Cambridge, U. K., December 9–11. Proceedings

[11] Stallings W 2011 Cryptography and Network Security: Principles & Practices. Fifth edition, Prentice Hall, ISBN-13: 978-0-13-609704-4

[12] Hashizume K, Rosado D G, Medina E F and Fernandez E B 2013 An analysis of security issues for cloud computing. Journal of Internet Services and Applications, a Springer open journal pp: 1-13

[13] Schneier B 1996 Applied Cryptography. Second Edition: Protocols, Algorithms, and Source Code in C (cloth); Wiley, J.& Sons. Inc. ISBN: 0471128457

[14] Howard J D April1997 An Analysis of security incidents on the internet. Pittsburgh, Pennsylvania 15213 USA

[15] Menezes A J, Oorschot and Vanstone 1996 Handbook of Applied Cryptography, CRC Press, Inc., Massachusetts Institute of Technology USA