RSA 32-bit Implementation Technique

Dian Kurnia¹, Haida Dafitri², Sugianto³, Mardiana⁴, Andysah Putera Utama Siahaan⁵

^{1,5}*Faculty of Computer Science, Universitas Pembangunan Panca Budi, Medan, Indonesia*

^{2,4}*Department of Informatics, Sekolah Tinggi Teknik Harapan, Medan, Indonesia*

³*Department of Information System, Sekolah Tinggi Teknik Harapan, Medan, Indonesia*

Abstract - Encryption is a technique that transforms a code from an understandable into an incomprehensible code. Many methods can be applied to an encryption process. One such method is RSA. RSA works by appointing on byte values. The value is obtained from character conversion to ASCII code. This algorithm is based on the multiplication of two relatively large primes. Applications of the RSA algorithm can be used in data security. This research provides RSA algorithm application on data security system that can guarantee data confidentiality. RSA algorithm is known as a very secure algorithm. This algorithm works with the number of bits in the search for prime numbers. The larger the bits, the less chance of ciphertext can be solved. The weakness of this method is the amount of ciphertext capacity will be floating in line with the number of prime numbers used. Also, to perform the process of encryption and decryption, RSA requires a relatively long time than other algorithms. The advantage of RSA is that complicated ciphertext is solved into plaintext.

Keywords - Cryptography, RSA, Public Key, Prime

I. INTRODUCTION

Data security and confidentiality issues are an important aspect of information systems. Because of the confidentiality and security of data, it is essential always to be concerned both for common security, as well as for the privacy of individuals [6]. In this case, it is closely related to how important the information and data is sent and received by the interested person. Information is no longer useful if the information is tapped by an irresponsible person. For the data is not known by parties who are not concerned, then each data owner is always trying to do security with some specific techniques.

To secure the data, one way can be applied to use cryptography. Cryptography will encrypt the data before the submission. There are many algorithms for cryptography that can be used. The use of keys in cryptography is divided into two, symmetrical ones that only use a secret and asymmetric key that uses a pair of public keys and a secret key. This research uses RSA [1][2]. It was discovered by Ron Rivest, Adi Shamir, and Leonard Adleman in 1978. RSA stands for the initials of the names of the three of them. RSA is used because it is the most commonly used asymmetric cryptography algorithm at present. This algorithm is well known and safe. The length of keys in bits can be set. The longer bit used, the more difficult to solve. It is because of the difficulty of factoring two huge numbers. However, the greater the prime used, the longer the decryption process.

II. BASIC CONCEPT

2.1 Cryptography

Cryptography is a science or art of securing a message and done by a cryptographer. While cryptanalysis is a science and art of solving ciphertext to plaintext. The person doing it is called cryptanalyst. The word cryptography comes from the Greek word "kryptos" which means to hide and "graphein" which means to write. Cryptography can be defined as a science that transforms

information from understandable forms into incomprehensible forms. Cryptography Algorithm always consists of two parts, namely encryption, and decryption. Encryption is a process done to convert a readable message into an unreadable message (ciphertext). Decryption is the opposite of the encryption process, returning unread messages to unread messages. The encryption and decryption process is governed by one or more cryptographic keys. In a system where there is a cryptographic algorithm, plus all possible plaintext, ciphertext and keys are called cryptosystems [5].

2.2 Public-Key

One of the major difficulties of conventional encryption is the need for security to distribute keys used in a secure state. The next generation technique is a modern cryptography. It is a way to remove this weakness with an encryption model that does not require a key to be distributed. This method is known as the "public-key" encryption and was first introduced in 1976. For conventional encryption, the keys used in the encryption and decryption process are the same. However, this is not necessary conditions. However, it is possible to construct an algorithm that uses one key for encryption and decryption. This process requires different keys for encryption and decryption. Furthermore, it is possible to create an algorithm in which the knowledge of the encryption algorithm and the encryption key is insufficient to determine the decryption key [3].

The following techniques will be possible:

1. Each of the systems makes a key pair used for encryption and decryption.
2. Each of the systems will publish its public key by installing it in a general register or file, while its partner is kept as a private key.
3. If the sender wants to record a message to the receiver, it will encrypt its message with the receiver's public key.
4. When the receiver gets a message from the sender, it will use its private key to encrypt a message from the sender.

Figure 1. Public-Key cryptography scheme

Figure 1 explains how public-key cryptography works. Both plaintexts are covered by public and private keys. Several of them use the same key to encrypt and decrypt, but there also use the different keys. Public-key solves the distribution problem because it does not need a key to share. All users have access to public keys, and private keys are generated individually by each user, so there is no need to share private keys between each other. As long as the user keeps the private key well, then the information sent will always be safe and secure. Any system changing the private key of its partner public key will replace the old public key. The weakness of public key encryption method, when compared with the conventional encryption method, is this encryption has the more complex algorithm. So for comparison the size and price of the hardware. The public key method will result in lower performance than conventional methods.

Things to watch out for in Public-Key encryption such as:

1. The algorithm used for encryption and decryption with the key pair, one for encryption one for decryption.
2. The sender and receiver must have a matching pair of keys.
3. One of the keys must be kept secret.
4. It is not possible or very impractical to translate encrypted information.
5. Knowledge of the algorithm and sample of the encrypted word is insufficient to determine the key.

2.3 RSA

RSA is one example of cryptography that applies the concept of the public-key cryptosystem [4]. In the RSA algorithm, there are three main steps such as key generation, encryption, and decryption. The keys to RSA include two keys, public key, and private key. The public key is used to perform encryption and can be known by others. While the private key is kept secret and used to perform decryption. RSA has several attributes indicate the input and output parameters [7][8]. The following figure shows the process of RSA algorithm.

Figure 2. A flowchart illustrating the RSA algorithm

There are seven aspects we have to understand before trying to hack the RSA secret key such as:

1. P and Q : private
2. $N = P \cdot Q$: public
3. $\phi(N) = (P - 1)(Q - 1)$: private
4. E (encryption key) : public
5. D (decryption key) : private
6. M (plaintext) : private
7. C (ciphertext) : public

RSA uses two kinds of keys, public and private. A public key is a prime number which is shared and unclassified. Both users can know the key, and anybody can get as well. A private key is a key which is not shared or it is classified. Both users who keep the key must keep it secretly. The sender and user hope nobody gets those values. N is got from P times Q. RSA uses the Euler function. It is a function that is used in mathematical calculations. Euler function is a function that is used in mathematical calculations on the RSA algorithm. It defines $\phi(N)$ for $N \geq 1$ indicates the number of positive integers $< N$ relatively prime to N. Two numbers "A" and "B" are relatively prime if $GCD(A, B) = 1$. The value of "E" and "D" are used to encrypt and decrypt. The "M" and "C" are the plaintext and ciphertext byte arrays.

III. EVALUATION

The following illustration will discuss the RSA algorithm implementation which consists of encryption and decryption process. For example, the sender sends a message to the recipient. The process is done starting from the formation of the key, encryption and then the results are described again the steps are as follows:

Table 1. Key Generation

Variable	Value
P	9661
Q	48781
N	471273241
ϕ	471214800

Table 1 shows the key capture. Taken two small prime numbers of 5 and 11. N is derived from the multiplication of both primes, $N = 55$; While Totien is 40.

Table 2. The Encryption Key and GCD

E	GCD
459226353	3
459226354	2
459226355	35
459226356	12
459226357	1
459226358	2
459226359	9
459226360	40
459226361	1
459226362	42
459226363	1
459226364	4

Furthermore, in Table 2 will be selected value of E which has a value of $\text{GCD} = 1$. There are several possible values to choose from because some have $\text{GCD} = 1$ viewed from the table. In this experiment, we will choose the value $E = 459226363$, because $\text{GCD}(459226363, 471214800) = 1$. Then we will find the value of the private key by using the algorithm and obtained that $D = 459226363^{-1} \bmod 471214800 = 307475827$. Thus, the public key is $(N, E) = (471273241, 459226363)$ and the secret key is $D = 307475827$.

Table 3. The complete parameters of RSA

Variable	Value
P	9661
Q	48781
N	471273241
T	471214800
E	459226363
D	307475827

The calculations below will illustrate the encryption and decryption process of the RSA algorithm.

Encryption Process:

$$\begin{aligned}
 E1 &= 144^{459226363} \bmod 471273241 \\
 &= 174408074 \\
 E2 &= 102^{459226363} \bmod 471273241 \\
 &= 118193768 \\
 E3 &= 235^{459226363} \bmod 471273241 \\
 &= 443990101 \\
 E4 &= 218^{459226363} \bmod 471273241 \\
 &= 409440301 \\
 E5 &= 121^{459226363} \bmod 471273241 \\
 &= 474605588 \\
 E6 &= 2^{459226363} \bmod 471273241 \\
 &= 445186215
 \end{aligned}$$

Decryption Process:

$$\begin{aligned}
 D1 &= 174408074^{307475827} \bmod 471273241 \\
 &= 144 \\
 D2 &= 118193768^{307475827} \bmod 471273241 \\
 &= 102 \\
 D3 &= 443990101^{307475827} \bmod 471273241 \\
 &= 235 \\
 D4 &= 409440301^{307475827} \bmod 471273241 \\
 &= 218 \\
 D5 &= 474605588^{307475827} \bmod 471273241 \\
 &= 121 \\
 D6 &= 445186215^{307475827} \bmod 471273241 \\
 &= 2
 \end{aligned}$$

Table 4. RSA Encryption & Decryption

ASCII	Encryption	Decryption
144	174408074	144
102	118193768	102
235	443990101	235
218	409440301	218
121	474605588	121
2	445186215	2

From the above example, it can be seen that the data before the encryption is the same as the data after the decryption as shown in Table 4. The RSA cryptosystem makes our data more secure from people who want to steal the data. In the example above the author used a 32-bit prime number. To improve the security of data should use a bigger prime number and it is hard to factorize.

IV. CONCLUSION

Secrets and data security should be a top priority so that the data we want to send is only accepted by the person who has been appointed as the recipient of the information. By using RSA Algorithm, a system capable of ensuring data confidentiality can be established. From a technical point of view, RSA has easy and simple encryption. However, seeing the size of the prime used, once encrypted is a very difficult thing to return to the plaintext without knowing the prime number. In the process of creating public keys and private keys, there are several factors to consider, namely the size of the key, the determination of the p and q values to be difficult to crack, and the possible weaknesses that can be known when the data is encrypted. The RSA algorithm's security is based on the difficulty of factoring large numbers into their prime factors. RSA is very superior to security but very weak of speed.

REFERENCES

- [1] B. R. Ambedkar dan S. S. Bedi, "A New Factorization Method to Factorize RSA Public Key Encryption," *International Journal of Computer Science*, vol. 8, no. 6, pp. 242-247, 2011.
- [2] H.-M. Sun, M.-E. Wu, W.-C. Ting dan M. J. Hinek, "Dual RSA and Its Security Analysis," *IEEE Transactions on Information Theory*, vol. 53, no. 8, 2007.
- [3] N. Hegde dan P. Deepthi, "Pollard RHO Algorithm for Integer Factorization and Discrete Logarithm Problem," *International Journal of Computer Applications*, vol. 121, no. 18, pp. 14-17, 2012.
- [4] A. P. U. Siahaan, "Factorization Hack of RSA Secret Numbers," *International Journal of Engineering Trends and Technology*, vol. 37, no. 1, pp. 15-18, 2016.
- [5] M. Iqbal dan A. P. U. Siahaan, "The Understanding of GOST Cryptography Technique," *International Journal of Engineering Trends and Technology*, vol. 39, no. 3, pp. 168-172, 2016.
- [6] E. Hariyanto dan R. Rahim, "Arnold's Cat Map Algorithm in Digital Image Encryption," *International Journal of Science and Research*, vol. 5, no. 10, pp. 1363-1365, 2016.
- [7] N. Y. Goshwe, "Data Encryption and Decryption Using RSA Algorithm in a Network Environment," *International Journal of Computer Science and Network Security*, vol. 13, no. 7, pp. 9-13, 2013.
- [8] I. Jahan, M. Asif dan L. J. Rozario, "Improved RSA Cryptosystem Based on the Study of Number Theory and Public Key Cryptosystems," *American Journal of Engineering Research*, vol. 4, no. 1, pp. 143-149, 2015.