Public Key Cryptography

Dwi Liestyowati*

Faculty of Science and Engineering, Faletehan University, Bandung, Indonesia

*dliestyowati@gmail.com

Abstract. Public Key Cryptography is a software model that presents the process of encoding information, in this case the documents contained in a file. The encoding process begins by determining the master file or document that is ready to be encoded, then by applying the combination method, shifting and implementing the pass phrase to the contents of the document, the encoded document will be formed by Encryption function. The contents of the encoded document are then returned back with the pass phrase implementation method, shifting and combinations to form the master document again by decryption function.

1. Introduction

Security in the world of internet has become a very important need and necessity in all aspects of social life. Information data security is the main and leading factor that determines whether the information data is still useful and can be used. The level of security of the information data to be used varies depending on the usefulness of the information data. In the world of e-commerce, data information that is used and exchanged has a high level of security criteria to prevent misuse and piracy [2].

One of the techniques of securing data information in the internet world is the Asymmetric cryptography technique. A cryptographic algorithm contains mathematical functions that are used to carry out the encryption and decryption process. The mathematical basis that underlies the process of encryption and decryption is the relation between two sets, namely those containing plaintext elements and those containing cipher text elements[1].

1.1. Cryptography

Cryptology is one of the sciences that studies a safe way of communication, which includes cryptography and cryptanalysis. Cryptography is a branch of cryptology regarding the design of algorithms for the encryption and decryption process, which is intended to ensure the confidentiality and or authenticity of a message. Cryptography does not mean only providing information security, but rather towards the techniques or in broad terms cryptography can be interpreted as an art and science to maintain the security of a message. Cryptanalysis is a branch of cryptology that discusses how to decrypt encrypted messages (Cipher text) to get information, or forge encrypted information so that information is considered authentic.

There are three basic objectives of cryptography, namely:

- **Confidentiality** is a provision that is used to secure the information content of anyone except those who have the authority to own it.

- **Data Integrity** is a provision relating to the security of unauthorized data changes. To maintain data integrity, the system must have the ability to detect a state of attempted data manipulation by unauthorized parties, including the insertion, deletion and substitution of other data into actual data.
- **Authentication** is a provision related to identification where the information sent must be authenticated.

The cryptographic system is divided into 3 different dimensions, including:

a) The type of method used in the transformation of plaintext to cipher text. All encryption algorithms are based on 2 basic principles, namely substitution, where each element in the plaintext is mapped with other elements, and transposition, where the elements in the plaintext are rearranged. The fundamental need is the absence of missing information. Most existing systems involve tiered levels of substitution and transposition.
b) Key used. If the sender and receiver use the same key, the system is called symmetric, single key, secret key, or conventional encryption. If the sender and recipient use different keys, the system is called asymmetric, dual key, or public key encryption.
c) Plaintext processing method. Block ciphers process one block's input at a time, producing one block's output from one block's input. Stream ciphers process input elements continuously, producing one element at a time.

In cryptography a message that will be kept secret will be encrypted using an algorithm. Messages that have been encoded are called plaintext and messages that have been encrypted or encrypted are called cipher text. The process to convert plaintext to cipher text is called encryption and the process to restore plaintext from cipher text is called decryption.

Encryption and decryption are functions of transformation between these sets. If the plaintext elements are denoted by M, the cipher text elements are denoted by C, while for the encryption process is denoted by E, decrypted by notation D. The mathematical notation of this process is:

- Encryption : $E(M) = C$
- Decryption : $D(C) = D(E(M)) = M$

With a block diagram, the encryption and decryption process can be described as follows:

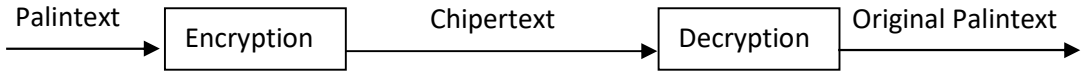

Figure 1. Block Diagram Encryption and Decryption process

1.2. Symmetric and Asymmetric algorithm

In encryption and decryption operations, a key is needed to maintain the confidentiality of the workings of the encryption and decryption algorithm. Encryption algorithms based on keys are classified into two parts:

1. Symmetric Algorithms, where the keys used for the encryption and decryption processes are the same. This algorithm can also be called secret-key algorithm or one-key algorithm.
2. Asymmetric algorithm, which uses a different key that is the public key to do the encryption process and private key to do the decryption process.

Symmetric algorithms in the encryption and decryption process can be symbolized mathematically and described as follows:

- Encryption : $E_K(M) = C$
- Decryption : $D_K(C) = D_K(EK(C)) = M$

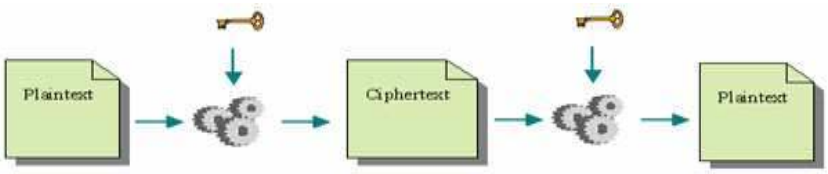

Figure 2. Symmetric Algorithm

Asymmetric algorithm uses different encryption keys and decryption keys. The encryption key can be distributed to the public and named as a public key, while the decryption key is kept and kept private for its own use and is named as a private key. The confidentiality factor in this algorithm is very dependent on the confidentiality of the private key used. The validity factor depends on the security of the private key. Therefore, this algorithm is also known as the public key algorithm.

This Asymmetric Algorithm uses key sizes, both public and private keys, with a longer size or greater value compared to the secret key in the symmetric algorithm. Asymmetric algorithms are slower in terms of time use and are only effective in processing small amounts of data.

Asymmetric algorithm or public key cryptography is divided into two main branches, namely:

- Public key encryption, where messages encrypted by public key users cannot be decrypted by others unless other private key users have been submitted by public key users.
- Private key encryption, where messages that have been marked with the user's private key can be verified by others who can use the user's public key to prove that the user has marked it and the message has not changed.

The asymmetric algorithm in the encryption and decryption process can be symbolized mathematically and is described as follows:

- Encryption : $E_{K1}(M) = C$
- Decryption : $D_{K2}(C) = D_{K2}(E_{K1}(C)) = M$

The public key is denoted by K1 while the private key is denoted by K2.

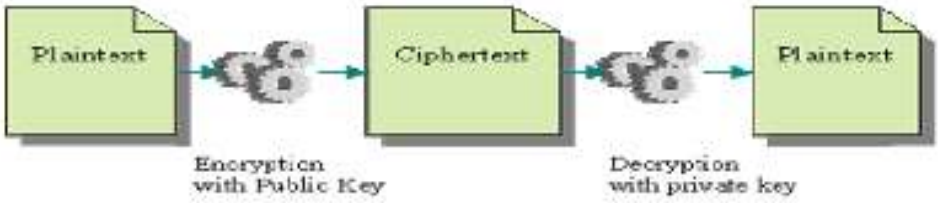

Figure 3. Asymmetric Algorithm

2. Method

2.1. Public Key Cryptography

In public Key encryption two different keys are used to encrypt and decrypt the data. These two different keys are mathematically related. One is the public key and the other is the private key, they come as a pairs.

The public key encryption is also known asymmetric key encryption because two different keys are use. In public key encryption, The Public key is public to anyone, while the private key belongs only to the person who creates these two keys

How its work:

The public key method to encrypt the sender's message starts with the receiver, not the sender. The public key is public to everyone. The private key is only known to the receiver.

2.2. Asymmetric key

- An Asymmetric key algorithm requires two keys called a public key and a private key. One of the key is used for encryption of a plaintext and the other key is used for decryption of the ciphertext

- For instance; if Arias generates a private key and a corresponding public key, than anyone is allowed to know her public key, but Arias must keep her private key secret.
- A big disadvantage is that asymmetric key algorithms are generally much slower (hundreds to thousands times) to encrypt and decrypt a message than symmetric key algorithms.
- The advantage of using an asymmetric key algorithm is that any sender can encrypt a message using the receiver public key, but only the receiver can decrypt the cipher text using its private key.
- A public key and private key are mathematically interconnected. Meaning each public key has only one corresponding private key.
- Few asymmetric key algorithms are: RSA (Rivest Shamir Adleman), ECDSA (Eliptic Curve Digital Signature Algorithm)
- In Blockchain the Elliptic Curve Digital Signature Algorithm is often used

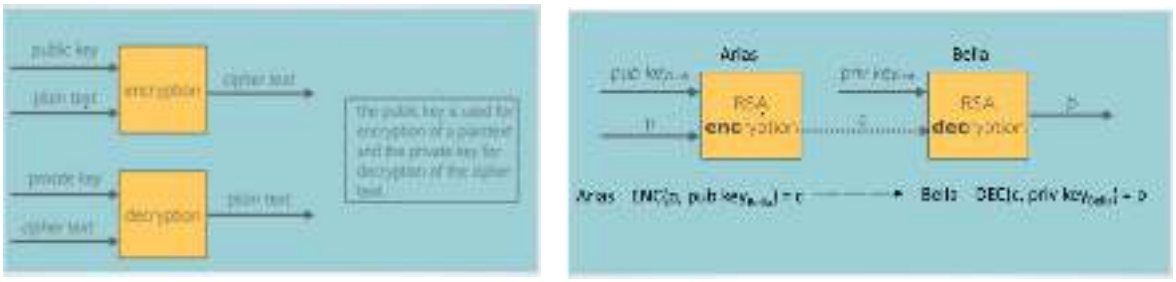

Figure 4. Asymmetric Key

2.3. RSA Public Key

One of the best-known asymmetric key (public-key) cryptographic algorithms is RSA (Rivest, Shamir, Adleman). This algorithm was made by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA security algorithm addresses the difficulty of factoring large numbers into prime factors. Factoring is done to obtain a secret key. During factoring, large numbers into prime factors have not yet been found the algorithm so long as the security of the RSA algorithm remains safe [6].

- Public Key Cryptosystem : It means the encryption key is public
- Asymmetric Cryptosystem : Different keys for encryption and decryption

Variables for further ease;
p, q : Two very large primes
n : Modulus, $n = p*q$
e : Public Key Exponent
d : Private Key Exponent
M : Plaintext
C : Ciphertext
$\phi(n)$: Euler's Totient Function

Key Generation:

- Choose two different large primes p and q
- Compute $n = p*q$
- Calculate the value of $\phi(n) = (p - 1)*(q - 1)$ in this case
- Choose an integer e such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$
- Compute d as $d = e^{-1} \bmod \phi(n)$
- The pair (e, n) is known as public key and (d, e) is known as private key

3. Result and discussion

Let see Arias receipt Cipher text like this:

"05046020304785054634104269320172949032068304610960021952087619404066300261968"

Formula of Encryption Function

$$E = f_z(x) = x^p \pmod m \quad (1)$$

$f_z(x)$ is the Encrypt Function that produces a Cryptogram of 7 digit numbers, while {p, m} is the Public Key, which has been determined by Bella p = 2173 and m = 1085323

The encrypt process as follows:

a) Each Alphabet letter from A to Z is replaced by a number from 10 to 35, plus a space expressed by the number 46

A	B	C	D	E	F	G	H	I	J	K	L
10	11	12	13	14	15	16	17	18	19	20	21

M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Space
22	23	24	25	26	27	28	29	30	31	32	33	34	35	46

Figure 5. Shifting Alphabet with number

b) The message is then replaced by a series of numbers, then divided into groups of numbers consisting of 4 digits.

c) Then each of the 4 digit numbers is increased in value by the rank of p of the modulo m residue, so that it turns into a group of numbers consisting of 7 digits.

From the above encoding produces a message, the steps taken to solve the message are:

a) The Encrypt function that produces a Cryptogram of the 7-digit numbers is inverse, so the inverse function produces decrypt.

b) Then the decrypt results are mapped back to the Alphabet

Decrypt inverse function:

$$D = f_z^{-1}\{f_z(x)\} = \{f_z(x)\}^d (mod\ m) \quad (2)$$

Key {d, m}

Problem: How to determine d by only knowing {p, m}?

If m the prime number factors c_1 and c_2, then p and d must satisfy the relation:

$$p.d = 1 \bmod (c_1 - 1)(c_2 - 1) \quad (3)$$

First we look for the Prime factors of m = 1085323

$m = c_1 . c_2 = 1085323$, Therefore $c_1 = 1021$ and $c_2 = 1063$

Then the secret key $Z = \{ c_1 , c_2 , p\} = \{1021, 1063, 2173\}$,

So that $p.d = 1 \bmod (c_1 - 1)(c_2 - 1)$

$2173.d = 1 \bmod (1021 - 1)(1063 - 1)$

$2173.d = 1 \bmod (1083240)$

$2173.d = k(1083240) + 1$

When $k = 2$,

then $2173.d = 2(1083240) + 1$

$d = 2(1083240) : (2173) = 997$

These are relative prime to the number 1083240

Decryption process

we get Private Key {d, m}

Now use d = 997 and m = 1085323 in the equation $D = \{f_z(x)\}^d (mod\ m)$ with

$fz_1(x) = 504602 \rightarrow D_1 = (504602)^{997} \pmod{1085323} = 3023$
$fz_2(x) = 304785 \rightarrow D_2 = (304785)^{997} \pmod{1085323} = 1831$
$fz_3(x) = 546341 \rightarrow D_3 = (546341)^{997} \pmod{1085323} = 1427$
$fz_4(x) = 426932 \rightarrow D_4 = (426932)^{997} \pmod{1085323} = 2818$
$fz_5(x) = 172949 \rightarrow D_5 = (172949)^{997} \pmod{1085323} = 2910$
$fz_6(x) = 320683 \rightarrow D_6 = (320683)^{997} \pmod{1085323} = 2846$
$fz_7(x) = 461096 \rightarrow D_7 = (461096)^{997} \pmod{1085323} = 1510$
$fz_8(x) = 21952 \rightarrow D_8 = (21952)^{997} \pmod{1085323} = 211\ 4$
$fz_9(x) = 876194 \rightarrow D_9 = (876194)^{997} \pmod{1085323} = 2914$
$fz_{10}(x) = 406630 \rightarrow D_{10} = (406630)^{997} \pmod{1085323} = 1710$
$fz_{11}(x) = 261968 \rightarrow D_{11} = (261968)^{997} \pmod{1085323} = 2346$

The decryption results are rearranged into alphabet:

30231831142728182910284615102114291417102346

30	23	18	31	14	27	28	18	29	10	28	46	15	10	21	14	29	14	17	10	23	46
U	N	I	V	E	R	S	I	T	A	S		F	A	L	E	T	E	H	A	N	

4. Conclusion

4.1 Every individual gets not just one key, but a key pair. The pair is generated together. One key is called the private key while the other key is called the public key. The qualities of the key are:

- Even if the public key is know n it is impossible to determine from this what the private key is
- A message can be encrypted using either the public key or the private key
- If the public key has been used to encrypt a message, then only the corresponding private key can decrypt it
- If the private key has been used to encrypt a message, then only the corresponding public key can decrypt it
- When an individual has a key pair he openly publishes the public key, but never tells anyone the private key.

The security of method depends on never letting anyone know your Private key.

Downside to Asymmetric cryptology: Encryption speed is about 1000 times slower than using a Symmetric algorithm like AES. There are Asymmetric cryptography is generally only used for key exchange purposes, while Symmetric cryptography is used for bulk encryption of data.

Arias has already generated a key pair. She allows anybody to get her public key. Bella takes Arias public key and uses it to encrypt his personal information. She sends this cipher text across the public internet over to Arias. Since Arias never shares her private key she is the only one that can decrypt the message, thus guaranteeing its confidentiality over the public internet.

When Arias receives the message she simply decrypts it with her private key that only she has

4.2 RSA Strength and Safety

The strength of the RSA algorithm lies in the level of difficulty in factoring nonprime numbers into prime factors, in this case $n = a \times b$.

Once n is factored into a and b, then $m = (a - 1) \times (b - 1)$ can be calculated. Furthermore, because the encryption key e is announced (not secret), the decryption key d can be calculated from the equation $e \times d \equiv 1 \pmod{m}$. This means the decryption process can be carried out by unauthorized people.

The inventor of the RSA algorithm recommends values a and b of more than 100 digits in length. Thus the product of $n = a \times b$ will be more than 200 digits in size [8].

According to Rivest and his colleagues, an attempt to find a 200 digit number factor requires 4 billion years of computing time! (assuming that the factoring algorithm used is the fastest algorithm at the moment and the computer used has a speed of 1 millisecond) [8].

Acknowledgement:
Researches is supported by Faculty of Science and Engineering, Faletehan University, and realized that during the process of this research found many difficulties. These difficulties will not be resolve by researchers without the help and encouragement of various parties.
Brief biography of First author: Dwi Liestyowati (Lecturer in Electrical Engineering, Faculty of Science and Engineering, Faletehan University)

Reference
[1] Davies, 1989, D. dan W. Price, *Security for computer networks*, Wiley, New Yorks.
[2] Stallings, William, 2003, *Cryptography and network security; Principles and practices*, Prentice Hall, New Jersey.
[3] Tsudik, G, 1992, *Message authentication with one-way hash functions*, INFOCOM92.
[4] http://www.answers.com
[5] http://en.wikipedia.org
[6] Munir, Rinaldi. (2006). *Dikat Kuliah IF5054 Kriptografi*.
[7] Swastyayana. 2008. *Metode Enkripsi RSA*. Bandung: Makalah Institut Teknologi Bandung.
[8] Mollin, Richard A. 2002. *RSA and PUBLIC-KEY CRYPTOGRAPHY*. Florida, Boca Raton: CRC Press LLC.
[9] Mukodim, Didin. 2002. Teknik Pengamanan Data dengan RSA. *Proceedings, Komputer dan Sistem Intelijen (KOMMIT 2002)*. Jakarta: Universitas Gunadarma.
[10] Riyanto, M. Zaki & Ardhi Ardian, 2008, *Kriptografi Kunci Publik: Sandi RSA*. http://sandi.math.web.id
[11] Iqbal, Muhammad. 2006. *Studi Teknis Metode Enkripsi RSA dalam Perhitungannya*. Bandung: Institut Teknologi Bandung.
[12] Menezes, Alfred J., Paul C. van Oorschot & Scott A. Vanstone. 2001. *Hand Book of Applied Cripthography*. CRC Press