RSA KEY DEVELOPMENT USING FINGERPRINT IMAGE ON TEXT MESSAGE

Sayuti Rahman¹, Indah Triana², Sumi Khairani³, Amru Yasir⁴, Siti Sundari⁵

¹,²,³Jurusan Teknik Informatika, Sekolah Tinggi Teknik Harapan Medan
⁴Universitas Dharmawangsa Medan
¹masay.ram@gmail.com,² indahtriana46@gmail.com ,³adek_sumi@yahoo.co.id,
⁴cougara25@gmail.com,⁵sundaristth@gmail.com

Abstract. Along with the development of technology today, humans are very facilitated in accessing information and communicate with various media, including through the Internet network. Messages are sent by media such as text are not necessarily guaranteed security. It is often found that someone wants to send a secret message to the recipient, but the messages can be known by irresponsible people. So the sender feels disappointed because the secret message that should be known only to the recipient only becomes known by the irresponsible people. It is necessary to do security the message by using the RSA algorithm. Using fingerprint image to generate RSA key. This is a solution to enrich the security of a message, it is needed to process images firstly before generating RSA keys with feature extraction.

Keywords : RSA, Fingerprint, Cryptography, Image Processing.

1. Introduction

The development of information technology is currently increasing widely so that human needs for the latest information, accurate, fast and reliable is increasingly easy and more inseparable in human life. Such as through telecommunication network and internet.

With the development of information technology so many users communicate the Internet network, therefore many cases of interception of communication made by a handful of people who are not responsible for unnecessary purposes, because everyone has a secret, whether private secrets, family secrets, group secrets, Even state secrets. So therefore there is a need for security text messages when communicating over the Internet network.

Security issues are one of the important aspects of an information system. One of the important things in communication using computers and in computer networks to ensure the security of messages, data or information is encryption. Encryption is a process done to the original message to be encoded or made into another form so that it can't be seen the original form of the message, in other words the original message is often called the plaintext changed into a password or cipher text. To see the message again, the decryption process or change the message encoded into the original message again (Alvianto, 2015).

Encryption and decryption process requires an algorithm to be able to secure data well and can be used in communication and transaction information one of them is with RSA algorithm, RSA has been formulated as a practical algorithm to be implemented in cryptography system using public key designed by Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. The key pair used for the encryption process are the public key (e, n) and private key d as the decryption key where e, d and n are positive integers. The RSA algorithm is a block cipher algorithm that groups plaintext into blocks before encryption becomes cipher text. (Alvianto, 2015)

Information that has been encrypted with RSA algorithm can be sent and shared by distributing the public key on receiver and private key stored in file, but in this research how to use fingerprint image to generate public key as opening message. Image is a data that has many meanings that can be processed into complete information, the use of fingerprint image because it
can represent the identity of the sender who can be recognized by the owner or called biometric identification. (S Rahman, 2017)

2. Methods

a. Data Security

Security and confidentiality of messages is a very important thing in communicating through the Internet because the network is prone to the crime by spreading the badness of someone to who is not entitled to know the information. Computer users that want the data unknown to unauthorized parties are always trying to get around how to secure the information to be communicated or to be stored. So the protection for data confidentiality increases, one way is data encryption. Encryption is a process of converting an original message into an unreadable character. There are several commonly used encryption algorithms such as Block Cipher, Stream Cipher, Data Encryption Standard (DES), Triple DES, Advanced Encryption Standard (AES), and so on.

b. Cryptography

The word cryptography comes from greek, "Kriptos" which means hidden and "graphien" which means write. So the word cryptography can be interpreted as "hidden text". This means cryptography is an art and science used to hide information or messages from unauthorized recipients. Cryptography is a science that relies on mathematical techniques to deal with information security such as confidentiality, data integrity and entity authentication. In a cryptographic algorithm, there are two elements:

1. Encryption, ie the process of converting the original message into an encoded message, and.
2. Decryption, ie the process of converting the encoded message to the original message.

c. RSA Algorithm Encryption

The next process after generating the key to the RSA is the Encryption process. Encryption is the process of converting the original message (plaintext) into a secret message (chipertext). In this process the original message is first converted into decimal form, then the decimal message are then divided into several decimal blocks of a regular basis. Each decimal block will have a value that must be less than the value of n called P. The formula used to perform the Encryption process of RSA is:

\[ C = P^e \pmod{n} \]

where

- \( P \) = Plain text
- \( C \) = Cipher text
- \( e \) = public key
- \( n \) = public key (ab)

d. RSA Algorithm Decryption

The decryption process in RSA is similar to the encryption process, only in the decryption process using private key d. The formula for the decryption process of RSA is as follows:

\[ P = C^d \pmod{n} \]

where

- \( P \) = Plaintext
- \( C \) = Ciphertext
- \( d \) = private key
- \( n \) = public key (ab)

e. Image
Image is an important component in multimedia that has a deeper meaning compared to text data by displaying data visually and representing information that takes place when image retrieval, either object, condition, color, weather and many more meaning that can be extracted from an image. Viewed from a mathematical point of view, the image is a continuous function of the intensity of light in the field of two dimensions. Light sources illuminate objects, objects reflect light provided with different reflection levels of each object. This light reflection is captured by optical devices, such as human eyes, cameras, scanners, and so on. So the image of the object called the image is recorded. (Permadi, 2015)

f. Fingerprint

A fingerprint is formed by a combination of curves. The bright areas are called ridges while the dark areas are called valleys. Fingerprint are the result of reproduction of the skin of the finger surface either deliberately taken / stamped on ink or traces left to the object. The reproduction results in the form of paintings that consist of lines of papilair groove. Characteristics and features in this plot of papilair that distinguishes between people with each other. Human Fingerprints are divided into 5 main groups of fingerprints, namely: Whorl, Arch, Tanted Arch, Right Loop and Left Loop.

g. Problem analysis

The messaging security is very necessary when sending messages via electronic media. Then the message must remain safe during the delivery process. In the message delivery process, the public key can be known by anyone, but the key to the description is known only to the recipient of the message. For the sending of messages in secret then the need for security in the process of delivery. RSA cryptography is an asymmetric key cryptography. The key to RSA cryptography consists of two keys: private key and public key. Given these two keys the process of sending messages does not require a lot of keys to sending many messages, simply made two keys, namely the public key to encrypting the message for the recipients and the description as a private key. Private keys are usually stored in a file, so it is easy about others to extract the private key. Then, to prevent theft of keys, it is necessary to use a fingerprint method as a key generator of the RSA algorithm.

In generating a key using fingerprint image. The process to do is to read the binary image of the fingerprint image. Here is an example of the pixel value of the fingerprint image.

\[
\begin{array}{cccccccccc}
1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\
\end{array}
\]

Figure 1 Fingerprint Image Pixel

From the fingerprint image pixel data onto is known the number of pixels worth 1 is 34, and the number of pixels is 0 is 26. To get the value of \(a\) and \(b\) is taken from the first primary number of the number of pixels. Number of pixels values 1 becomes a reference value of variable \(a\) and pixel value 0 becomes reference variable value \(b\). So the value of \(a\) obtained is 34 and the value of \(b\) is 26.

The flowchart of the key generator in RSA:
Figure 2 shows the RSA key generation process flowchart. The initial value of \( e \) is setting equal to two and \( k \) equals 1. The values of \( a \) and \( b \) are obtained from the input of the fingerprint image. Next the calculation of values of \( n \) and \( m \). The value of \( e \) is obtained from the relative prime number of \( m \) that starts from 2 and increases one when it has not been obtained relatively prime. The value in is obtained from the formula \( d = \frac{1+km}{e} \) where \( k \) starts from one and increases one onwards until the \( d \) value is obtained as an integer. Then get the public key \( e \), \( n \) and private key \( d \), \( n \).

3. Results and Discussion

From the design result to generate RSA key is to use fingerprint image, this image as input variable \( a \) and \( b \) in RSA process, automatically generate both the public and private key, following the view of taking value of fingerprint image seen in picture 3.
In Figure 3 it can be seen that the public e, n key has been obtained from the extract of the fingerprint feature to be used for encrypting text messages as shown in Figure 4.

The "indah" message on the image with the key generated from the fingerprint image succeeds to secure the message as shown in Figure 4, to decrypt the message using the stored private key.

The message decryption process can be seen in Figure 5 below:
The following encryption process results are presented in table 1:

| No | Plaintext          | Ciphertext                                                                 | Citra | Keterangan |
|----|--------------------|-----------------------------------------------------------------------------|-------|------------|
| 1  | Nama saya Indah    | 0000000000000000057060297200000000000000479340371 0000000000000000032852547500000000000000479340371 0000000000000000003355443200000000000000422715009 000000000000000000479340371000000000000000455139245 000000000000000000479340371000000000000000033554432 00000000000000000033564304600000000000000455139245 0000000000000000000015457156700000000000000479340371 |  | Berhasil |
| 2  | Hari ini Hari Senin | 00000000000000000549473610000000000000000353650977 000000000000000002364922010000000000000000403214886 00000000000000001113170340000000000000000403214886 |  | Berhasil |

The decryption process of the encrypted message is done successfully as shown in table 2:

| No | Citra | Ciphertext                                                                 | Plaintext                  | Keterangan |
|----|-------|-----------------------------------------------------------------------------|----------------------------|------------|
| 1  |  | 0000000000000000057060297200000000000000479340371 0000000000000000032852547500000000000000479340371 | Nama saya Indah | Berhasil |
| 2  |  | 00000000000000000549473610000000000000000353650977 | Hari ini Hari Senin | Berhasil |
4. **Conclusion**

From the design results RSA key generator using fingerprint image in the message security, obtained conclusion of which is as follows:

1. Application to secure text message using fingerprint image with RSA Algorithm Cryptography method for better security successfully done.
2. The fingerprint image is used as a prime number in RSA key generation.
3. Private key stored information in fingerprint image.
4. Public key is generated from fingerprint image in the form of numbers that can be stored or sent.
5. RSA algorithm method can be combined with other methods to improve the security of a file.
6. In terms of time, when the process of reading fingerprint image takes a long time.

5. **Bibliography**

[1] A. Fallis, 2013, Aplikasi Pengamanan File Menggunakan Kombinasi Algoritma C-RSA, Arcfour, Dan C-AES (CAC), J.Chem. inf. Model., vol. 53, no. 9, pp. 1689-1699.

[2] Nafi’iyah, Nur. 2015. Algoritma Kohonen Dalam Mengubah Citra Graylevel Menjadi Citra Biner, Vol.9 No.2, Agustus 2015.

[3] Hafizah, dkk. 2015. Penerapan Jaringan Syaraf Tiruan Dengan Algoritma Perceptron untuk Mendeteksi Karakteristik Sidik Jari, Vol.14, No. 2. 2015.

[4] Rosmala, dkk. 2012. Implementasi Mode Operasi Chiper Block Chaining (CBC) Pada Pengamanan Data, Vol. 3, No.2, Mei – Agustus. 2012.

[5] Sadikin, Rifki. 2012. Kriptografi untuk Keamanan Jaringan. Yogyakarta: ANDI.

[6] Hasibuan, Andi Hazri. 2013. Penambahan Chiner Reminder Theorem Untuk Mempercepat Proses Enkripsi Dan Dekripsi Pada RSA, Universitas Sumatera Utara Medan.

[7] Permadi, Yuda.2015, Aplikasi Pengolahan Citra Untuk Identifikasi Kematangan Mentimun Berdasarkan Tekstur Kulit Buah Menggunakan Metode Ekstraksi Ciri Statistik,Universitas Ahmad Dahlan.

[8] Hatta Muttaqin, Ismail, Risnandar. 2012, Modul Pengiriman Data Untuk Pemindai Barcode Nirkabel, Bandung: Politeknik Telkom.

[9] S Rahman, M Ulfayani. 2017, Perancangan Aplikasi Identifikasi Biometrika Telapak Tangan Menggunakan Metode Freeman Chain Code, CESS (Journal of Computer Engineering, System and Science) Vol.2 No.2, 121-130