Implementation of Rivest Shamir Adleman Algorithm (RSA) and Vigenere Cipher In Web Based Information System

Aryanti Aryanti [1,*], *Ikhthison* Mekongga[2]

[1] Telecommunication engineering State Polytechnic of Sriwijaya, Palembang - Indonesia
[2] Computer engineering State Polytechnic of Sriwijaya, Palembang - Indonesia

Abstract. Data security and confidentiality is one of the most important aspects of information systems at the moment. One attempt to secure data such as by using cryptography. In this study developed a data security system by implementing the cryptography algorithm Rivest, Shamir Adleman (RSA) and Vigenere Cipher. The research was done by combining Rivest, Shamir Adleman (RSA) and Vigenere Cipher cryptographic algorithms to document file either word, excel, and pdf. This application includes the process of encryption and decryption of data, which is created by using PHP software and my SQL. Data encryption is done on the transmit side through RSA cryptographic calculations using the public key, then proceed with Vigenere Cipher algorithm which also uses public key. As for the stage of the decryption side received by using the Vigenere Cipher algorithm still use public key and then the RSA cryptographic algorithm using a private key. Test results show that the system can encrypt files, decrypt files and transmit files. Tests performed on the process of encryption and decryption of files with different file sizes, file size affects the process of encryption and decryption. The larger the file size the longer the process of encryption and decryption.

1 Introduction

Data security and confidentiality are one of the most important aspects of information systems today. One attempt to secure data such as by using cryptography. Cryptography is the art or science used to maintain the security of information or messages by turning it into something that has no meaning. In cryptography, encryption and decryption, encryption is to convert the message into data that cannot be read or understood while the decryption is to restore the data as before so that data can be read properly [1].

Various kinds of cryptographic algorithms can be implemented to realize the data security system. Among them is Rivest Shamir Adleman (RSA) cryptography algorithm. RSA that use asymmetric algorithms have two different keys, called the key pair for the encryption and decryption process. The security level of the RSA encryption algorithm depends heavily on the key size of the password, because the smaller the key size, the greater the possible combination of locks can be broken by the method of examining the combination of one by one key or better known as Brute Force Attack. The prime numbers generated in the RSA algorithm affect the key size of the password [2].

Cryptography using the Vigenere Cipher Algorithm by adopting the operation mode of Cipher Block Chaining (CBC) operation is one of the methods of many data security methods. This application includes encryption and data decryption, created using Borland Delphi 6.0. The encrypted data will have an extension. Merging the Vigenere Chiper algorithm and the CBC mode of operation will produce a new method that researchers call Vigenere Chiper +, in this method the weaknesses of the Vigenere Chiper algorithm will be improved. As it extends the reach of 26 letters of the alphabet into 256 ASCII characters [3].

In this study developed a data security system by implementing the cryptography algorithm Rivest Shamir Adleman (RSA) and Vigenere Chiper. The research was done by combining Rivest Shamir Adleman (RSA) and Vigenere Cipher cryptographic algorithms to document file either word, excel, ppt and pdf. This application includes encryption and data decryption, created using PHP and my SQL. Data encryption is done on the send side through RSA cryptographic calculations first using public key, then proceed with Vigenere Cipher algorithm which also use a public key. As for the stage of the description side received by using the Vigenere Cipher algorithm first still use public key and then use the RSA cryptographic algorithm using a private key.

2 Research methods

2.1 The proposed method

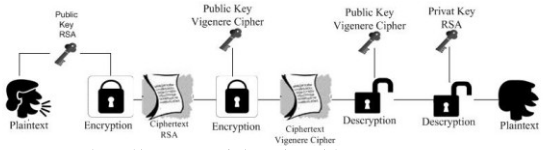


Fig. 1. Design diagram of the algorithm

The method used in this research is by combining Rivest Shamir Adleman (RSA) cryptographic algorithm and Vigenere Cipher. Plain text or first original file will be encrypted using the RSA cryptographic algorithm by using public key. And it will generate RSA ciphertext. Then in encryption again using public key cryptography algorithm vigenere cipher. After going through a double locking process. Furthermore, the decryption process uses cryptography algorithm vigenere cipher by using public key. Because vigenere cipher is a symmetric algorithm which in the process of encryption and decryption using the same key. And finally the decryption process uses the private key RSA cryptographic algorithm. Then back to the plaintext.

2.2 Stages of key establishment

2.2.1 RSA lock generation stage

For the RSA key generation process in this test the following steps are performed [4]:

1 Determine the two prime numbers, with the names p and q. Suppose the value of p = 51 and q = 5.

2 Calculate the modulus value (n):

$$n = p * q \quad (1)$$

$$n = 51 \text{ x } 5$$

$$n = 255$$

3 Calculate the totient value n:

$$\phi(n) = (p\text{-}1) * (q\text{-}1) \quad (2)$$

$$\phi(n) = (51\text{-}1) * (5\text{-}1)$$

$$\phi(n) = (50 * 4)$$

$$\phi(n) = 200$$

4 Determine the value of e with the terms gcd (e, ϕ (n)) = 1
Where e = prime number, and 1 <e <ϕ (n).
Select public key e is 7 (relatively primed tor 200)

5 Looking for exponent deciphering value (d), then:

$$d = (1 + (k \text{ x } \phi(n)) / e) \quad (3)$$

$$d = (1 + (k \text{ x } 200)) / 7$$

The value of k is any number of searches until an integer or integer value is generated. By trying the value of k = 1,2, ..., to obtain the value of d that is round, that is d = 343.

6 From the previously described steps, the values n, e, and d have been obtained so that the key pair has been formed.
Public key pair (n, e) = (255, 7)
The secret key pair (n, d) = (255, 343)

2.2.2 RSA encryption process

For the encryption process uses the public key of the RSA that has been established previously e = 7 by using the formula $a^e \bmod n$ [5].
For example, ICENIS is taken as Plain text.
I have a value of 73 in the ASCII table
C has a value of 67 in the ASCII table
E has a value of 69 in the ASCII table
N has a value of 78 in the ASCII table
I have a value of 73 in the ASCII table
S has a value of 83 in the ASCII table
For the encryption process uses the public key from RSA, which has been formed before that is 7 pieces, using the formula $a^e \bmod n$
73^7 mod 255 = 112 on the ASCII table p
67^7 mod 255 = 118 on the ASCII table v
69^7 mod 255 = 69 on the ASCII table E
78^7 mod 255 = 192 on ASCII table └
73^7 mod 255 = 112 on the ASCII table p
83^7 mod 255 = 212 on ASCII table ╘

After the encryption process using RSA public key has obtained ciphertext which will be used as the plaintext for encryption process using a vigenere cipher.

2.2.3. The formation of vigenere cipher keys

In the first process is done by determining the length of key variables that will be used. In this study, the authors limit the length of values ranging from 0-96. In this study using ASCII code them for mod used mod 256. As for the encryption formula of vigenere cipher is Ci = (pi + ki) mod 256. Plain text used is the result Of the ciphertext contained in the RSA. IE pvE╘p╘. In this study, the authors use the POLSRI key as its public and private key

2.2.4. An Encryption process vigenere cipher

P has a value of 112 in the ASCII table
Shift: (P) -96
80-96 = -16
Ci: 112 + (- 16) mod 256
= 96 in the ASCII table = `
V has a value of 118 in the ASCII table
Shift: (O) -96

79-96 = -17
Ci: 118 + (- 17) mod 256
= 101 in ASCII table = e
E has a value of 69 in the ASCII table
Shift: (L) -96
76-96 = -20
Ci: 69 + (- 20) mod 256
= 49 in the ASCII table = 1
└ has a value of 192 in the ASCII table
Shift: (S) -96
83-96 = -13
Ci: 192 + (- 13) mod 256
= 179 in ASCII table = |
P has a value of 112 in the ASCII table
Shift: (R) -96
82-96 = -14
Ci: 112 + (- 14) mod 256
= 98 in ASCII table = ~
╘ has a value of 212 in the ASCII table
Shift: (I) -96
73-96 = -23
Ci: 212 + (- 23) mod 256
= 189 in ASCII table = ╜

2.2.5. The Decryption process vigenere cipher

For the decryption stage of Vigenere Cipher, the process is almost identical to the encryption process. It's just the mathematical process that distinguishes Ci = (pi-ki) mod 256. With the same key with encryption, as also at the time of decryption is POLSRI Has a value of 96 in the ASCII table

Shift: (P) -96
80-96 = -16

Ci: 112+(-16) mod 256
=96 in the ASCII table = `
v has a value of 118 in the ASCII table
Shift: (O) -96
79-96=-17
Ci : 118+(-17) mod 256
=101 in the ASCII table = e
E has a value of 69 in the ASCII table
Shift : (L)-96
76-96=-20
Ci : 69+(-20) mod 256
=49 in the ASCII table = └
└ has a value of 192 in the ASCII table
Shift : (S)-96
83-96=-13
Ci : 192+(-13) mod 256
=179 in the ASCII table = |
~ has a value of 98 in the ASCII table
Shift : (R)-96
82-96=-14
Ci : 98-(-14) mod 256
= 112 in the ASCII table =
Has a value of 189 in the ASCII table
Shift : (I)-96
73-96=-23
Ci : 189-(-23) mod 256
=212 in the ASCII table ╘

2.2.6. RSA decryption process

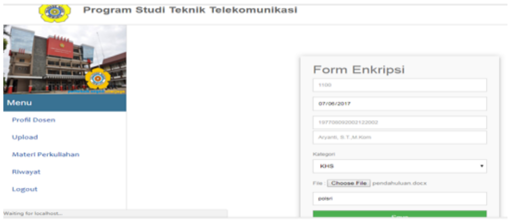
In the RSA decryption process, use the specified private key that is d = 343
112^{343} mod 255 = 73 on the ASCII table I
118^{343}mod 255 = 67 on the ASCII table C
69^{343}mod 255 = 69 on the ASCII table E
192^{343}mod 255 =78oin the ASCII table N
112^{343} mod 255 = 112 on the ASCII table I
212^{343} mod 255 =83 on the ASCII table S

3 Results and discussion

3.1 Program Implementation

3.1.1 Testing of encryption and decryption process

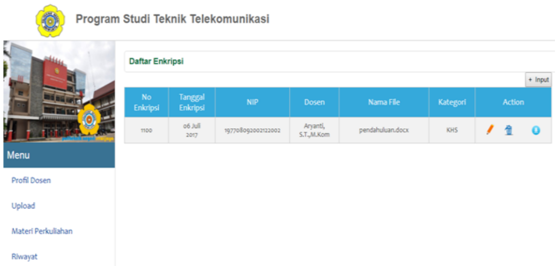
For testing, performed the process of encryption and decryption as shown below. In this menu will be the file encryption process. Before the process of uploading password input for the file can be maintained its security. Then click save, then the encryption process will run and will generate a random file



Form Enkripsi
1100
07/06/2017
197708092002122002
Aryanti, S.T.,M.Kom
Kategori
KHS
File : Choose File pendahuluan.docx
polsri

Fig. 2. Shows the encryption form

Files that have been successfully encrypted will appear on the encryption list.



Daftar Enkripsi

No Enkripsi	Tanggal Enkripsi	NIP	Dosen	Nama File	Kategori	Action
1100	06 Juli 2017	197708092002122002	Aryanti, S.T.,M.Kom	pendahuluan.docx	KHS	

Fig. 3. Shows the encryption list

In the decryption process can be done in the file list. Encrypted files can be downloaded and use the same password during the encryption process. If the password differs between encryption and decryption, then the file will not be a decrypted file or an actual file.

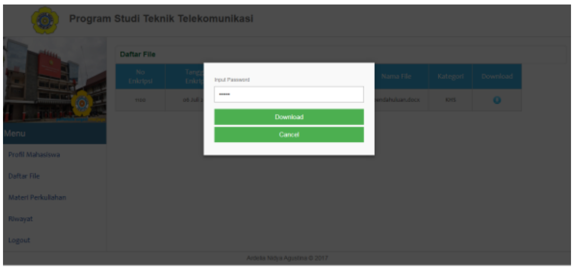
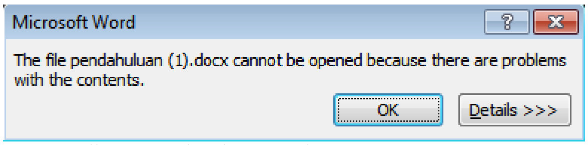


Fig. 4. Display input decryption password

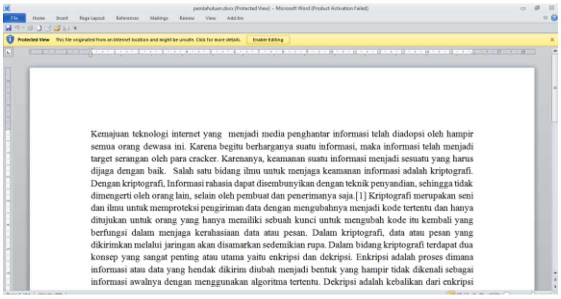
Figure 4 is a password input view. When the student encryption process first input password. If the password is correct then the downloaded file will be decrypted. But if the password is wrong the downloaded file is an encrypted file or a random file that cannot be read.


Microsoft Word

The file pendahuluan (1).docx cannot be opened because there are problems with the contents.

Fig. 5. File cannot be decrypted

Figure 5 incorrect password of the downloaded file is an encrypted file or a random file that cannot be opened.



This file originated from an Internet location and might be unsafe. Click for more details.

Kemajuan teknologi internet yang menjadi media penghantar informasi telah diadopsi oleh hampir semua orang dewasa ini. Karena begitu berharganya suatu informasi, maka informasi telah menjadi target serangan oleh para cracker. Karenanya, keamanan suatu informasi menjadi sesuatu yang harus dijaga dengan baik. Salah satu bidang ilmu untuk menjaga keamanan informasi adalah kriptografi. Dengan kriptografi, Informasi rahasia dapat disembunyikan dengan teknik penyandian, sehingga tidak dimengerti oleh orang lain, selain oleh pembuat dan penerimanya saja.[1] Kriptografi merupakan seni dan ilmu untuk memproteksi pengiriman data dengan mengubahnya menjadi kode tertentu dan hanya ditujukan untuk orang yang hanya memiliki sebuah kunci untuk mengubah kode itu kembali yang berfungsi dalam menjaga kerahasiaan data atau pesan. Dalam kriptografi, data atau pesan yang dikirimkan melalui jaringan akan disamarkan sedemikian rupa. Dalam bidang kriptografi terdapat dua konsep yang sangat penting atau utama yaitu enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi atau data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi

Fig 6. File Decryption

Figure 6 is the result of the file successfully decrypted. When downloading the file, first enter the password. The file will be decrypted if the password is correct.

3.2 Discussion

To analyze the security of files, it is necessary to check the file. Is the file perfectly encrypted so that information on the file cannot be accessed by unauthorized people.

In the tests that have been performed on the file "data2.docx", the original file structure or files that have not been decrypted can be viewed as follows. The encrypted file is named data2 (1). Here is an encrypted file structure in hexadecimal form.

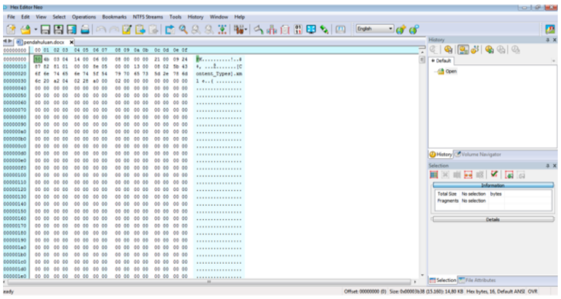


Fig 7. View Files"data2.docx in hexadecimal"

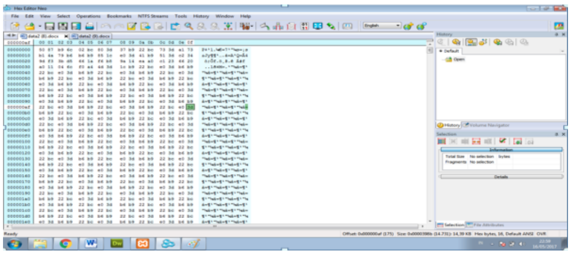


Fig 8. View Files "Data2 (1) .docx in hexadecimal"

In Figure 8 is the structure of the file "Data2 (1) .Docs" in the left side of the display shows the file structure in the form of hexadecimal, while on the right is the character form (ASCII) of hexadecimal. Can be seen in the picture above. Both of them have different results. This can prove that the "Design Diagram.docx" file is successfully encrypted. To prove that the application is running well, we can do the decryption process to file "Data2 (1) .Docs"

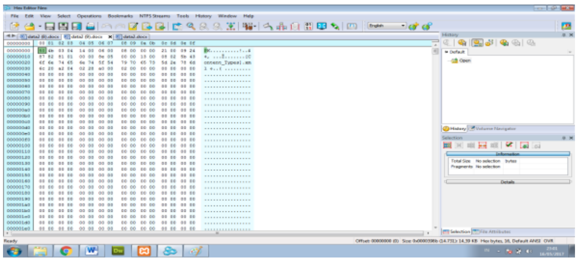


Fig 9. View Files "Data2 (2) .docs" in the decimal, hex

Figure 9 shows that the file decryption process is successful. Can be seen from its file structure.

4 Conclusions

From the research conducted can be seen that the implementation of RSA and Vigenere Chiper algorithm on the WEB-based information system is successfully encrypted and decrypt the file well. Test results show that the system can encrypt files, decrypt files and transmit files. Tests performed on the process of encryption and decryption of files with different file sizes, file size affects the process of encryption and decryption. The larger the files size the longer the process of encryption and decryption.

References

1. JB, R. Kristoforus and BP. Stefanus Aditya. *Impl of Rijndael Algthm for Encrypt and Decrypt In Dgtl Img.* Yogyakarta (2012)
2. N. Aini, DA. Ningrum, Pradhipta M RSA *Algthm Impl for Encryp and Decrypt Using Java Progrm Language on Netbeans* (2012).
3. EK. Nurnawati, *National Appl Science and Tech. IST AKPRIND* Yogyakarta (2008)
4. *RSA*Algthm:www.dimgt.com.au/rsa_alg.html
5. Evgeny Milanov, *"The RSA Algthm"*, June. pp. 1-11(2009)