Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 7 – No. 17, June 2018 – www.caeaccess.org

Document Office Safety Application using Asimetric Cryptography Algorithm RSA

Susanto
Department of Informatics Engineering Faculty
Musamus University, Merauke Papua Indonesia

ABSTRACT
Document has an important role in the efficiency of time and work. Document is a media of information storage such as text, images, or graphics. The security aspect of important documents is necessary, unfortunately this aspect is usually ignored, even excluded. This case can cause serious problems and could be harmful to the owner of the document. This study aims to perform document security by using Asymmetric Cryptography Algorithm RSA (Rivest Shamir Adleman).

The design of document security application is using Asymmetric Cryptography Algorithm RSA (Rivest Shamir Adleman). The process of securing documents was done with two types of keys: public keys and private keys that both locks can be set up to 1024 bits or more. The system was built by using Microsoft Visual C# 2010 software. The tests were conducted on thirty-six document samples.

The result which can be obtained from this study indicates that the application of securing office document by using Asymmetric Cryptography RSA (Rivest Shamir Adleman) algorithm with key length 1024 Bit succeeded in performing keyword generation function by changing the form of number and irregularly arranged random symbols and samples of encrypted documents in the text file format (*.txt).

Keywords
Application, Cryptography, Document, RSA (Rivest Shamir Adleman)

1. INTRODUCTION
We ask that authors follow some simple guidelines. In essence, we ask you to make your paper look exactly like this document. The easiest way to do this is simply to download the template, and replace the content with your own material.

Background of study

Document is a tool which is used to store information in the form of text, images, or graphics. The use of document has already covered several sectors such as business, health and others. Document is the main point for an institution or organization. The information can be in the form of data concerning finances and formal contracts that are stored in document form. The information can help an institution or organization to continue to grow.

Documents are letters or valuable items, including records that can be used as evidence to support information to be more convincing. Nowadays, document can be distinguished into two form file, they are soft file document and hard file document.

The use of electronic documents is required to always secure the information contained in the document, whether it is private or corporate. But in the reality, the awareness of information security is low, security is often a matter of little concern, even eliminated [1]. This will be a serious problem when information is scattered due to theft, tapping, or falsifying information will cause a bad effect or even harmful to the owner of the information stored in the document.

One of the ways that can be used in securing information is by utilizing cryptographic technology to create office document security applications. Asymmetric Cryptography Algorithm RSA (Rivest Shamir Adleman) is an encryption method that uses complex mathematical calculation process. It is also accompanied by public and private key that serves to reduce the risk of infiltration and breaking of information by irresponsible parties that often occur when the document is brought by different person or when sent over the network / internet.

1.1 Identification of the Problem
- Information security in the form of important office documents is still low.
- Understanding of cryptographic functions in securing information in the form of important office documents is still limited.

1.2 The problem of study
How to secure information in the form of important office documents by using Asymmetric Cryptography Algorithm RSA (Rivest Shamir Adleman). What is the function of office document security application by using Asymmetric Cryptography RSA (Rivest Shamir Adleman)

1.3 The purpose of the study
To secure important office documents containing text, images and graphics using Asymmetric Cryptography RSA (Rivest Shamir Adleman) based on desktop applications.

Establish systems that can perform cryptographic functions such as creating public keys and private keys, encryption and decryption in securing documents containing important office text, images, and key algorithms using Asymmetric Cryptography RSA (Rivest Shamir Adleman) to the user

1.4 Scope and Limitation
Document format to be secured are from Ms Office 2003, Ms Office 2010, and PDF (Portable Document Format) with .doc, .docx, .xls, .xlsx, .ppt, .pptx, .mdb, .accdb, and .pdf with the size of each sample is under 2 Megabytes

The program which is used for cryptographic application creation is Microsoft Visual C# 2010.

The length of the key which is used for testing Office Document Security (Office) by using Asymmetric Cryptography Algorithm RSA is 512 bit and 1024 bit.

Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 7 – No. 17, June 2018 – www.caeaccess.org

There is no discussion about the captivity of encrypted documents Asymmetric Cryptography Algorithm RSA (Rivest Shamir Adleman).

2. THEORETICAL FRAMEWORK

2.1 Review of Literature

A similar research that has been done is RSA Cryptography on Client-Server Based Transfer File Application. The result of this study indicates that RSA Cryptography Algorithm can be applied in FTP (File Transfer Protocol) client software such as filezilla by using upload time and result in better security. The application can be implemented to all file types with a maximum size of 9 megabytes due to the limited memory of JVM (Java Virtual Memory) [2].

The other research is focused on Securing Digital Land Certificate by using SHA-512 and RSA Digital Signature. The result of this study indicates that the digital land certificate security system by using xref table can identify the presence or absence of significant changes in the digital certificate document file so it can be concluded that the system can verify the authenticity of the files by using SHA-512 and RSA by using the calculation process of xref table [5].

Another study entitled "The Application of Asymmetric Cryptographic Algorithms RSA for Data Security at Oracle." The result of this study indicates that the application of RSA asymmetric cryptography algorithm can be applied to database and data type of Oracle scalar varchar2 to maintain data security and rank function in Oracle PL / SQL (Procedural Language / Structured Query Language) cannot handle large fraction numbers. Therefore, java classes are used to perform calculations [6].

2.2 Cryptography

Cryptography is the science of encryption techniques in which data is randomized by using an encryption key, and it becomes to be difficult to read or even unable to read by a person who does not have a decryption key. Decryption uses the decryption key to recover the original data [7].

A cryptography algoritm is a mathematical function used in the encryption and decryption process. Its work in combination with a key, a word, number or phrase to encrypt the text. The security of encrypted data is depend on two things, the strenght of the cryptography and the secrecy of the key[3].

Encryptoin is the process of transforming plaintext data into something that appear to be random and meaningless, called ciphertext. Decryption is the process of converting cipher text back to plaintext [4].

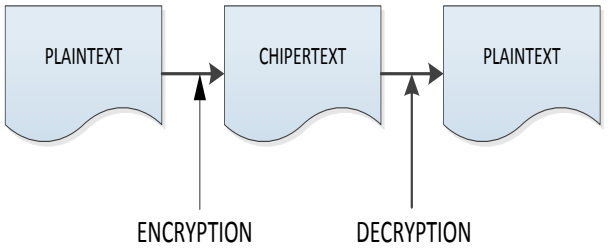

Figure 1: Encryption and Decryption Process

2.3 Asymmetric Cryptography Logarithm

Asymmetric Cryptography Algorithm is cryptography that has a pair of cryptographic keys that are public key and private key. The process of description made is only one, and it is only reserved by the author to decrypt it which is called private key.

The advantage of this asymmetry cryptographic algorithm is to correspond secretly with many parties which is not required the generation of secret keys as much as the number of parties receiving the documents, but simply create two keys which is called public-key for correspondents to encrypt messages, and private-key to decrypt the message [9].

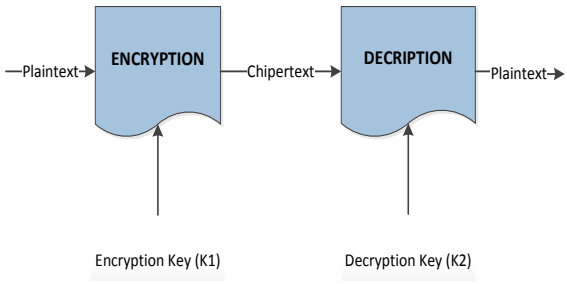

Figure 2: Encryption Process and Description of Process

2.4 RSA (Rivest Shamir Adleman)

Len Adleman, Ron Rivest and Adi Shamir published the RSA Asymmetric Cryptography Algorithm system in 1978. Originally the system was patented in the United States and should be patent-out in 2003, but RSA Security abandoned the patent after September 20, 2000 [7].

RSA (Rivest Shamir Adleman) expresses the original text that is encrypted into blocks in which each block has a binary number value given the symbol "n", the block of original text "M"and the text block code "C". To encrypt the message "M", the message is divided into numeric blocks which is smaller than "n" (binary data with the largest rank). If a prime number with a length of 200 digits, it can be added a few bits 0 in the left of the number to keep the message less than "n", RSA is divided into two processes such as the generation of key pairs, encryption, and decryption with examples of the questions below [1].

Generating of Key Pairs (Public and Private)

p and q of prime number	(secret)
n = p.q	(Public)
$\Phi(r) = (p - 1)(q - 1)$	(secret)
e (Encryption key)	(public)
d (Description key)	(secret)
m (plaintext)	(secret)
c (chipertext)	(Public)

In generating key pairs, the selected value is p = 47 dan q = 71 (it is required that both numbers are primes). Then it is calculated as:
n = p.q = 3337
Φ (r) = (p - 1) (q - 1) = 3220
The public key selected is e = 79, because:
(FPB/GDC dari (79, 3337))
3337 , 79 = 42 dengan sisa 19
79 , 19 = 4 dengan sisa 3
19, 3 = 6 dengan sisa 1

It is selected to the public key pair as e and n that is (79 and 3337). Then, it is calculating the key of d:

$$d = \frac{1+(k \times 3220)}{79} = \frac{1+(25 \times 3220)}{79} = 1019$$

Therefore, the calculation of the key given result as private

and public key:

Public Key (e = 79, n = 3337),

Private key (d = 1019, n = 3337)

Encryption and Description of RSA
Encryption: Symbol message m = BAUTS (no spacing) Then it is converted from ASCII code (American Standard Code for Information and Interchange) into 6665858483. The value of m is divided into blocks which is smaller in form of 2 digits or double blocks:

m_1= 66, m_2= 65, m_3= 85, m_4= 84, m_5= 83
When it is found that the public key is e=79 and n=3337, it becomes time to encrypt each blocks og plaintext as follows:

$c_1 = 66^{79} \bmod 3337 = 795$;
$c_2 = 65^{79} \bmod 3337 = 541$;
$c_3 = 85^{79} \bmod 3337 = 3048$;
$c_4 = 84^{79} \bmod 3337 = 1995$;
$c_5 = 83^{79} \bmod 3337 = 2251$;
So, the chipertext result is: c = 795 541 3048 1995 2251

The description is performed by using the private key of d = 1019. The blocks of chipertext is described below:

$m_1 = 795^{1019} \bmod 3337 = 66$;
$m_2 = 541^{1019} \bmod 3337 = 65$;
$m_3 = 3048^{1019} \bmod 3337 = 85$;
$m_4 = 1995^{1019} \bmod 3337 = 84$;
$m_5 = 2251^{1019} \bmod 3337 = 83$;
The block of another plaintext is returned by using the similar way. Finally the original plaintext is recovered as previous form: m = 6665858483

Those numbers which is in the coding system of ASCII (American Standart Code for Information Interchange) are : m=BAUTS (no spacing)

2.5 Security of Asymmetric Cryptography Algorithm RSA

The security of this asymmetric cryptography algorithm RSA (Rivest, Shamir, Adleman) is concerned to the difficulty of factoring large number into factor of prime number. In Asymmetric Cryptography Algorithm RSA (Rivest, Shamir, Adleman) the problem of factoring such as: invoice n becomes two prime number factor, p and q, into n = p . q. Once n is succesfully factored into p and q, then $\Phi(n) = (p - 1)(q - 1)$ can be calculated. Furthermore, because the encrypted key e published (public), then the decription key of d can be calculated from the similarity form of $e \cdot d = 1 \pmod{\Phi}n$

3. SYSTEM DESIGN

3.1 Hardware Requirement

The role of hardware in supporting the system by using a laptop with these following specifications such as:

1. Processor Intel Celeron CPU N2840
2. Monitor 10,1”
3. Keyboard
4. Mouse
5. Hardisk 500 GB
6. RAM 2 GB

3.2 Software Requirement

The role of software in supporting and creating a system can be specified into the following part :

1. Operation System of Windows 8 x64 bit
2. Microsoft visual C# 2010 to create and run a program
3. Microsoft visio to create the system flow in the process.
4. Microsoft office to design user interface.

3.3 The Proposed System

The flowchart below shows the proposed system.

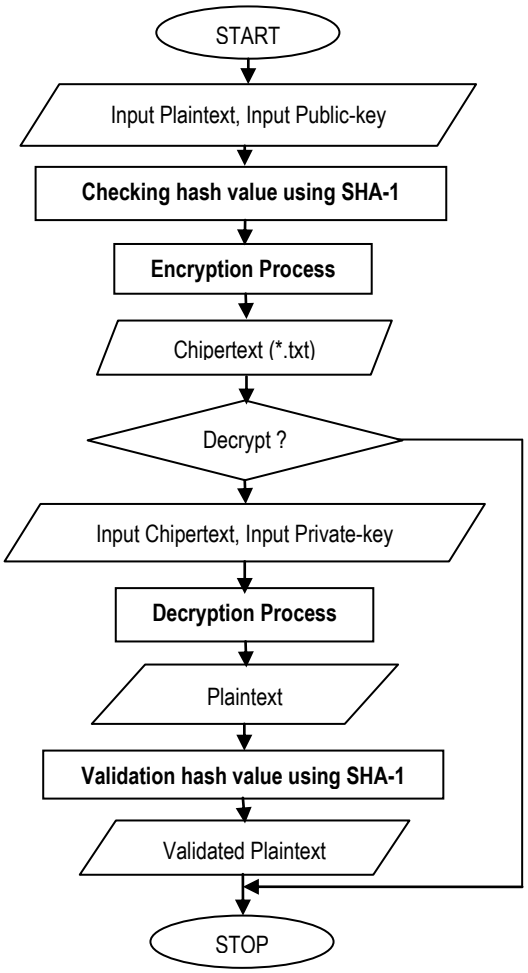

Figure 3: Flowchart Encryption and Description of RSA

3.3 The Proposed Display Design

Main Form of Design Display on Encryption and Description Process

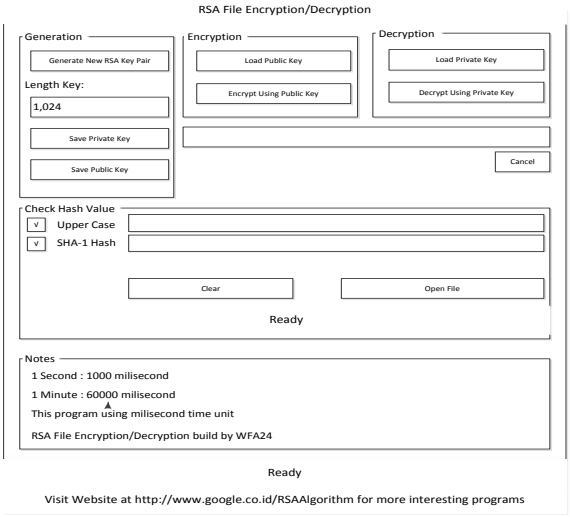

Figure 4: Main Form Design

Main Form, there are various functions in main form such as the generation of two pair of keys, key length settings, lock storage on the computer, encryption and decryption, calculation of encryption and decryption time, progress bar to know the level of encryption and decryption process, and checkbox SHA-1 Hash file to search hash value.

4. RESULT AND DISCUSSION

4.1. Main Displayed Menu

The Form of Main Display has ten buttons which can be used regularly by the user such as" Generate New RSA Key Pair", "Save Public Key", "Save Private Key", "Load Public Key", "Encrypt Using Public Key", "Load Private Key", "Decrypt Using Private Key", "Cancel", "Clear", and "Open File". The following chart is the form of Main Menu:

Figure 5: The Display Form of Main Menu

4.2 Encryption Testing

Table 1: Encryption testing of Microsoft Office 2010 Document Format (.docx)

File Name	Sample Size (kB)	Encryption Time (ms)
TEST SAMPLE (1).docx	100	1470
TEST SAMPLE (2).docx	344	3382
TEST SAMPLE (3).docx	544	3907
TEST SAMPLE (4).docx	714	4707
TOTAL	**1702**	**13466**

The table shows the result of encryption time in milisecond using Office 2010 Document Format (.docx)

Table 2: Encryption Testing of Microsoft Office 2010 Document Format (.xlsx)

File Name	Sample Size (Kb)	Encryption Time (ms)
test sample (1).xlsx	50 Kb	958
test sample (2).xlsx	100 Kb	1077
test sample(3).xlsx	350 Kb	2862
test sample (4).xlsx	502 Kb	3885
TOTAL	1002 Kb	8782

The table shows the result of encryption time in milisecond using Office 2010 Document Format (.xlsx)

4.3 Decription Testing

Tabel 3: Decription testing of Microsoft Office 2010 Document Format (.docx)

File Name	Size (Kb)	Decryption Time (ms)
test sample(1).docx	400 Kb	10729
test sample (2).docx	1374 Kb	41435
test sample (3).docx	2175 Kb	55582
test sample (4).docx	2854 Kb	72100
TOTAL	6803 Kb	179846

The table shows the result of decryption time in milisecond using Office 2010 Document Format (.docx)

Tabel 4: Description Testing of Microsoft Office 2010 Document Format (.xlsx)

File Name	Size of Encrypted Sample (kB)	Description Time (ms)
test sample (1).xlsx	198	5434
test sample (2).xlsx	398	10566
test sample (3).xlsx	1400	34897
test sample (4).xlsx	2005	50713
TOTAL	**4001**	**101610**

The table shows the result of decryption time in milisecond using Office 2010 Document Format (.xlsx)

4.4 Key Generation Speed Testing

The tables below shows the test result key generation speed using RSA and WFA software

Table 5: Test Results Key Generation Speed Using RSA-Keygen Software Windows 7

Key Length (bit)	Test I (ms)	Test II (ms)	Test III (ms)
512	610	790	660
1024	710	770	600

Table 6: Testing Key Generation Speed Using WFA Software 24

Key Length (bit)	Test I (ms)	Test II (ms)	Test III (ms)
512	760	720	860
1024	740	810	810

The table below shows the average key rate speed generation

Table 7: Average Key Rate Speed Generation Using RSA-Keygen Software Windows 7 and WFA 24

Length Key (bit)	Average Rate Speed of Generating Key Using Software (ms)	
	RSA-Keygen Windows 7	WFA 24
512	686,66	780
1024	693,33	786,66

There are no significant diferences result in two key length and two key rate speed generation.

4.5 Encryption Speed Testing

The table below shows the Result of Encryption Speed Testing Using Software RSA-Keygen Windows 7 and WFA 24.

Table 8: The Result of Encryption Speed Testing Using Software RSA-Keygen Windows 7 and WFA 24

Key Length (bit)	Encryption Speed (ms)	
	RSA-Keygen Windows 7	WFA 24
512 bit	540	117
1024 bit	990	143

The table shows that encryption using WFA24 faster than RSA-Keygen Windows 7.

4.6 Decription Speed Testing

The table below shows the Result of Deccription Speed Testing Using Software RSA-Keygen Windows 7 and WFA 24

Table 9: Result of Decription Speed Testing Using Software RSA-Keygen Windows 7 dan WFA 24

Key Length (bit)	Description Speed (ms)	
	RSA-Keygen Windows 7	WFA 24
512 bit	630	error
1024 bit	1220	216

The table shows that decryption using WFA24 faster than RSA-Keygen Windows 7.

5. CONCLUSION

Testing information security in the form of important documents of the office is running well in the form of text file with the arrangement of numbers, letters, and symbols arranged randomly when encrypted by using Asymmetric Cryptography RSA (Rivest, Shamir, Adleman) with key length 1024 Bit.

Office Document Security Application (Office) Using Asymmetric Cryptography RSA (Rivest, Shamir, Adleman) can perform public or private key generation functions repeatedly, and it can be saved, also adjustable to key length (1024 Bit or more).

Need more research using many type of file (plaintext) and other encryption methodes to knows the results as comparisson.

6. BIOGRAPHIES OF AUTHORS

Author, received bachelor's of Informatics from AKAKOM, Yogyakarta, Indonesia in 2000, received Master of Informatics Engineering from Hasanuddin University, Makassar, Indonesia in 2011, Currently, he is a lecturer at Department of Informatics Engineering in Universitas Musamus, Merauke, Papua, Indonesia.

7. REFERENCES

[1] Ariyus, D. 2008. Pengantar Ilmu Kriptografi: Teori, Analisis, dan Implementasi, Andi, Yogyakarta.

[2] Arief, M. 2015. Kriptografi RSA Pada Aplikasi File Transfer Client-Server Based, Jurnal, Universitas Telkom, Bandung .

[3] Ayushi, 2010, A Symetric Key Cryptographic Algoritm, International Journal of Computer Application, (0975-8887), Volume 1 – No. 15.

[4] Rahman, MM., Akter T., Rahman A., 2016, Development of Cryptiography-Based Secure Messaging System, Journal of Telecommunication System & Management, DOI: 10.4172/2167-0919.1000142.

[5] Refialy, L. 2015. Pengaman Sertifikat Tanah Digital Menggunakan Digital Signature SHA-512 dan RSA, Jurnal, Salatiga : Universitas Kristen SatyaWacana

[6] Wibowo I. 2009. Penerapan Algoritma Kriptografi Asimetris RSA Untuk Keamanan Data Di Oracle, Jurnal, Yogyakarta : Universitas Kristen Duta Wacana.

[7] Kromodimoeljo, S. 2009. Ebook Teori dan Aplikasi KriptografI, Indonesia : SPK IT.

[8] Qiong Huang, Duncan S. Wong. 2008. On the relation among various security models for certificateless cryptography. Int. J. of Applied Cryptography.Vol. 1. No.2.

[9] Sanchita Paul, Tausif Anwar, Abhishek Kumar. 2016. An innovative DNA cryptography technique for secure data transmission. Int. J. of Bioinformatics Research and Applications. Vol. 12. No.3.

[10] Prakash Kuppuswamy, Saeed Q.Y. Al-Khalidi. 2014. Hybrid encryption/decryption technique using new public key and symmetric key algorithm. Int. J. of Information and Computer Security 2014.Vol. 6. No.4.