International Journal of Pure and Applied Mathematics
Volume 117 No. 15 2017, 805-816
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

CRYPTOGRAPHIC ALGORITHM WITH APPLICATIONS RC4 AND RSA WEB BASED ON PT PACKET SYSTEMS INDONESIA

Ady Widjaja[1],Mujito[2], Adam Kalabadzi[3]

Email : ady_w168@yahoo.co.id,jitosalemba@gmail.com,kalabadzi@gmail.com

ABSTRACT - Cryptography is a method of encryption of data that can be used to maintain the confidentiality of data, the authenticity or integrity of the data, as well as the authenticity of the sender. This method aims so that important information is limited or secret sent by means of public telecoms cannot be known or utilized by parties who are not entitled to. PT Packet Systems Indonesia is a company engaged in the field of providers IT services often use other media such as email or FTP in distributing data or information such as device configuration of telecommunications-related devices, such as a cisco router, switches and firewalls. The data is vulnerable once stolen by other parties with the intent that is not good. If the data that fell to a person who is not entitled to can easily read its contents and utilized for find out the gaps that exist on the device or communications network or even access into device or communications networks. Therefore it takes a cryptographic system so that the important data the company can do the process safeguards, so as to avoid theft, wiretapping and hijacking important data which becomes the secret of the company. Use of the cryptographic system double is intended so that data is not easily exploited due process safeguards the data being done twice so the data has security that double as well. Although the application was built using symmetric algorithm RC4 and RSA asymmetric, however not required distribution of private key and public key because the private key and the public key will be raised on the basis of symmetric key being entered when performing encryption.Authentication facilities and protection of data integrity, because it uses a hash function to the method SHA256. The programming language used in building this data security application is the language programming PHP (PHP: Hypertext Preprocessing) based web. The results of testing this binary cryptography, data can be secured in order to avoid double attack cryptanalysis. Then the time it takes to perform encryption and decryption, depending on the size of data/file, as well as the hardware specification is used.

Keyword: Data security, encryption, cryptography, RC4, RSA, SHA 256

1. Introduction

In addition to a wide range of benefits offered with the use of information technology, there is a the dangers posed by the existence of possibility of data leakage or misuse the data can be catastrophic for an organization. To resolve this problem required a system safeguards against communication networks, in particular the communication between computers that are owned by an organization. In data communications, There is a method of encryption (Bavisha. T.E and MadlinAsha.M)of data that is known with cryptography (Cryptography). Cryptography a method of securing data can be used to maintain the confidentiality of data, the authenticity or integrity of the data, as well as the authenticity of the sender. This method aims so that important information limited or confidential nature sent through means of public telecoms cannot be known or utilized by parties who are not entitled to. PT Packet Systems Indonesia is a company in the IT services provider in the process of its business solution that is often going on Exchange of information or data that important and confidential between fellow employees or with customers, either through the medium of email or other media such as FTP. Important data This device configuration such as routers, switches, and Firewall belongs to the customer. This data is vulnerable once for the stolen and utilized by the parties are not responsible, because when the data read by a party which is not responsible can be utilized to infiltrated the network of customers and an attack that ultimately affect business processes of the customer. To maintain confidentiality, authenticity and integrity such important data required a system reliable encryption. With this encryption system only those who are eligible who have the key who can read the data. In the unlikely event the data falls to the parties that are not interested parties, will remain safe because those data already encrypted. With this data encryption system that previously could be read by all can be read only by those who are entitled who has the key. To further secure the encryption process and detulisan scientific, a mechanism needs to be done that provides little likelihood so that the original data can not be disassembled by an attacker. So the author uses 2 algorithms in doing the process of encryption and detulisan scientific, i.e. algorithms symmetric and asymmetric algorithms RSA RC4. With using

the RC4 algorithm and a combination of RSA data security generate expected to which has a higher level of security. Especially for data – data device configuration telecommunications so that the data cannot be stolen by the attackers.

2. The Cornerstone Of The Theory

Data security is one of the important factors to look for computer users. If No, a variety of important data may be intercepted, or even taken by parties that are not entitled. Computer security (computer security) covers four aspects [2], namely:

a. Privacy/Confidentiality, i.e. the effort of keeping data information from people who are not entitled to access (make sure that the data or personal information We keep private).
b. Integrity, i.e. the attempt to keep the data or the information may not be modified without the permission of the owner information.
c. Authentication, i.e. the effort or the method for State that the information is exactly original, accessing or providing the information is exactly the person who referred to, or the server which we call was exactly the original server.
d. Availability, related to the availability of system and data (information) when needed.

2.1. Cryptography (Cryptography)

Cryptography appears to answer the needs of data security. Cryptography itself comes from languages of Greece, namely the crypto and graphia. Crypto own means secret (secret), whereas the graphia means writing (writing). According to terminology Cryptography is the science and art to keep security message when the message is sent from an place to another. Cryptography may also defined as the study of the technical math-related aspects security information such as data confidentiality, the validity of the data, data integrity, and data authentication. Cryptographic algorithm consists of three basic functions [1], IE:

a. Encryption (Encrypt), is the safeguarding of data submitted in order to be maintained in strict confidence. Original message called plaintext, which is converted into codes that are not understood.
b. Decrypting (Decrypt), is the antithesis of encryption. The message that has been encrypted (ciphertext) restored to its original form (plaintext), called by decrypting the message.
c. key (Key), the key question here is the key used for encryption and decryption. The key is divided into two parts: secret key (private key) and public key (the public key).

2.2 The Rc4 Cryptographic Algorithms

Cryptographic algorithm Rivest Cipher 4 (RC4) It is one of the key symmetrical algorithms by RSA Data Security Inc. (RSADSI) which shaped as a stream cipher. This algorithm was found in 1987 by Ronald Rivest and become RSA Security symbol (stands for three inventors: Rivest Shamir Adleman). RC4 is a proprietary encryption symmetric stream created by RSA Data Security Inc. (RSADSI). Disclosure of a source code believed to be the RC4 and published in ' anonymously ' in 1994. The algorithms This is identical to published implementation of RC4 on official products. RC4 widely used in some applications and commonly expressed very secure. RC4 is not patented by RSADSI, just not traded freely (trade secret). RC4 is one form of stream cipher which is a lot used in the encryption protocols, such other WEP, WPA, and SSL/TSL. RC4 is the one type of stream cipher, i.e. process unit or input data, message or information at a time. The unit or data is generally a byte or sometimes even a bit (byte in terms of RC4). In this way the encryption or decryption can implemented on a long variable. Algorithm This does not have to wait a certain amount of input data, the message or specific information before being processed, or Add an extra byte for encryption. RC4 algorithm using two pieces of S-Box that is an array that contains all 256 permutations of numbers 0 to 255 S-Box, and the second, containing the the permutation is a function of keys with the length of the variable. RC4 evokes the flow of bits pseudorandom (keystream). As with any stream cipher, it can be used for encryption with combine the plaintext using XOR, decryption is done the same way (because exclusive or operation is symmetric). Similar to the Vernam cipher except that pseudorandom bits are produced, not the flow of prepared, used To generate the keystream, the cipher uses a secret internal State consisting of two section:

a. a permutation of all 256 bytes Maybe (denoted "S" below).
b. Two 8-bit index-pointers (denoted "i" and "j"). Permutation intialized with key length variable, typically between 40-2048 bits. First array S are initialization with the identity permutation. S then processed for

256 iterations in a way that is the same as the PRGA, but also in the combination with the key at the same time. To generate the RC4 keystream, using internal State which includes two parts:

1). Stage Key Scheduling Algorithm (KSA)

where state automaton is given initial values based on the encryption key. State that are the initial value in the form of an array represent a permutation with 256 elements, so the results of the algorithm KSA is the initial permutation. Array have a 256 element (with index 0 up to 255) was named Following S. is in a form of pseudocode for the algorithm of KSA where key is the encryption key and keylength is great the encryption key in the bytes (128 bit key, keylength = 16).

```
for i from 0 to 255
    S[i] := i
endfor
j := 0
for i from 0 to 255
    j := (j + S[i] + key[i mod keylength]) mod 256
    swap values of S[i] and S[j]
endfor
```

2). Stages Of Pseudo Random Generation Algorithm (PRGA)

In which the state operates and automatons produces the output keystream. Each round, part of the keystream of 1 byte (with a value of between 0 up to 255) in-output by PRGA based on state S. Here are the PRGA algorithm in the form of pseudo-code:

```
i := 0
j := 0
while GeneratingOutput:
    i := (i + 1) mod 256
    j := (j + S[i]) mod 256
    swap values of S[i] and S[j]
    K := S[(S[i] + S[j]) mod 256]
    output K
endwhile
```

The value of K which is then used as the keystream. The value of k which is already obtained from the steps above are then put in the operation XOR with the plaintext, with earlier the message is first cut into byte. After the operation is done, step 1) back done to get new index of each element of S. In the encryption process flowchart RC4 can be seen as Figure 1 and 2.

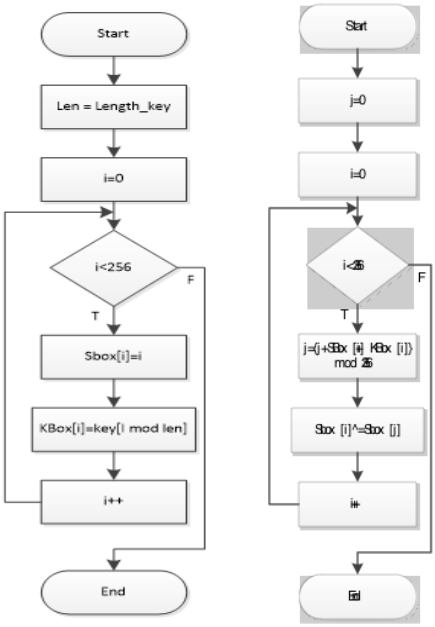

Figure 1: Flowchart of the process initialization and permutations SBox RC4

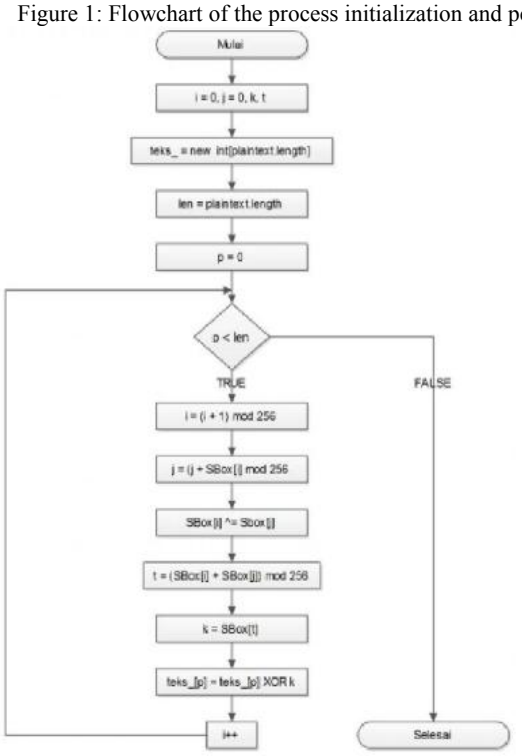

Figure 2: RC4 encryption process Flowchart

2.3 RSA Cryptographic Algorithms

RSA is an asymmetric cryptographic algorithms, where the key used to encrypt the different from the one used to decrypt. The key used to encrypt the called with the public key, and is used to decrypting it is called

with the private key. RSA is one of the cryptographic algorithms that use the concept of public key cryptography. The RSA requires three steps in the process, namely the generation keys, encryption, and decryption. The process of encryption and decryption is the process that is almost the same. If the resurrected strong random numbers, it will be It's harder to do a cracking against the message. Powerful parameter whether a lock is present on the the magnitude of random numbers are used. RSA algorithms described in 1976 by three people: Ron Rivest, Adi Shamir and Len Adleman from the Massachusetts Institute of Technology. Letter " RSA " itself comes from the initials of their names (' R'ivest-S'hamir ' – ' A'dleman). Clifford Cocks, a mathematician working for United Kingdom GCHQ, the outlines of the system on equivalen an internal document in 1973. The Discovery Of Clifford Cocks was not revealed until 1997 due to the reason the top-secret " classification ". RSA Algorithm patented by the Massachusetts Institute of Technology in 1983 in the United States as a US patent 4405829. The patent is valid to 21 September 2000. After September the year 2000, the patent expires, so the current everyone can use it freely. RSA is an algorithm based on schema public-key cryptography. Further, RSA is the algorithm is easy to implement and to understand. the RSA algorithm is an application of the many theories such as extended Euclid algorithm, the euler's function to fermat's theorem. Fundamental concepts of public-key cryptography invented by Whitfield Diffie and Martin Hellman, and separately by Ralph Merkle. While basic concepts of public-key cryptography is located at understanding that the key is always in pairs: the key encryption and decryption key. Also keep in mind that a key can not be raised from the key others. Understanding encryption and decryption key often referred to as a public key and a private key. Someone should give public keys in order to the other party can encrypt a message. Decryption only happen if someone has a private key. The RSA algorithm is based on Euler's theorem that States that:

$a\phi(n) \equiv 1 \pmod{n}$

provided that a relative had to be primed against n.

Based on theorem-a theorem on the discussion kekongruenan before, can we get:

$a\phi(n) \equiv 1 \pmod{n}$

Based on $ap \equiv bp \pmod{m}$:

$\approx ak\phi(n) \equiv 1\ k \pmod{n}$

a m is replaced with:

$\approx mk\phi(n) \equiv 1\ k \pmod{n}$

Both sides are multiplied by m:

$\approx mk\phi(n) + 1 \equiv m \pmod{n}$ (second segment multiplied by the m)

Equation 1:

For example, e and d are selected such that $ed = 1 \pmod{n}$ or $ed = k\phi(n) + 1$.

Then substitution to Equation 1:

$Med \equiv m \pmod{n}$

$(me)\ d \equiv m \pmod{n}$

The above equation can be interpreted as exponentiation of m by e followed by exponentiation with d yield return m. Then based on These equations, encryption and decryption on the RSA

It can be formulated as follows:

$EE(m) = me \pmod{n} = cDc(c) = cd \pmod{n}$

a. The RSA Generation Algorithm

The advantages of RSA lies in pairs the key used to encrypt the and decrypt the message. The following step by step used for RSA key pair aroused:

1) Select two primes any p and q in the application. Cryptography in the wake, the value of p is generated from the second character from the secret key input added decimal 50 then selected numbers the nearest Prime and q is taken from the third character of the secret key that the inputted added decimal 10, then selected primes nearby. Or it could be written as the following::
   P = next prime > K [1] + 50
   Q = next prime > K [2] + 10
2) Calculate $n = p * q$, with $p \neq q$.
3) Calculate phi/totient$\phi(n) = (p-1)(q-1)$
4) Select key public e, relative prima against $\phi(n)$. e said relative prime against the totient in fpb of e and the totient = 1
5) Lift the private key $d = 1 + k\,\phi(n)/e$ or $e\text{-}1\ d = (1 + k.\ \phi(n))$.
   The result of the algorithm above is:
   a) public Key (n, e)

b) private key (n, d)

b. The Encryption And Decryption Algorithm

On the RSA encryption algorithm is as the following:

1) Grab Grab key public property message recipients (n and e).
2) Plainteks Broke into blocks m1, M2, ..., such that each block represents a value in the interval [0, n-1].
3) Each block being encrypted block mi CI = ci with the formula mi e mod n
4) to get the plainteks back, block cipherteks ci decrypted into block mi with the formula mi = ci d mod n

For example the known plaintext and key as the following:

Plaintext = ADAM

Key = SALEMBA

Initial steps i.e. do key generation with the stage as follows:

a). Find the value of p and q,

p = next prime > K [1] + 50, where K [1] = A value is decimal 65

p = next prime > 65 + 50

p = next prime > 115

p = 127

q = next prime > K [2] + 10, where K [1] = L that has a value of byte 76

q = next prime > 76 + 10

q = next prime > 86

q = 89

b). Calculate the value of n,

n = p x q, where p and q = 127 = 89

n = 127 x 89

n = 11303

c). Calculating the totient,

$\phi(n) = (p-1)\ (q-1)$

$\phi(n) = (127-1)\ (89-1)$

$\phi(n) = 126\ 88$

$\phi(n) = 11088$

d). Select the key public reltive e, which primed against ϕ (n). the e relative said prima against $\phi(n)$

If gcd/fpb of e and $\phi(n) = 1$ Select e > 2 and gcd (e, 11088) = 1

By using the algorithm of Euclid, sample We select e = 5.

11088:2217 = 5 with the remaining 3

5:3 = 1 with the remaining two

3:2 = 1 with a remainder of 1

e). Lift the key private d, where d = 1 + k ϕ (n) /e or d e-1 = (1 + k. ϕ (n)) or d. e mod totient = 1, then come by d = 6653

We stopped because it gets the value 1, so e = 5

f). Thus obtained:

Public key = (e, n) = 5.11088

Private key = (d, n) = (6653.11088)

g). Perform the encryption against a plaintext with formula:

For i = 0, i <strlen (plaintext), the i ++

CI = mi

e mod n

Cipher from A = 655 mod 11088 = 3766

Cipher from D = 685 mod 11088 = 6072

Cipher from A = 655 mod 11088 = 3766

Cipher from M = 775 mod 11088 = 9535

Cipher text from ADAM was 3766.6072.3766.9535

h). Decrypt against plaintext with formula:

For i = 0, i <strlen (plaintext), then i ++

MI = ci

d mod n

Cipher from A = 37666653 mod 11088 = 65 = A

Cipher of D = 60726653 mod 11088 = 68 = D
Cipher from A = 37666653 mod 11088 = 65 = A
Cipher from M = 95356653 mod 11088 = 77 = M
So come by the plaintext = ADAM

2.4 Data Structure

As has been explained earlier that at When performing decryption process there is a process hashing, which had been pasted on the file results of encryption with the use of algorithms SHA256. The following is a data structure from a file the encryption process has done, looks like in Figure 3.

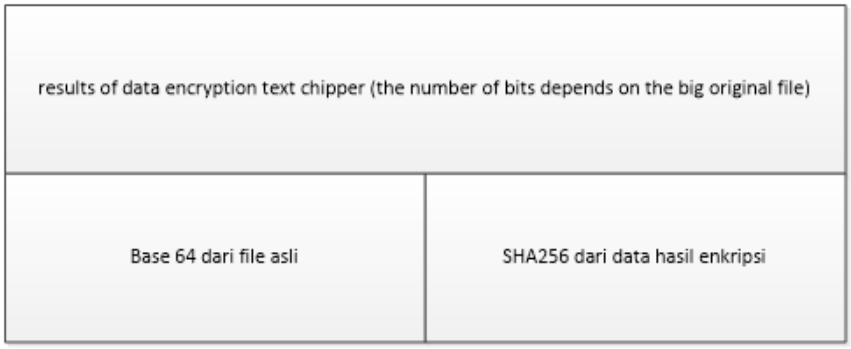

Figure 3: structure of the data file encryption results results

3. The Design Of The System And Application

The design is a process that is done to design the application. The design of the system made in General is to encrypt and decrypt using the method of the RC4 cryptographic algorithms and RSA-based web.

3.1. Design application page

The following page design application that has been designed based on their respective functions:

1. Login page

The early stage in design is the page login, like Figure 4.

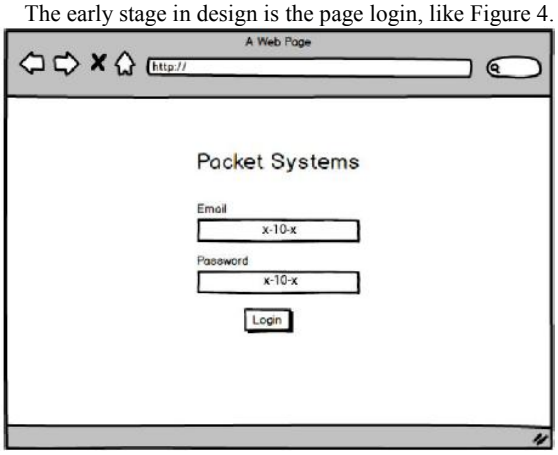

Figure 4: design form login screen display

2. Home page

The next step in the design is the application options page, as seen in Figure 5.

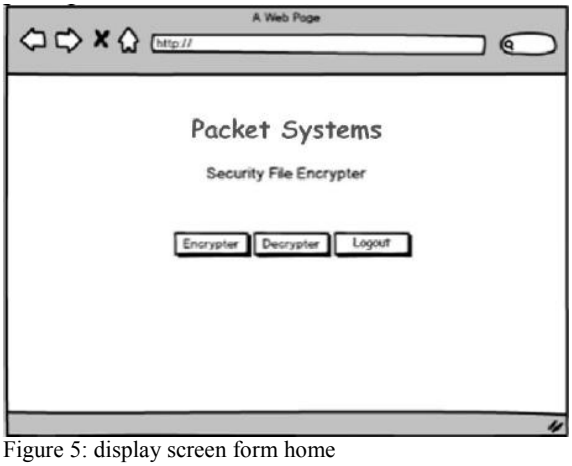

Figure 5: display screen form home

3. Page Encrypter/Decrypter
The design of the page when the menu at encrypter Select as in Figure 6.

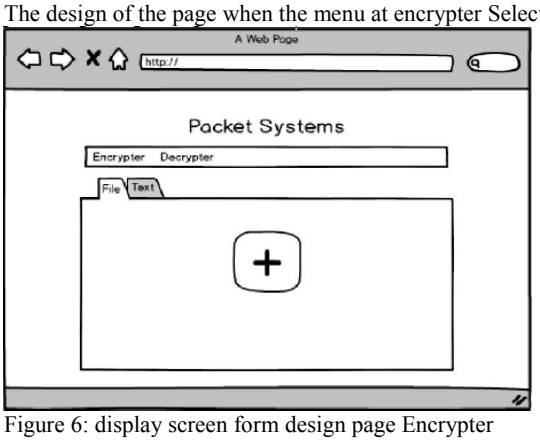

Figure 6: display screen form design page Encrypter
On the page will direct encrypter displayed menu file encryption, and then there is menu for file encryption options or text, on this display format there are some parts function as follows:
1) files, function as an option to file encryption
2) Text, for encryption of text to a menu
3) Add file area, serving to enter file will be encrypted When a file is included, it will come out look like in Figure 7.

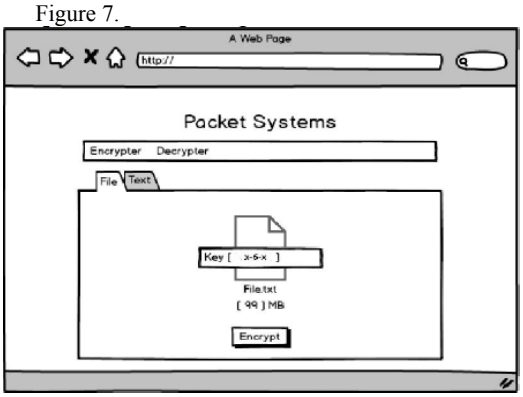

Figure 7: display screen file input form

When the encryption process was successful there will be size comparison of files between file before encrypted and which has successfully encrypted, the on a file that has been encrypted the file extension will changed to psi. In this menu there are the Download option to download the file has been encrypted. Like the boom of the figure 8.

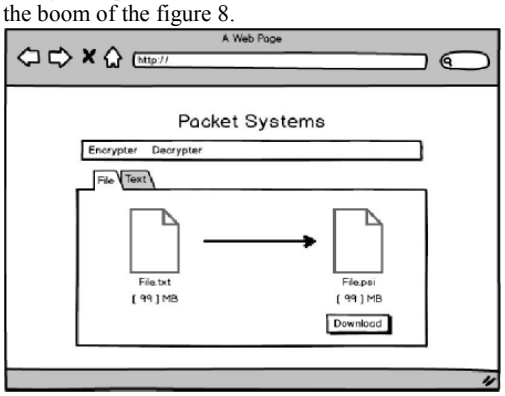

Figure 8: display screen form encryption successfully

4. Results And Discussion

In this discussion, carried out 10 times more tests the file to different formats. The result of the the test is done, the file is successfully do data security processes, so that the parties others cannot see the contents of the data indeed. The example pdf file will do the encryption process can be seen in Figure 9 below:

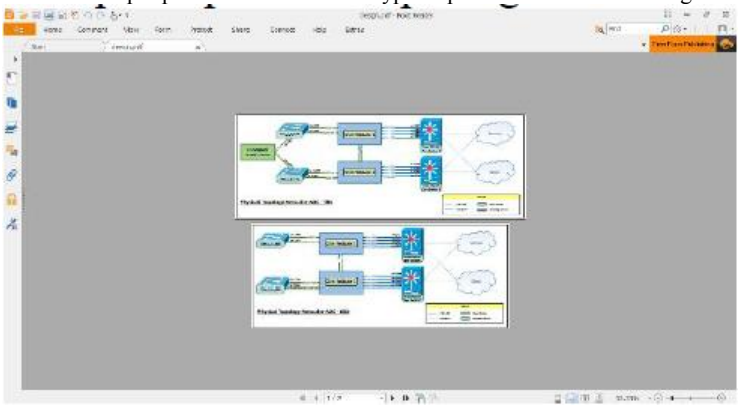

Figure 9: PDF files before encryption

Encryption results file with extension. as can be seen in Figure 10, the following:

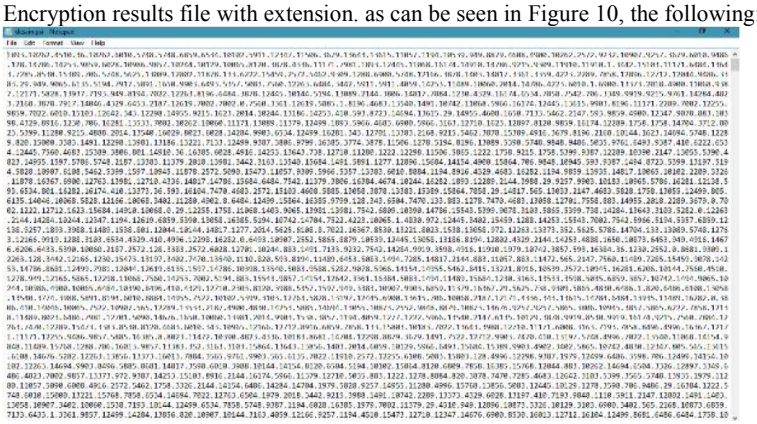

Figure 10: File after encryption

Table 5: table of results a test encryption and decryption

No	File Before Encrypt			File After Encrypt			Encryp Time (ms)	Decrypt Time (ms)	Presentase Size Changes	Avg time Encrypt/byte	Avg time Decrypt/byte
	File Name	Format	Size (bytes)	File Name	Format	Size (bytes)					
1	archive	.rar	390994	archive	.psi	2103346	1699	327991	537.95%	0.004345335	0.15593773
2	artikel	.docx	421051	artikel	.psi	2264966	2256	358967	537.93%	0.005358021	0.158486706
3	audiomsg	.mp3	59318	audiomsg	.psi	319168	267	56671	538.06%	0.004501163	0.177245213
4	design	.pdf	424163	design	.psi	2281654	1796	360972	537.92%	0.004234221	0.158206284
5	layer1	.png	84177	layer1	.psi	452882	337	79102	538.01%	0.004003469	0.174663599
6	layer3	.jpg	264011	layer3	.psi	1419852	1647	260328	537.80%	0.006238376	0.183348687
7	note	.xlsx	8724	note	.psi	47009	38	8040	538.85%	0.0043558	0.171031079
8	topologi	.vsd	146944	topologi	.psi	789995	642	138146	537.62%	0.004369011	0.174869461
9	videomsg	.mp4	471012	videomsg	.psi	2534235	2010	398032	538.04%	0.004267407	0.157061993
10	sample4	.docx	1058080	sample4	.psi	5691389	4036	906687	537.90%	0.003814456	0.159308562
Average									538.01%	0.004548726	0.167015931

5. Conclusions And Suggestions

The conclusion to be drawn from scholarly writings, as the following:

a. Data can be secured with the algorithm RC4 and RSA Cryptography,
b. The time required to perform encryption and decryption, depending on the size of data/files, as well as the hardware specification used,
c. Change size on the file once done encryption algorithm RC4 and RSA double which is about 538% with encryption time per bytes required is ms and 0.0045 decryption time needed per byte is 0, 167ms,
d. Look at the magnitude of the change in size of the file and also the time it takes to perform encryption and decryption, then the file should processed with this application a maximum of 1 MB for encryption and decryption for 5 MB.
e. The existence of this data security applications, It is expected that PT Packet Systems Inodnesia ready to respond to security issues will the data.

This application is still not perfect and still needs to be repair-repair. Some suggestions that can be given to improve the quality of the application These include:

a.The encryption result file size can be reduced by applying compression process.
b.In order to perform encryption and decryption on a data/files with a greater size (> 1MB),
c.In order to perform the encryption process and decryption with less time,
d.Implementation and testing in order to use the hardware specification or higher software to get the best results.

BIBLIOGRAPHY

a. Ariyus, Dony 2008, PengantarIlmuKriptografiTeoriAnalisisdanImplementasi, Yogyakarta, CV Andi Offset.
b. Gupta, SouravSen, et. al. 2014, Journal of Cryptology, JurnalDepartemnt of Computer Science and Engineering Jadaspur University Vol.27 Issue 1
c. Hakim, ElkaLukman, Khairil, Utami, FerryHari 2014, AplikasiEnkripsi Dan tulisanilmiah Data MenggunakanAlgoritma Rc4 DenganMenggunakanBahasaPemrogramanPhp, Bengkulu, Jurnal Media Info Utama, Vol 10 No.1.
d. Jumrin, Sutardi, Subardin 2016, AplikasiSistemKeamanan Basis Data DenganTeknikKriptografi Rc4 Stream Cipher, JunalTeknikInformatikaUniversitasHaluole, ISSN : 2502- 8928, Vol2 No.1.
e. Kurniawan, Yusuf 2004, KriptografiKeamanan Internet &JaringanKomunikasi, Jakarta,Informatika.
f. Lestari, Puji 2013, ImplementasiAlgorithmaRsa (Rivest Shamir Adleman) DalamSistemEnkripsi File Dan Pengamanan Folder, Jogjakarta, JurnalTenikInformatika UIN Sunan Kali Jaga.
g. Mujiarto, Duwi 2014, APLIKASI PENGAMAN DATA MENGGUNAKAN ALGORITMA RSA (Rivest-Shamir-Adleman), Surabaya, JurnalTeknikInformatikaUniversitas Pembangunan Nasional.

h. Munir, Rinaldi 2006, Kriptografi, CetakanPertamaPenerbitInformatika, Bandung.
i. Nugroho, Adi 2008, AlgoritmadanStruktur Data DalamBahasa Java .Yogyakarta :penerbitAndi.
j. Prajapati, Priteshkumardkk, 2014, Comparative Analysis Of Des, Aes, Rsa Encryption Algorithms, India, Department of Information Technology ISSN No.: 2250-0758.
k. Saipul, 2011, ImplementasiTandaTangan Digital MenggunakanFungsi Hash AlgoritmaSha 256 Dan RsaDalam Proses Otentikasi Data, TulisanilmiahUniversitas Ahmad Dahlan.
l. Setiawan, Okie , Fiati, Rina , Listyorini, Tri 2014, AlgoritmaEnkripsi Rc4 SebagaiMetode Obfuscation Source Code Php, JurnalTeknikInformatikaUniversitasMuria Kudus, ISBN 978-602-1180-04-4.
m. Bavisha .T.E and MadlinAsha.M, "A Keyword Based User Privacy-Preservation and Copy-Deterrence Scheme for Image Retrieval in Cloud", International Journal of Innovations in Scientific andEngineering Research (IJISER), ISSN: 2347-971X (online), ISSN: 2347-9728(print), Vol.4, no.1, pp.30-35, 2017, http://www.ijiser.com/.
n. Rajesh, M., and J. M. Gnanasekar. "Annoyed Realm Outlook Taxonomy Using Twin Transfer Learning." International Journal of Pure and Applied Mathematics 116 (2017): 547-558.
o. Rajesh, M. & Gnanasekar, J.M. Wireless Pers Commun (2017),https://doi.org/10.1007/s11277-017-4565-9
p. Rajesh, M., and J. M. Gnanasekar. "GCCover Heterogeneous Wireless Adhoc Networks." Journal of Chemical and Pharmaceutical Sciences (2015): 195-200.
q. Rajesh, M., and J. M. Gnanasekar. "CONGESTION CONTROL IN HETEROGENEOUS WANET USING FRCC." Journal of Chemical and Pharmaceutical Sciences ISSN 974: 2115.
r. Rajesh, M., and J. M. Gnanasekar. "GCCover Heterogeneous Wireless Ad hoc Networks." Journal of Chemical and Pharmaceutical Sciences (2015): 195-200.
s. Rajesh, M., and J. M. Gnanasekar. "CONGESTION CONTROL USING AODV PROTOCOL SCHEME FOR WIRELESS AD-HOC NETWORK." Advances in Computer Science and Engineering 16.1/2 (2016): 19.
t. RAJESH, M. "TRADITIONAL COURSES INTO ONLINE MOVING STRATEGY." The Online Journal of Distance Education and e-Learning 4.4 (2016).
u. Rajesh, M. "Object-Oriented Programming and Parallelism."
v. Rajesh, M., K. Balasubramaniaswamy, and S. Aravindh. "MEBCK from Web using NLP Techniques." Computer Engineering and Intelligent Systems 6.8: 24-26.