Analysis of Combination RSA Algorithm using EM2B Keys Genertor Algorithm in Data Encription

Elwin Yunith Purba[1], Syahril Efendi[1], Pahala Sirait[1], Rahmad W. Sembiring[2]
[1]*Department of Informatics Engineering, "Universitas Sumatera Utara"*
Jl. Universitas Kampus USU, Medan, 20155, Sumatera Utara
[2]*Politeknik Negeri Medan, Medan-Indonesia*

Keywords: Cryptography, Encryption, Decryption, RSA Algorithm, EM2B Key Generator.

Abstract: In this increasingly sophisticated era almost all circles of government, industry, business to individual companies do computer work. In addition to the advantages that can be obtained from the use of computers, the most important thing to note is part of the security, if information / data stored on the computer damaged due to interference from hackers it can lead to huge losses as well. There are many cryptographic algorithms such as One Time Pad, RC4, RSA, and so on that are considered really capable of maintaining the security and confidentiality of the data. Therefore cryptographers are trying to create complex algorithms to better ensure their safety. Of the many public key cryptography algorithms ever made, the most popular algorithm is the RSA algorithm. RSA algorithm is a modern cryptographic algorithm that is often used for data security, until now still no one can solve it. RSA algorithm security lies in the difficulty of factoring large numbers into prime factors. The factoring is done to obtain private key. During the factoring of large numbers into prime factors has not found the right algorithm, so long as it is also RSA algorithm security is guaranteed. The combination of RSA algorithm with EM2B Key Generator can secure data more difficult to solve, and able to overcome the problem of execution time of encryption and decryption.

1 INTRODUCTION

Information Technology has caused a change and a way of looking at human life as well as an organization. Such rapid development brought the world into a new era faster than ever imagined. Such a computer that not only serves as a data processing tool, but has become a major weapon in competing. This is because with the computer can simplify and accelerate a job in accessing information (Pahrizal, David Pratama, 2016). Of the many advantages derived from the use of technology, not least the opportunity losses contained in it either a small loss or a big loss can even lead to someone lose everything. Some examples of hacking cases in 2016 include Ransomware emerges as a top cyber threat to business, UK second only to US in DDoS attacks, 412 million user accounts exposed in FriendFinder Networks hack, Financial Conduct Authority concerned about cyber security of banks and other cases caused by the weakness of the security system. For that required a computer security system. Security of data in a computer is very important to protect the data from other parties that do not have the authority to determine the content of the data (Zaeniah, Bambang Eka Purnama, 2015). Security concerns relate to risk areas such as external data storage, dependency on the public internet, lack of control, multi-tenancy and integration with internal security (K Hashizume et al, 2013).

2 LITERATURE REVIEW

Cryptography from Greek , "hidden, secret" respectively is the practice and study of techniques for secure communication in the presence of third parties (called adversaries). More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Modern cryptography intersects the disciplines of

Purba, E., Efendi, S., Sirait, P. and Sembiring, R.
Analysis of Combination RSA Algorithm using EM2B Keys Genertor Algorithm in Data Encription.
DOI: 10.5220/0010039401220128
In *Proceedings of the 3rd International Conference of Computer, Environment, Agriculture, Social Science, Health Science, Engineering and Technology (ICEST 2018)*, pages 122-128
ISBN: 978-989-758-496-1

mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce (M. Preetha, M. Nihiya, 2013).

Cryptography is one field of science that studies about information security / data to avoid the adverse effects of misuse of information by irresponsible parties. Cryptography has an important role in maintaining the confidentiality of information both in the computer and at the time of transaction data. Cryptography also uses techniques applied for encryption and decryption (William Stallings, 2011).

In the field of cryptography there are several techniques available for encryption / decryption. This technique can generally be grouped into two major groups, namely conventional and public key cryptography (Sundram Prabhadevi, Rahul De, Pratik Shah, 2013). To determine the Cryptographic algorithm that will be used in data security system in addition to consideration of strength against Cryptanalis and Bruteforce attacks is no less important is the consideration of speed. At present there are various algorithms of cryptography as well as symmetry and asymmetry. If a cryptographic algorithm is believed to be robust, but it is known to be slow in its encoding process it will not be user choice. This consideration of speed will be more important, if the use of Cryptographic algorithms concerning computer networks, especially on clien-server architecture (K Hashizume et al, 2013).

RSA is one of the modern cryptographic algorithms that until now is still widely developed by researchers. The RSA algorithm was made by three researchers from MIT (Massachusetts Institute of Technology) in 1976. The name RSA is an abbreviation of the name of the three inventors, namely Rivest, Shamir, and Adleman. RSA algorithms do factoring of very large numbers into prime factors. Factoring is done to obtain private key (Muhammad Arief, Fitriyani, Nurul Ikhsan, 2015).

2.1 *Rivest-Shamir-Adleman* (RSA)

The RSA is an algorithm used by modern computers to encrypt and decrypt. It is a type of an asymmetric cryptographic algorithm. RSA algorithm includes two keys a public key and a private key. The public key is distributed to all so will be known to everyone, it is used to encrypt datas. Datas encrypted with public key only decrypted with private key (S. Kamara, and K. Lauter, 2010). RSA can be used for digital signatures, key exchange, or encryption of small block data. The size of the key that is used by RSA algorithm is variable not fixed and also the size of the encryption block. RSA has been widely used for establishing a secure communications channel and for authentication and the identity of the service provider over insecure communication medium (K., Dr Ch., and S. Yogesh, 2013). In proposed scheme RSA algorithm is used to find out the key pair for both mobile user and third party auditor. These keys are used to encrypt and decrypt the file (W. , C. , et al. 2010). The figure below illustrates the work of the RSA Algorithm:

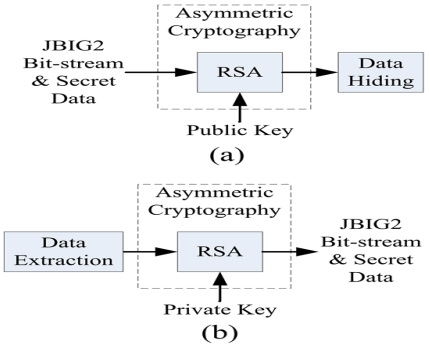


Figure 2.1: Working of RSA

RSA algorithm has the following scale:

1. p and q are primes → Secret
2. $n = p\,q$ → Not a secret
3. $(n) = (p-1)(q-1)$ → Secret
4. e (Encryption key) → Not a secret

   Stipulation: PBB $(e, (n)) = 1$
5. d (Decryption key) → Secret

   d Calculated from $d \equiv e - 1 \bmod ((n))$
6. m (Plaintext) → Secret
7. c (Ciphertext) → Not a secret

The following procedures describe the encryption and decryption of RSA (D.Welsh, 1998):

1. Choose two prime numbers, a and b → Secret
2. Calculate the product $n = a\,b$.
   Magnitudes of n no need to be kept secret.
3. Calculate $(n) = (a-1)(b-1)$.
4. Select an integer for the public key, say its name e, which is relatively prime against (n).
5. Calculate the decryption key, d, through
   $ed \equiv 1 \pmod{m}$ or $d \equiv e - 1 \bmod (\varphi (n))$

   Results from the above algorithm:
1. The public key is a couple of (e, n)
2. Private key is couple of (d, n)

2.2 EM2B Key Generator Algorithm

EM2B key algorithm is an algorithm that functions to change the primary key into a new key that is

converted into ASCII characters. The EM2B algorithm also has an increment key algorithm that works if the key length is less than the length of the plaintext. Increment key is a method to add key character length by summing two previous key characters and is modulated with 256 ASCII-based letters. The EM2B algorithm has the following equation:

$$K_{i\,[new]} = [\, K_i + (K_i \bmod 26) \,] \bmod 256 \qquad (2.1)$$

Explanation:

a. K_i = The Main Key,
b. K_j = The Main Key do mod with 26 (K_i mod 26),
c. $K_{i\,[new]}$ = New Key Generated.

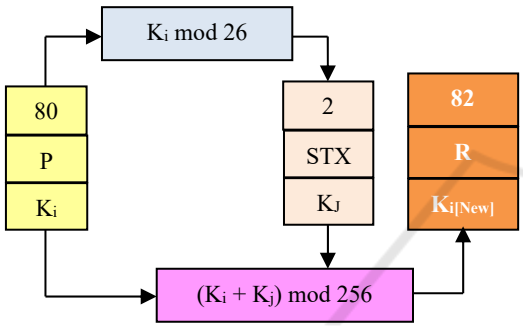


Figure 2.2: The Process of EM2B Key Generator Algorithm

As for icreament key algorithm:

$$IncK_i = K_{i\,[max]} + K_{i[max]\,-\,1} \bmod 256 \qquad (2.2)$$

Explanation:

a. $K_{i[max]}$ = The last Key index in ASCII,
b. $IncK_i$ = Icreament Key,

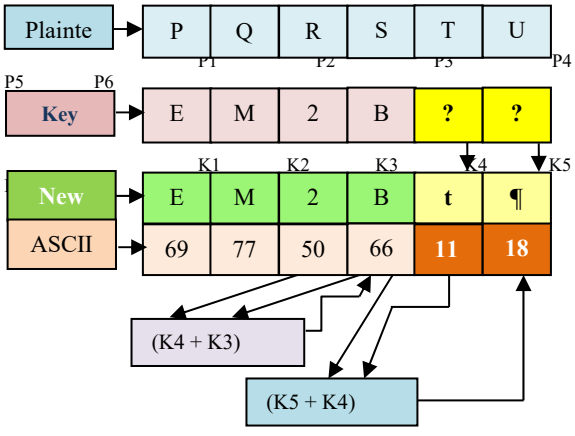
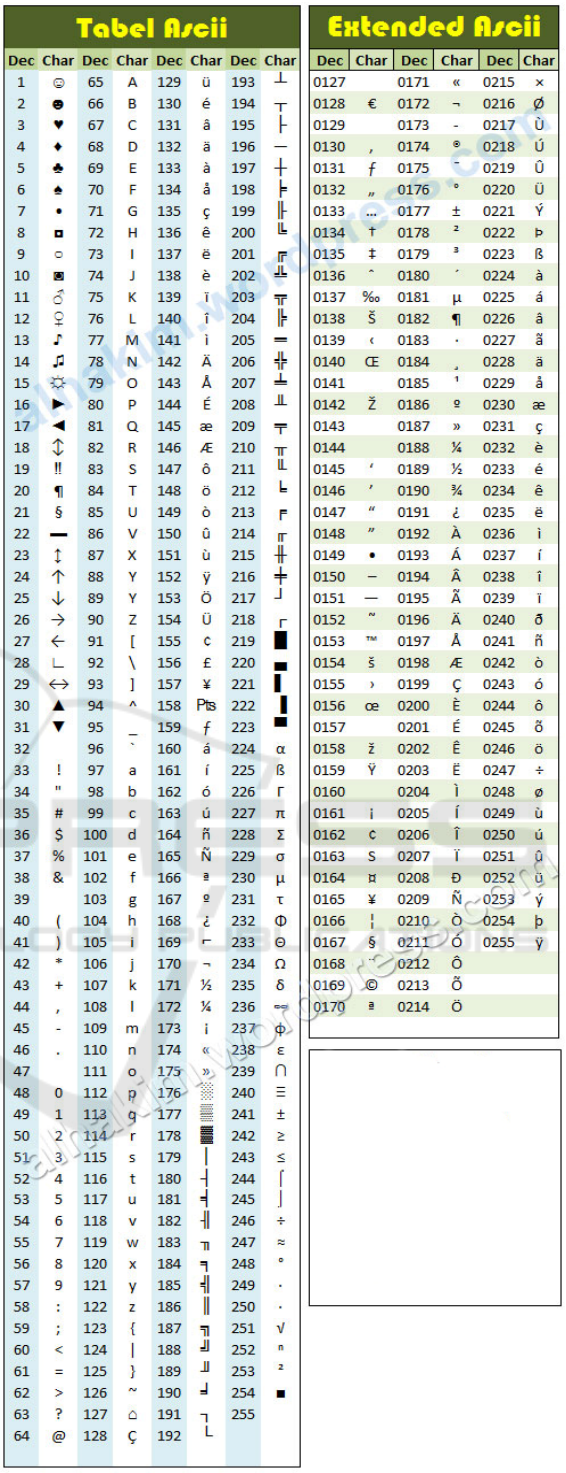


Figure 2.3: The Process of Increament Key

To help convert decimal numbers to ASCII code or vice versa, ASCII table is required as shown below:



Tabel Ascii

Dec	Char	Dec	Char	Dec	Char	Dec	Char
1	☺	65	A	129	ü	193	┴
2	☻	66	B	130	é	194	┬
3	♥	67	C	131	â	195	├
4	♦	68	D	132	ä	196	─
5	♣	69	E	133	à	197	┼
6	♠	70	F	134	å	198	╞
7	•	71	G	135	ç	199	╟
8	◘	72	H	136	ê	200	╚
9	○	73	I	137	ë	201	╔
10	◙	74	J	138	è	202	╩
11	♂	75	K	139	ï	203	╦
12	♀	76	L	140	î	204	╠
13	♪	77	M	141	ì	205	═
14	♫	78	N	142	Ä	206	╬
15	☼	79	O	143	Å	207	╧
16	►	80	P	144	É	208	╨
17	◄	81	Q	145	æ	209	╤
18	↕	82	R	146	Æ	210	╥
19	‼	83	S	147	ô	211	╙
20	¶	84	T	148	ö	212	╘
21	§	85	U	149	ò	213	╒
22	▬	86	V	150	û	214	╓
23	↨	87	X	151	ù	215	╫
24	↑	88	Y	152	ÿ	216	╪
25	↓	89	Y	153	Ö	217	┘
26	→	90	Z	154	Ü	218	┌
27	←	91	[	155	¢	219	▉
28	∟	92	\	156	£	220	▄
29	↔	93	]	157	¥	221	▌
30	▲	94	^	158	Pts	222	▐
31	▼	95	_	159	ƒ	223	▀
32		96	`	160	á	224	α
33	!	97	a	161	í	225	ß
34	"	98	b	162	ó	226	Γ
35	#	99	c	163	ú	227	π
36	$	100	d	164	ñ	228	Σ
37	%	101	e	165	Ñ	229	σ
38	&	102	f	166	ª	230	µ
39		103	g	167	º	231	τ
40	(	104	h	168	¿	232	Φ
41	)	105	i	169	⌐	233	Θ
42	*	106	j	170	¬	234	Ω
43	+	107	k	171	½	235	δ
44	,	108	l	172	¼	236	∞
45	-	109	m	173	¡	237	φ
46	.	110	n	174	«	238	ε
47		111	o	175	»	239	∩
48	0	112	p	176	▒	240	≡
49	1	113	q	177	▒	241	±
50	2	114	r	178	▓	242	≥
51	3	115	s	179	│	243	≤
52	4	116	t	180	┤	244	⌠
53	5	117	u	181	╡	245	⌡
54	6	118	v	182	╢	246	÷
55	7	119	w	183	╖	247	≈
56	8	120	x	184	╕	248	°
57	9	121	y	185	╣	249	∙
58	:	122	z	186	║	250	·
59	;	123	{	187	╗	251	√
60	<	124	|	188	╝	252	ⁿ
61	=	125	}	189	╜	253	²
62	>	126	~	190	╛	254	■
63	?	127	⌂	191	┐	255	
64	@	128	Ç	192	└		

Extended Ascii

Dec	Char	Dec	Char	Dec	Char
0127		0171	«	0215	×
0128	€	0172	¬	0216	Ø
0129		0173	-	0217	Ù
0130	‚	0174	®	0218	Ú
0131	ƒ	0175	¯	0219	Û
0132	„	0176	°	0220	Ü
0133	…	0177	±	0221	Ý
0134	†	0178	²	0222	Þ
0135	‡	0179	³	0223	ß
0136	ˆ	0180	´	0224	à
0137	‰	0181	µ	0225	á
0138	Š	0182	¶	0226	â
0139	‹	0183	·	0227	ã
0140	Œ	0184	¸	0228	ä
0141		0185	¹	0229	å
0142	Ž	0186	º	0230	æ
0143		0187	»	0231	ç
0144		0188	¼	0232	è
0145	‘	0189	½	0233	é
0146	’	0190	¾	0234	ê
0147	“	0191	¿	0235	ë
0148	”	0192	À	0236	ì
0149	•	0193	Á	0237	í
0150	–	0194	Â	0238	î
0151	—	0195	Ã	0239	ï
0152	˜	0196	Ä	0240	ð
0153	™	0197	Å	0241	ñ
0154	š	0198	Æ	0242	ò
0155	›	0199	Ç	0243	ó
0156	œ	0200	È	0244	ô
0157		0201	É	0245	õ
0158	ž	0202	Ê	0246	ö
0159	Ÿ	0203	Ë	0247	÷
0160		0204	Ì	0248	ø
0161	¡	0205	Í	0249	ù
0162	¢	0206	Î	0250	ú
0163	Ś	0207	Ï	0251	û
0164	¤	0208	Đ	0252	ü
0165	¥	0209	Ñ	0253	ý
0166	¦	0210	Ò	0254	þ
0167	§	0211	Ó	0255	ÿ
0168	¨	0212	Ô		
0169	©	0213	Õ		
0170	ª	0214	Ö		

Figure 2.4: ASCII Code Table (Source: www.alhakim.wordpress.com)

Another supporting algorithm is Vigenere Cipher. This type of encryption algorithm is well known for being easy to understand and implement.

Techniques to produce ciphertext can be done using the substitution of numbers and square vigènere (Ahmad Rosyadi, 2015). Character letters used in vigenere cipher are A, B, C, ..., Z and equated with the numbers 0, 1, 2, ..., 25. The encryption process is done by writing the key repeatedly. Repeated key writing is performed until each character in the Data has a pair of characters from the key. The characters in the Data are then encrypted using the caesar cipher method with the key value that has been paired with the number (Katz, J. and Y. Lindell, 2015). The encryption process can be calculated by the following equation (Stallings, W, 2011).

$$E_i = (P_i + K_i) \bmod 26 \quad (2.3)$$

where E_i, P_i and K_i are encrypted characters, Data characters and key characters. While the decryption process can use the following equation:

$$D_i = (C_i - K_i) \bmod 26 \quad (2.4)$$

with D_i is a decrypted character, C_i is a ciphertext or password character, K_i is a key character.

3 MATERIALS AND METHODS

In designing a cryptographic algorithm, a maximum accuracy is required. The level of security is the key to the success of the cryptographic algorithm itself. Time efficiency also needs to be considered because if the encryption and decryption process takes a long time, it will be bad for encrypting Datas on a large scale. Broadly speaking the process of encryption and decryption on RSA algorithm implementation and EM2B Keys Generator Algorithm in encrypting data can be observed through the following diagram blog.

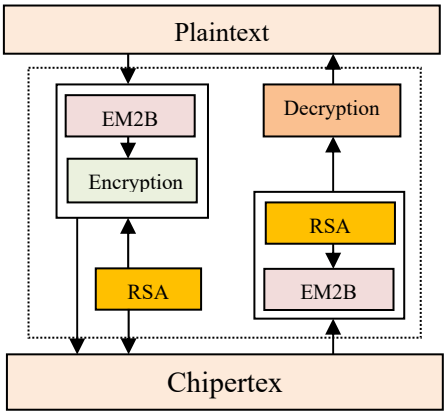


Figure 3.1: Encryption and Decryption Process

In this research used RSA Cryptography Algorithm and EM2B Key Generator to improve the security of encrypted data. It is expected that EM2B Key Generator can be a key algorithm for encrypting plaintext as well as RSA algorithm capability in encrypting keys will make the data very difficult to solve. Therefore it is necessary to analyze each algorithm both RSA and EM2B key generator used in encrypting the data. RSA Algorithm Analysis can be seen as follows:

A. Take randomly two large and different p and q primes, but the size of both or the number of digits in the base of numbers used should be the same.

B. Calculate the n modulus and Euler's Totient function φ (n) by the formula: n = p q
φ (n) = (p – 1) [q - 1]
with :
n = modulus (public key)
p and q = Two primes generated randomly.

C. Select an integer e such that I < e < φ (n) and gcd(e, φ(n)) = 1 where:
I = Integer number,
E = Public Key (Encryption Key),
gcd = Greatest common divisor.

D. Calculate the integer value d where I < d < φ (n)
such that:
d = e – 1 mod φ (n) or I(mod φ (n)),
where:
d = Private Key (Decryption Key).

E. Create a table to present each character.

F. The plaintext (encrypted text) is encrypted with numbers corresponding to the table formed by process E and an M will be obtained which is a collection of numbers from the plaintext, then the set of numbers is blocked every 4 numbers into m_1, m_2, ..., m_n. The encryption process is done per block and each block of the encryption formula is:
$c_1 = m_1^e \pmod n$, $c_2 = m_2^e \pmod n$, ... etc, so resulting in a value of C where C is a collection of numbers from c_1, c_2, ..., c_n.

G. The decryption process is done by using logic like step F by performing an inverse calculation, ie: $m_1 = c_1^d \pmod n$
, $m_2 = c_2^d \pmod n$, ...,etc, so resulting in the value of M where M = m_1, m_2, m_3, the final value of M is re-presented with the constructed table as in process E above.

To improve the security of RSA algorithm, then specified security key in the form of private key password, public key and modulo generated from two prime numbers. This key will continue to be used by the sender and recipient of the data in encrypting and decrypting the data. If the security key password by the system owner is deemed to be insecure, then both parties immediately inform it to be changed altogether. This security key view consists of:

Analysis of EM2B algorithm as follows:

A. Specify some words used as the primary key for encrypting datas. Key is given a symbol with K_i where $K_i = K_1, K_2, ..., K_n$.

B. The key is converted into decimal ASCII numbers.

C. Determine the modulus value of 26 of each key character that has been converted into decimal places.
$K_j = K_i \text{ Mod } 26$.

D. Add K_i with K_j ($K_i + K_j$) then modulated with 256 and generate a new key ($K_{i[new]}$) which is converted in decimal ASCII characters.

In the EM2B algorithm, the key we choose does not have to have the same character length as plaintext. Plaintext may consist of several sentences and even paragraphs. The key will adjust the length of its character with plaintext by using the increament key algorithm already stored in it. The performance analysis of the increment key algorithm can be noted below.

A. The maximum character index is summed with the previous character index ($K_{i[max]} - K_{i[max-1]}$), and generate a new key character index ($K_{i[new]}$).

B. New key index ($K_{i[new]}$) becomes the maximum key index, then added again to the previous key index.

C. This looping step will stop if the maximum index of the key is equal to the plaintext maximum index. $K_{i[max]} = P_{i[max]}$.

The implementation process of RSA and EM2B algorithms in encrypting the data can be explained by the following steps.

A. A data or plaintext is encrypted using a key.

B. First the key is converted into EM2B and then generates a new ASCII character.

$$K_{i\,[new]} = [\, K_i + (K_i \bmod 26)\,] \bmod 256$$

C. If the key length is still smaller than the length of the plaintext, then the key in the process with increament key $IncK_i = K_{i\,[max]} + K_{i[max]\,-\,1} \bmod 256$.

D. Next do the encryption where, every plaintext is added with the key and modulated with 256 to generate a ciphertext. $C_i = P_i + K_i \bmod 256$. Ciphertext in the process is a data that will be sent to the recipient.

E. Then the primary key value is put together into one block and then split into several blocks. The value of each block is not greater than the value of n on the RSA generator.

F. After the block process is done then it is decrypted using RSA. $E_k = M_e \bmod n$. E_k is the encrypted result of K_i.

G. The information sent to the recipient is ciphertext (C_i), and key encryption results (E_k).

Furthermore the following process to decrypt the data.

A. The first stage by decrypting the key using the formula $K_i = D_k = M^d \bmod n$.

B. The decryption results are separated into each two-digit number, which will generate the main key character.

C. The primary key is reprocessed into the EM2B algorithm to generate a new key in the decimal ASCII number.

D. Re-used the increament key algorithm to obtain the same key length as plaintext.

E. After that the ciphertext is decrypted by using the new key, using the equation $P = C - K \bmod 256$.

4 RESULTS AND DISCUSSION

The results offered in this study are methods to improve data security from irresponsible parties. This study provides an example of a process of encryption and decryption. Plaintext used are “HERLINAWATI” with the main key "PURBA" as in the following figure:

Plaintext (P)	H	E	R	L	I	N	A	W	A	T	I
ASCII Code	72	69	82	76	73	78	65	87	65	84	73
EM2B Key Generator And Increament Key											
KEY (K)	P	U	R	B	A						
ASCII Code	80	85	82	66	65	?	?	?	?	?	?
Ki MOD 26	2	7	4	14	13	?	?	?	?	?	?
[Ki + (Ki MOD 26) MOD 256] OR Ki [max] + Ki[max] - 1 mod 256	82	92	86	80	78	158	236	138	118	0	118
Increamnet Key	R	\	V	P	N	ž	ì	Š	v	NUL	v
Encryption with EM2B Generator Key											
P + K MOD 256	154	161	168	156	151	236	45	225	183	84	191
Chipertext	š	¡	¨	œ	—	ì	-	á	·	T	¿

Figure 4.1: EM2B Key Generator Encryption Process

Plaintext is converted into decimal. Then the key is processed with EM2B into characters (R, \, V, P, N), and the key length increases by using increament key. The key generated is ASCII characters. The Generate new keys consist of: (R\VPNžìŠvNULv). The next step is to encrypt the plaintext with a new key that has been generated previously. Cipherteks generated include: (š¡¨œ—ì-á·T¿).

Next the RSA key creation process by following the steps below:

* Find the value of p and q: p & q primes,
* Find p x q to generate the value of n,
* Determine the value of $\varphi(n) = (p-1)*(q-1)$,
* Determine the value of e as the encryption key, e relative prime $1 < e < \varphi(n)$,
* Calculate the value of d as the decryption key.

p	q	n	φ(n)	e	d
7	17	119	96	13	37

Figure 4.2: Key Making In the determination of the key

Determination of Value (e)						
φ(n)	96	48	24	12	37	3,36
Primes	2	2	2	2	11	11
Results	48	24	12	6	3,36	STOP

Figure 4.3: Calculation of Value (e)

Calculation of Value (d)	1	2	3	4	5	6	7
a =	1	0	1	-2	3	-5	
b =	0	1	-7	15	-22	37	
d =	96	13	5	3	2	1	
k =	-	7	2	1	1	2	

Figure 3.5: Calculation of Value (d)

From this process we find the key value for encrypting data on RSA is $e = 13$ and the decryption key is $d = 37$.

Manipulation of Length of EM2B Key Generator							
The Length Of Primary Key	8085826665						
		M1	M2	M3	M4	M5	M6
10	8085826665	80	85	82	66	65	

EM2B Generator Key Encryption With RSA							
P^e MOD n	87	5	58	61	93	67	4
Chipertext	W	ENQ	:	=	]	C	EOT

Figure 4.4: EM2B Generator Key Encryption With RSA

Cipherteks above is an information or data obtained from a combination of several algorithms and their implementation in the information. To decrypt the data obtained test results as follows.

Chipertext	W	ENQ	:	=	]	C	EOT
ASCII	87	5	58	61	93	67	4
Description of EM2B Generator Key With RSA							
Mi - n	M1	M2	M3	M4	M5	M6	
C^d MOD 119	80	85	82	66	65	12	
Join Ci	808582666512						
EM2B Key	80	85	82	66	65		
Key	P	U	R	B	A		

Figure 4.5: Key Decryption Process using RSA algorithm

EM2B Key Generator And Increament Key											
Key	P	U	R	B	A						
ASCII	80	85	82	66	65						
Ki [max] + Ki[max] - 1 mod 256	80	85	82	66	65	131	196	71	11	82	93
Increament Key	P	U	R	B	A	ƒ	Ä	G	VT	R	]

Figure 4.6: Decryption of EM2B Key Generator Algorithm

Chipertext	š	¡	"	œ	–	ì	-	á	·	T	¿
P + K MOD 256	154	161	168	156	151	236	45	225	183	84	191

EM2B Key Generator And Increament Key											
KEY (K)	P	U	R	B	A						
ASCII Code	80	85	82	66	65	?	?	?	?	?	?
Ki MOD 26	2	7	4	14	13	?	?	?	?	?	?
Ki [max] + Ki[max] - 1 mod 256	82	92	86	80	78	158	236	138	118	0	118
Increamnet Key	R	\	V	P	N	ż	ì	Š	v	NUL	v

THE RESULT OF DECRYPTION (Decryption Using EM2B Generator Key)											
ASCII (Ci -Ki) MOD 256	72	69	82	76	73	78	65	87	65	84	73
Plaintext	H	E	R	L	I	N	A	W	A	T	I

Figure 4.7: Ciphertext Decryption with EM2B Key Generator Algorithm

5 CONCLUSION

Based on the results of the above discussion, it can be concluded that: The application of data security using RSA algorithm has two readings technique that is encryption technique (convert original file into unreadable file) and decryption technique (convert unreadable file into original file). Security applications have passphare / password passphrases that must be remembered and are sensitive, ie capital and small letters are distinguished, so that passphare is difficult to guess by anyone.

REFERENCES

Pahrizal, David Pratama, "Implementation Of RSA Algorithm For Data Security Text", *Jurnal Pseudocode, Vol. 3, No. 1, 2016,* ISSN 2355-5920.

Zaeniah, Bambang Eka Purnama, "An Analysis of Encryption and Decryption Application by using One Time Pad Algorithm", *(IJACSA)* International Journal of Advanced Computer Science and Applications, 6(9), 2015.

K Hashizume et al., "An analysis of security issues for cloud computing", Journal of Internet Services and Applications, a Springer open journal, pp 1-13, 2013.

M. Preetha, M. Nihiya, "A Study And Performance Analysis Of RSA Algoritm, (*IJCSMC*) International Journal Of Computer Science and Mobile Computing, Vol. 2, 2013, ISSN 2320-088X.

William Stallings, "Cryptography and Network Security: Principles & Practices", Fifth edition, Prentice Hall, ISBN-13: 978-0136097044, 2011.

Sundram Prabhadevi, Rahul De, Pratik Shah, "Cost Effective Poly Vernam Cipher With Cache Optimization", Journal of Theoretical and Applied Information Technology, ISSN: 1992-8645, 2013.

Muhammad Arief, Fitriyani, Nurul Ikhsan, "*Kriptografi Rsa Pada Aplikasi File Transfer Client- Server Based",* Jurnal Ilmiah Teknolog informasi Terapan Volume I, No 3, 10 Agustus 2015, ISSN : *2407 – 3911*

S. Kamara, and K. Lauter, —Cryptographic cloud storage‖, Financial Cryptography and Data Security, Springer Berlin Heidelberg, pp. 136-149, 2010.

K., Dr Ch., and S. Yogesh. "Enhanced Security Architecture for Cloud Data Security." International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3.5, pp. 571-575 , 2013.

Ahmad Rosyadi, Electrical engineering major, University Of Diponegoro Semarang, "Implementation of AES Cryptography Algorithm for Email Encryption and Decryption", Transient, vol. 1, no. 3, September 2012, ISSN: 2302- 9927,64

W. , C. , et al. —Privacy-preserving public auditing for data storage security in cloud computing.‖ INFOCOM, 2010 Proceedings IEEE. Ieee, 2010.

D.Welsh, "Codes and Cryptography, Oxfors Science Publication." (1988).

Stallings, W. 2011. *Cryptography and Network Security: Principles and Practice*. 5th ed. Pearson Education Inc. New York.

T. Gunasundari and K. Elangovan, "A ComparativeSurvey on Symmetric Key Encryption Algorithms,"International Journal of Computer Science and Mobile Applications, ISSN, pp. 2321-8363, 2014.

Digital Economy Promotion Agency, under the Administrative Supervision of the Minister of Digital Economy and Society, 2016.

M. Agrawal and P. Mishra, "A comparative survey on symmetric key encryption techniques," International Journal on Computer Science and Engineering (IJCSE), vol. 4, pp. 877-882, 2012.

V. Beal. (2009, Encryption. Available: http://www.webopedia.com/TERM/E/encryption.html