

Penerapan Algoritma Rice Codes dan Algoritma Rivest Shamir Adleman (RSA) Untuk Kompresi dan Pengamanan Teks Pada Aplikasi Chatting

Vify Ernanda, Surya Darma, Fince Tinus Waruwu

Program Studi Teknik Informatika, STMIK Budi Darma, Medan, Indonesia

Email: vifyernanda2525@gmail.com

Abstrak—Dengan berkembangnya informasi di zaman sekarang ini chatting memegang peranan penting terhadap seluruh aspek kehidupan manusia. Dimana chatting sebagai alat komunikasi yang dapat membantu berkomunikasi tanpa ada batasan waktu dan bebas dari hambatan. Tetapi dalam berkomunikasi melalui aplikasi chatting tidak bisa leluasa atau sebebas dalam berkomunikasi pada biasanya. Dimana chatting memiliki jumlah bit yang telah ditetapkan, sehingga dalam pengiriman pesan teks aplikasi chatting tidak bisa sekaligus atau dalam sekali pengiriman melainkan dalam beberapa kali pengiriman. Maka dari itu aplikasi chatting membutuhkan sebuah pengompresian dimana pesan teks yang akan dikirimkan melalui aplikasi chatting dengan tidak menghabiskan waktu yang lama dan tidak dalam beberapa kali pengiriman. Cukup hanya dalam sekali pengiriman pesan teks dapat terkirim kepada mereka yang ditujukan. Tetapi terkadang dalam pengiriman pesan teks tidak hanya bermasalah dalam banyak atau sedikit nya pesan teks yang akan dikirimkan ada pun kendala lain dalam pengiriman pesan teks yang harus diatasi. Pesan teks yang telah dikirim pada mereka yang dituju, terkadang pesan teks tersebut telah berubah tidak pada semestinya atau pun tidak sama seperti apa yang dikirimkan. Maka dari itu aplikasi chatting sangat membutuhkan suatu pengamanan pada aplikasi chatting yang mana dapat mengamankan pesan teks yang akan dikirim kepada mereka yang dituju tanpa berubah sedikit pun. Aplikasi chatting memberikan solusi dalam atas kendala berkomunikasi dikarenakan terhambat oleh jarak dan waktu. Aplikasi chatting memberikan kemudahan dalam berkomunikasi chatting ke beberapa orang yang memiliki jarak yang jauh dengan menerapkan algoritma Rice Codes dan Rivest Shamir Adleman (RSA) pada aplikasi chatting yang dirancang dengan menggunakan menggunakan bahasa pemrograman Microsoft Visual Basic 2008 sebagai sarana pengompresian dan pengamanan dalam pengiriman pesan teks.

Kata Kunci: Penerapan, Kompresi, Kriptografi, Aplikasi Chatting, Rice Codes, Rivest Shamir Adleman (RSA)

Abstract—With the development of information in this day and age chat plays an important role in all aspects of human life. Where chat as a communication tool that can help communicate without any time restrictions and is free from obstacles. But in communicating through chat applications can not be free or as free in communicating as usual. Where chat has a predetermined number of bits, so that in sending text messages the chat application cannot be at once or in one delivery but in multiple transmissions. Therefore the chat application requires a compression where the text messages to be sent through the chat application do not take a long time and do not send several times. It is enough to send only one text message to those addressed. But sometimes text messaging is not only a problem in many or few text messages to be sent there are other obstacles in sending text messages that must be overcome. Text messages that have been sent to those intended, sometimes the text messages have changed not at its disposal or not the same as what was sent. Therefore the chat application is in need of security on the chat application which can secure text messages to be sent to the intended destination without changing one bit. Chat applications provide solutions to communication problems because they are hampered by distance and time. Chat application provides convenience in communicating chat to several people who have great distances by applying the Rice Codes and Rivest Shamir Adleman (RSA) algorithm to chat applications that are designed using Microsoft Visual Basic 2008 programming language as a means of compressing and securing text messages.

Keywords: Application, Compression, Cryptography, Chatting Application, Rice Codes, Rivest Shamir Adleman (RSA)

1. PENDAHULUAN

Aplikasi chatting membutuhkan sebuah pengompresian dimana pesan teks yang akan dikirimkan melalui aplikasi chatting dengan tidak menghabiskan waktu yang lama dan tidak dalam beberapa kali pengiriman. Cukup hanya dalam sekali pengiriman pesan teks dapat terkirim kepada mereka yang ditujukan. Dikarena kan disetiap pesan yang akan disampaikan nanti tidak sepenuhnya atau sekaligus dapat terkirim dikarena kan memiliki batasan setiap karakter pada aplikasi tersendiri batasan tersebut biasanya dibatasi dengan 160 char yang dalam sekali pengiriman pesan teks. Jika lebih dari batas yang telah ditentukan maka pengirim akan membayar lebih dari sekali. Walaupun pada saat ini dapat menulis lebih dari 160 karakter, maka system hanya mampu memmilahnya dalam beberapa pesan. Tetapi terkadang dalam pengiriman pesan teks tidak hanya bermasalah dalam banyak atau sedikit nya pesan teks yang akan dikirimkan ada pun kendala lain dalam pengiriman pesan teks yang harus diatasi. Pesan teks yang telah dikirim pada mereka yang dituju, terkadang pesan teks tersebut telah berubah tidak pada semestinya atau pun tidak sama seperti apa yang dikirimkan. Dan jika pesan teks yang akan dikirimkan kurang aman maka penyerang akan dengan mudah membobol dan menyerang seluruh saluran komunikasi yang terjadi. Dikarena kan pesan teks yang telah dikirim sudah diubah oleh seseorang yang tidak bertanggung jawab. Untuk mencegah hal itu terjadi maka dari itu aplikasi chatting sangat membutuhkan suatu pengamanan pada aplikasi chatting yang mana dapat mengamankan pesan teks yang akan dikirim kepada mereka yang dituju tanpa berubah sedikit pun. Dengan menggunakan pengamanan kriptografi maka penyerang komunikasi tersebut tidak dapat mengetahui isi pesan yang nantinya akan dikirimkan, dikarena kan pesan tersebut teracak. Dan nanti nya penerima, teks yang

telah tersandi tersebut nantinya akan dikembalikan lagi dengan semula dengan menggunakan proses dekripsi. Karena kriptografi disini menggunakan proses enkripsi dan dekripsi.

Adapun kompresi yang merupakan sebuah cara untuk memadatkan data sehingga hanya memerlukan ruangan penyimpanan lebih kecil sehingga efisien dalam menyimpannya atau mempersingkat waktu dalam pertukaran informasi. Karena kompresi bertujuan untuk mengurangi jumlah bit yang digunakan untuk menyimpan atau mengirim informasi. Firdaus Musyafi dan Irwan Afrianto melakukan penelitian aplikasi chatting. Aplikasi chatting memberikan solusi dalam atas kendala berkomunikasi dikarenakan terhambat oleh jarak dan waktu. Aplikasi chatting memberikan kemudahan dalam berkomunikasi chatting ke beberapa orang yang memiliki jarak yang jauh[1]. Muhammad Safri Lubis, Mohammad Andri Budiman dan Karina Lolo Manik melakukan pengujian terhadap Rivest Shamir Adleman perangkat lunak yang dibuat sudah mampu memberikan keamanan pada saat pengiriman pesan teks, kunci privat yang dibangkitkan selalu berubah-ubah nilainya walau terkadang nilai kunci publik yang dihasilkan nilainya sama. Pembangkitan bilangan acak diimplementasikan dalam suatu fungsi `Math.random`. sementara pada proses penentuan bilangan prima digunakan fungsi khusus `Math.sqrt` yang sesuai dengan metode The Sieve of Eratosthenes untuk menentukan nilai akar kuadrat dari suatu bilangan sehingga diharapkan pengecekan bilangan prima bisa dilakukan lebih cepat dan menhemat memori. Pembuatan aplikasi simulasi kriptografi berbasis algoritma RSA ini dapat membuktikan bahwa algoritma kriptografi RSA dapat diimplementasikan dengan menggunakan fungsi-fungsi khusus yang tersedia dalam bahasa pemrograman Visual Basic.Net 2008 walaupun masih bersifat stand alone dan hanya menampilkan proses dari algoritma RSA saja[2].

2. METODOLOGI PENELITIAN

2.1 Rice Codes

Rice Codes adalah salah satu algoritma kompresi yang dapat memperkecil ukuran data yang lebih kecil dari ukuran sebelumnya. Sebelum adanya Rice Code, terdapat algoritma yang disebut sebagai Golomb Codes yang merupakan family dengan Rice Code karena memiliki persamaan yang bergantung pada pemilihan parameter m , dimana m adalah himpunan dari 2^k ($m = 2^k$). Rice Code disebut juga sebagai Golomb-Rice Code, yang diberi nama sesuai dengan penciptanya yaitu Robert F. Rice pada tahun 1979[4]. Rice Code merupakan special case dari Golomb Codes yang mana nilai x dikodekan k pertama digeser kekanan untuk mendapatkan nilai unary coded. Kemudian urutan terendah dari k nilai asli dari x dilanjutkan sebagai k yang bernilai. Rice Code menunjukkan penggunaan sebuah subset dari turunan Golomb Code untuk menghasilkan sebuah kode yang sederhana dan mudah diimplementasikan dalam kasus aritmatika biner secara efisien, dan keduanya digunakan pada beberapa metode untuk kompresi audio lossless. Di dalam algoritma Rice, ada sebuah nilai k yang artinya adalah banyaknya angka 1 pada suffix dari kode terkompresi. Dalam proses encode, dilakukan pemisahan pada prefix dan suffix. Ketika proses decode, decoder membaca sign bit dan lompat ke angka 0 pertama dari sebelah kiri, yang mana akan berlanjut kembali untuk penambahan bit pada k selanjutnya.

2.2 Rivest Shamir Adleman (RSA)

Pada tahun 1977, Rivest, Shamir, dan Adleman merumuskan algoritma praktis yang mengimplementasikan sistem kriptografi kunci publik disebut dengan sistem kriptografi RSA, (Rives et al., 1983). Meskipun pada tahun 1997 badan sandi Inggris mempublikasikan bahwa Clifford Cocks telah merumuskan sistem kriptografi RSA 3 tahun lebih dahulu dari pada Rivest, Shamir dan Adleman. Algoritma kriptografi RSA didesain sesuai fungsinya sehingga kunci yang digunakan untuk dekripsi. Algoritma RSA disebut kunci public karena kunci enkripsi dapat dibuat kunci public yang berarti semua orang mengetahuinya, namun hanya orang tertentu yang dapat melakukan dekripsi terhadap pesan tersebut. Keamanan algoritma RSA didasarkan pada sulitnya memfaktorkan bilangan besar menjadi faktor-faktor primanya.

2.3 Aplikasi Chatting

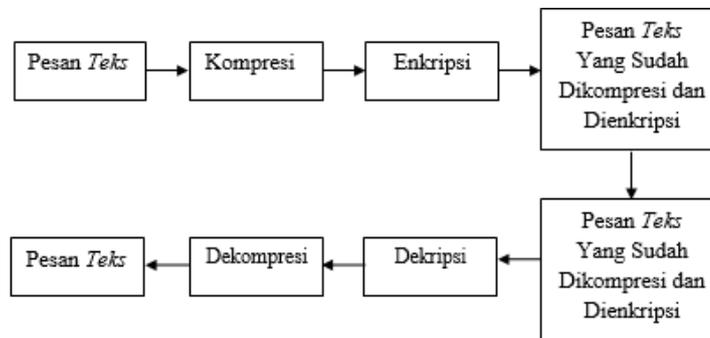
Komunikasi merupakan suatu proses sosial yang sangat penting dalam kehidupan manusia. Saat ini, banyak alat komunikasi yang dapat digunakan untuk berinteraksi dan berkomunikasi dari jarak jauh, dan aplikasi chatting merupakan salah satu aplikasi yang sering digunakan dalam berkomunikasi. Dengan menggunakan aplikasi chatting pengguna dapat berkomunikasi dengan pengguna lain tanpa terhambat jarak dan waktu. Aplikasi chatting adalah media komunikasi yang memungkinkan pengguna dapat mengirim pesan secara realtime ke pengguna lain. Aplikasi chatting juga memberikan kemudahan dalam berkomunikasi chatting ke beberapa orang yang berbeda jarak dan lokasi tempat dimana mereka bertempat tinggal. Karena chatting sudah dilengkapi fitur Group chat. Aplikasi chatting merupakan media komunikasi dimana pengguna nya dapat berkomunikasi dan dengan mudah bertukar pendapat, komentar, bertukar file, dan lain sebagainya[1].

3. HASIL DAN PEMBAHASAN

Komunikasi saat ini adalah sarana penting bagi kehidupan manusia dimana mereka saling bertukar informasi dengan penyampaian pesan antar sesama. Komunikasi yang dibentuk untuk menjalin hubungan dalam jarak jauh

dan dengan mempersingkat waktu dan menghemat biaya. Aplikasi *chatting* salah satu sarana yang dapat digunakan dalam berkomunikasi tanpa mengenal jarak dan waktu. Pengguna tak perlu menghabiskan waktu untuk mengirim informasi dalam beberapa kali pengiriman dan khawatir akan penyadapan pada aplikasi *chatting*. karena aplikasi *chatting* ini sudah menggunakan metode dimana jumlah *bit* yang sudah ditetapkan dapat dikompresi atau telah dipadatkan lagi agar tidak menghabiskan waktu yang lama untuk menyampaikan informasi. Dan informasi yang akan disampaikan tidak akan berubah, karena akan sama persis seperti awal pengiriman informasi pada siapa yang akan ditujukan.

Pengkompresian dan pengamanan *teks* dilakukan dengan menggunakan algoritma *rice codes* dan algoritma *rivest shamir adleman* (RSA). Dan akan dirancang dengan menggunakan bahasa pemrograman *visual basic 2008*.



Gambar 1. Prosedur Rice Codes Dan Rivest Shamir Adleman Pesan Teks

Penerapan aplikasi *chatting* ialah adanya pengulangan atau pengiriman informasi sehingga pengguna harus menghabiskan waktu sedikit lama dan tidak dengan sempurna dalam penyampaian sebuah informasi yang ingin disampaikan. Terkadang pun dalam penyampaian informasi ada nya hambatan dimana informasi yang akan disampaikan tidak seperti informasi awal yang akan disampaikan. Dikarena kan informasi yang telah disampaikan sudah diubah pada pihak yang tidak bertanggung jawab. Banyak nya contoh-contoh kasus yang sudah terjadi, misalnya sebuah perusahaan dimana sang pemilik perusahaan ingin mengetahui apa-apa saja kegiatan mereka dalam berkomunikasi dan apa-apa saja yang ingin dibahas oleh para karyawannya. Maka sang pemilik perusahaan mulai meyadap masing-masing aplikasi *chatting* yang selama ini digunakan oleh para karyawan. Dengan tanpa disadari bahwa aplikasi *chatting* mereka telah disadap oleh atasan mereka sendiri.

Tabel 1. Nilai k Rice Codes

n	k=0	k=1	k=2	k=3	k=4	k=5
0	0	0 0	0 00	0 000	0 0000	0 00000
1	10	0 1	0 01	0 001	0 0001	0 00001
2	110 0	10 0	0 10	0 010	0 0010	0 00010
3	110 1	10 1	0 11	0 011	0 0011	0 00011
4	1110 00	110 00	10 00	0 100	0 0100	0 00011
5	1110 01	110 01	10 01	0 101	0 0101	0 00100
6	1110 10	110 10	10 10	0 110	0 0110	0 00101
7	1110 11	1110 11	10 11	0 111	0 0111	0 00111
8	11110 000	1110 000	10 000	10 000	0 1000	0 01000
9	11110 001	1110 001	110 001	10 001	0 1001	0 01001
10	11110 010	1110 010	110 010	10 010	0 1010	0 01010
11	11110 011	1110 011	110 011	10 011	0 1011	0 01011
12	11110 100	1110 100	110 100	10 100	0 1100	0 01100
13	11110 101	1110 101	110 101	10 101	0 1101	0 01101
14	11110 110	1110 110	110 110	10 110	0 1110	0 01110
15	11110 111	1110 111	110 111	10 111	0 1111	0 01111
16	111110 0000	11110 0000	1110 0000	110 0000	10 0000	0 10000

Misalkan, terdapat string “VIFY AKAN MENEMUI IBRA DIRUMAH UWEK”, dimana :

|String| = 30

$\Sigma = \{Sp, I, A, M, E, U, K, R, V, F, Y, N, B, D, H, W\}|\Sigma| = 16$

Tabel 2. Sebelum Di Kompresi

Σ	ASCII Code	ASCII (Binary)	Bit (ASCII)	Frekuensi	Frek x Bit
Sp	32	00100000	8 bit	5	40
I	73	01001001	8 bit	4	32

Σ	ASCII Code	ASCII (Binary)	Bit (ASCII)	Frekuensi	Frek x Bit
A	65	01000001	8 bit	4	32
M	77	01001101	8 bit	3	24
E	69	01000101	8 bit	3	24
U	85	01010101	8 bit	3	24
K	75	01001011	8 bit	2	16
R	82	01010010	8 bit	2	16
V	86	01010110	8 bit	1	8
F	70	01000110	8 bit	1	8
Y	89	01011001	8 bit	1	8
N	78	01001110	8 bit	1	8
B	66	01000010	8 bit	1	8
D	68	01000100	8 bit	1	8
H	72	01001000	8 bit	1	8
W	87	01010111	8 bit	1	8
Jumlah					264

Setelah dibuat seperti pada tabel 3.2, kemudian terlebih dahulu diurutkan berdasarkan jumlah frekuensi terbanyak (*descending order*), maka urutannya dimulai dari Sp, I, A, M, E, U, K, R, V, F, Y, N, B, D, H, W. Dengan menggunakan *Rice Code* dengan nilai $k=2$, maka hasilnya seperti pada tabel 3.3:

Tabel 3. Kompresi

Σ	Rice Code	Bit	Frekuensi	Frek x Bit
Sp	000	3	5	15
I	001	3	4	12
A	010	3	4	12
M	011	3	3	9
E	1000	4	3	12
U	1001	4	3	12
K	1010	4	2	8
R	1011	4	2	8
V	10000	5	1	5
F	110001	5	1	5
Y	110010	6	1	6
N	110011	6	1	6
B	110100	6	1	6
D	110101	6	1	6
H	110110	6	1	6
W	110111	6	1	6
Jumlah				134

Hasil dari kalimat “VIFY AKAN MENEMUI IBRA DIRUMAH UWEK” yaitu:

10000001 11000111 00100000 10101001 01100110 00011100 01100111 00001110 01001000 00111010
01011010 00011010 10011011 10010110 10110110 00010011 10111100 00001010

Dari hasil kompresi maka akan diubah menjadi sebuah karakter:

Tabel 3. Hasil Kompresi

Bin	ASCII	Karakter
10000001	129	•
11000111	199	Ç
00100000	32	
10101001	169	©
01100110	102	f
00011100	28	
01100111	103	g
00001110	14	
01001000	72	H
00111010	58	:
01011010	90	Z
00011010	26	
10011011	155	>
10010110	150	–

Bin	ASCII	Karakter
10110110	182	¶
00010011	19	
10111100	188	¼
00001010	10	

Algoritma RSA memiliki besaran-besaran sebagai berikut:

- p dan q bilangan prima (rahasia)
- $n = p.q$ (tidak rahasia)
- $(n) = (p-1)(q-1)$ (rahasia)
- e (kunci enkripsi) (tidak rahasia)
- d (kunci dekripsi) (rahasia)
- m (*plaintext*) (rahasia)
- c (*chipertext*) (tidak rahasia)

Pembangkitan Kunci yaitu dalam membuat suatu sandi, RSA mempunyai cara kerja dalam membuat kunci public dan kunci privat adalah sebagai berikut:

- pilih dua bilangan prima sembarangan, p dan q .
- Hitung $n = p^2$ sehingga q dapat diperoleh dengan menarik akar pangkat dua dari n
- Hitung $(n) = (p-1)(q-1)$
- Dipilih kunci public e , yang relative prima terhadap (n) yaitu $1 < e < (n) = 1$
- Bangkitkan kunci privat dengan menggunakan persamaan

$$d = 1 \pmod{(n)}$$

$$(0 \leq d \leq n)$$

Sehingga hasil dari algoritma di atas adalah:

- Kunci public adalah pasangan (e, n)
- Kunci privat adalah pasangan (d, n)

Misalkan A akan membangkitkan kunci public dan kunci privat miliknya. A memilih $p = 13$ dan $q = 31$ (keduanya prima). Selanjutnya A menghitung $n = p.q=403$ dan $(n) = (p-1)(q-1) = 360$

A memilih kunci public $e = 7$ karena relative prima dengan 360. A menggunakan nilai e dan n . selanjutnya A menghitung nilai dengan dekripsi d , sehingga dituliskan berdasarkan persamaan:

$$7.d = 1 \pmod{360}$$

Kunci privat digunakan untuk mendekripsi pesan dan harus dirahasiakan A. jadi, perhitungan kunci ini menghasilkan pasangan kunci.

- Kunci public ($e = 7, n=403$)
- Kunci privat ($d = 130, n = 403$)

Pada RSA hanya diberikan kunci public, yaitu modulus n dan e . sedangkan kunci privat d dirahasiakan. Oleh karna itu, keamanan algoritma RSA terletak pada tingkat kesulitan dalam memfaktorkan bilangan non prima n menjadi factor primanya, dalam hal ini $n = p.q$. Sekali n berhasil difaktorkan menjadi menjadi p dan q , maka $(n) = (p-1)(q-1)$ dapat dihitung. Selanjutnya, karena kunci enkripsi e diumumkan (tidak rahasia), maka kunci dekripsi d dapat dihitung dari persamaan pertama dan melakukan dekripsi *chipertext* c menjadi *plaintext* m menggunakan persamaan kedua. Untuk menjaga keamanan tersebut, ada beberapa hal yang perlu diperhatikan dalam memilih p dan q .

- Nilai p harus cukup jauh dari nilai q . sebaiknya panjang dari p harus berbeda beberapa digit dari q .
- Sebaiknya $gcd(p-1, q-1)$ tidak terlalu besar.
- Sebaiknya $(p-1)$ dan $(q-1)$ mempunyai factor prima yang besar.

Proses Enkripsi

$$C = M^e \pmod{n}$$

$$n = 360$$

$$e = 7$$

Tabel 4. Merubah Kenilai ASCII

C	m	ASCII	C	m	ASCII
1	•	129	10	:	58
2	Ç	199	11	Z	90
3		32	12		26
4	©	169	13	>	155
5	f	102	14	-	150
6		28	15	¶	182
7	g	103	16		19
8		14	17	¼	188
9	H	72	18		10

Blok-blok plainteks yang telah dienkripsi sebagai berikut:

$$C_1 = 129^7 \text{ mod } 403 = 8385$$

$$C_2 = 199^7 \text{ mod } 403 = 8717$$

$$C_3 = 32^7 \text{ mod } 403 = 6456$$

Jadi, chiperteks yang dihasilkan adalah:

$$c = 8385\ 8717\ 6456\ 42097\ 19555\ 264\ 7868\ 891\ 37734\ 5158\ 3492\ 66400\ 23655\ 23815\ 1373\ 23164\ 38945\ 328000$$

Proses Dekripsi

Proses dekripsi pesan dari dekompresi sebagai berikut:

$C^d \text{ mod } n$

$$M_1 = 8385^{103} \text{ mod } 403 = 129$$

$$M_2 = 8717^{103} \text{ mod } 403 = 199$$

$$M_3 = 6466^{103} \text{ mod } 403 = 32$$

$$M_4 = 42097^{103} \text{ mod } 403 = 169$$

$$M_5 = 19555^{103} \text{ mod } 403 = 102$$

$$M_6 = 264^{103} \text{ mod } 403 = 28$$

$$M_7 = 7868^{103} \text{ mod } 403 = 103$$

$$M_8 = 891^{103} \text{ mod } 403 = 14$$

$$M_9 = 37734^{103} \text{ mod } 403 = 72$$

$$M_{10} = 5158^{103} \text{ mod } 403 = 58$$

$$M_{11} = 3492^{103} \text{ mod } 403 = 90$$

$$M_{12} = 66400^{103} \text{ mod } 403 = 26$$

$$M_{13} = 23655^{103} \text{ mod } 403 = 155$$

$$M_{14} = 23815^{103} \text{ mod } 403 = 150$$

$$M_{15} = 1373^{103} \text{ mod } 403 = 182$$

$$M_{16} = 23164^{103} \text{ mod } 403 = 19$$

$$M_{17} = 38945^{103} \text{ mod } 403 = 188$$

$$M_{18} = 328000^{103} \text{ mod } 403 = 10$$

Maka plainteks yang akan dihasilkan adalah m :

	Ç		©	f	g	H	:	Z	>	-	¶		¼	
--	---	--	---	---	---	---	---	---	---	---	---	--	---	--

4. KESIMPULAN

Adapun kesimpulan dari penelitian ini adalah:

- a. Pada pengkompresian pesan teks yang diterapkan pada aplikasi chatting maka aplikasi chatting akan menerapkan algoritma rice codes.
- b. Adanya pengamanan pesan teks yang sudah terkompresi pada aplikasi chatting dengan menerapkan algoritma rice codes yang nantinya pesan yang telah terkompresi akan di aman kan dengan algoritma rivest shamir adleman
- c. Dalam perancangan aplikasi chatting yang sudah diterapkan menggunakan algoritma rice codes dan algoritma rivest shamir adleman ialah dengan menggunakan Bahasa pemograman Miscrosoft Visual Basic 2008.

REFERENCES

- [1] J. Ilmiah, I. Komputa, J. Dipati, and U. No, "Membangun Aplikasi Chatting Dengan Penerjemah Otomatis Berbasis Mobile," vol. 4, no. 2, 2015.
- [2] M. S. Lubis, M. A. Budiman, and K. L. Manik, "Penggunaan Algoritma RSA dengan Metode The Sieve of Eratosthenes dalam Enkripsi dan Deskripsi Pengiriman Email," Semin. Nas. Apl. Teknol. Inf., no. 15 Juni 2013, pp. 28–33, NaN-5022, 2013.
- [3] N. P. Ayu and N. Fani, "Analisis Algoritma Huffinan Statis Dalam Kompresi Teks Pada Short Message Service (SMS)," Stud. Inform. J. Sist. Inf., vol. 3, pp. 69–76, 2016.
- [4] D. Salomon, HandBook of data compression. London: Springer, 2010.
- [5] B. Schneier, Applied Cryptography: Protocol, Algorithms, And Source Code, 2nd ed. New York: John wily & Sons, inc, 1996.
- [6] M. kom. Emy Setyaningsih, S.si., Kriptografi Dan Implementasi Menggunakan Matlab. yogyakarta: Andi Yogyakarta, 2015.
- [7] R. Sadikin, kriptografi untuk keamanan jaringan dan implementasi dalam bahasa java. yogyakarta: Andi Yogyakarta, 2012.
- [8] Y. Sugiarti, Analisi dan Perancangan UML Generated vb.6, 1st ed. yogyakarta: Graha Ilmu, 2013.

- [9] A. Nugroho, *Rekayasa Perangkat Lunak Berorientasi Objek Dengan Metode USDP*. Yogyakarta: CV.ANDI OFFSET(Penerbit ANDI), 2010.
- [10] M. . Primananda Arif Aditya, S.Si, *Dasar-Dasar Pemograman Database Desktop dengan Visual Basic.Net 2008*. Jakarta: PT.ELEX MEDIA KOMPUTINDO KOMPAS GRAMEDIA, 2013.