IMPLEMENTASI ALGORITMA KRIPTOGRAFI CAESAR CIPHER DAN ALGORITMA KOMPRESI HUFFMAN UNTUK MENGAMANKAN PESAN CHATTING PADA APLIKASI BERBASIS WEB DI PT. TASINDO MANDIRI INDONESIA

Soni[1)],Windarto[2)]
Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : sony17061990@gmail.com[1)] , windarto@budiluhur.ac.id[2)]

ABSTRAK

Perkembangan teknologi informasi pada zaman ini telah mengalami kemajuan yang sangat pesat dalam berkomunikasi melalui bermacam-macam media tanpa memperhitungkan jarak dan waktu. Penggunaan interkonektivitas sudah menjadi kebutuhan sekunder yang sangat mendasar,karena hampir semua media yang digunakan untuk bertukar informasi sudah menggunakan interkonektivitas jaringan internet. Namun kemudahan dalam menggunakan media komunikasi membawa dampak bagi keamananan informasi dalam menggunakan media tersebut. Informasi menjadi sangat rentan untuk diketahui oleh pihak-pihak yang tidak berkepentingan. Pada PT. Tasindo Mandiri Indonesia ini perusahaan yang bergerak di bidang Manufactures of Soft Bags, chatting merupakan salah satu media informasi yang sering digunakan untuk mengirim pesan di setiap departemen. Setiap informasi tidak boleh dipublikasikan ke sembarang departemen yang lain, karena dikhawatirkan terjadi pencurian informasi terutama jika ternyata informasi yang dicuri akan digunakan untuk hal-hal yang merugikan PT. Tasindo Mandiri Indonesia. Dari fenomena tersebut maka dibutuhkan sebuah metode untuk menjaga sebuah kerahasiaan pesan yang dikirim dan tersimpan ke dalam database melalui aplikasi chatting. Metode yang dimaksud adalah dengan cara proses enkripsi. Dengan aplikasi kriptografi yang menerapkan algoritma Caesar Cipher dan kompresi Huffman, diharapkan pesan atau informasi yang dikirim atau diterima melalui chatting akan aman dan tidak disalahgunakan oleh pihak yang tidak bertanggung jawab. Pada Penelitian ini dirancanglah sebuah sistem aplikasi berbasis web berupa aplikasi chatting yang menggunakan algoritma kriptografi Caesar Cipher untuk enkripsi isi pesan yang tersimpan di dalam database dan algoritma kompresi Huffman untuk kompresi pesan tersebut. Dengan metode enkripsi Caesar Cipher setiap pesan yang tersimpan ke dalam database akan diubah isi dari teks asli menjadi teks yang tidak bisa dibaca, sehingga kerahasiaan data dan informasi tetap terjaga. Kemudian untuk mengefisienkan ruang penyimpanan, pesan tersebut dikompresi dengan menggunakan algoritma kompresi Huffman. Penulis mengambil kesimpulan dengan adanya aplikasi kriptografi Pada PT. Tasindo Mandiri Indonesia ini mampu menjaga dan melindungi kerahasiaan setiap data dan informasi yang tersimpan dan diharapkan dapat memberikan manfaat bagi PT. Tasindo Mandiri Indonesia dalam menjalankan usahanya.

Kata Kunci : Caesar Cipher, Huffman, Chatting.

1. PENDAHULUAN

1.1. Latar Belakang

Pada zaman ini perkembangan informasi telah mengalami kemajuan yang sangat pesat dalam berkomunikasi melalui bermacam-macam media tanpa memperhitungkan jarak dan waktu. Penggunaan interkonektivitas sudah menjadi kebutuhan sekunder yang sangat mendasar,karena hampir semua media yang digunakan untuk bertukar informasi sudah menggunakan interkonektivitas jaringan internet.

Pada PT. Tasindo Mandiri Indonesia, chatting adalah salah satu media informasi yang sering digunakan untuk mengirim pesan di setiap departemen seperti laporan invoice, penerimaan barang masuk, surat jalan dan material bahan pembuatan tas. Setiap informasi tidak boleh dipublikasikan ke sembarang departemen yang lain, karena dikhawatirkan terjadi pencurian informasi terutama jika ternyata informasi yang dicuri akan digunakan untuk hal-hal yang merugikan PT. Tasindo Mandiri Indonesia. Untuk mengatasi masalah tersebut maka dirancang sebuah sistem aplikasi berbasis web berupa aplikasi chatting yang menggunakan algoritma kriptografi Caesar Cipher untuk enkripsi isi pesan yang tersimpan di dalam database dan algoritma kompresi Huffman untuk kompresi pesan tersebut.

1.2. Permasalahan

Berdasarkan latar belakang yang telah disampaikan diatas, rumusan masalah yang dihadapi dalam perancangan sistem yaitu:

a. PT. Tasindo Mandiri Indonesia belum memiliki sistem keamanan data yang tersimpan di dalam *database* untuk

mengamankan pesan teks yang dikirim melalui aplikasi *chatting.*

b. Dengan aplikasi yang sudah ada, pesan yang dikirim melalui aplikasi *chatting* masih mudah untuk disadap oleh pihak-pihak yang tidak bertanggung jawab, sehingga sangat rentan data dicuri yang dapat merugikan PT. Tasindo Mandiri Indonesia.

1.3. Batasan Masalah

Adapun batasan masalah yang ditemukan pada penelitian ini adalah sebagai berikut:

a. Algoritma kriptografi yang digunakan adalah algoritma kriptografi *Caesar Cipher* dan algoritma kompresi *Huffman.*
b. Isi percakapan yang akan dienkripsi dan didekripsi berupa teks.
c. Hanya dapat mengirim ke satu *user* saja.
d. Kunci yang digunakan untuk enkripsi dan dekripsi adalah kunci simetris.

2. LANDASAN TEORI

2.1. Definisi Chatting

Chatting adalah salah satu fasilitas untuk berkomunikasi antar sesama pemakai jaringan internet dengan menggunakan media tulis online secara real-time. Komunikasi dilakukan oleh pengguna komputer yang terhubung ke dalam internet secara online yang umumnya berupa teks. Dengan aplikasi chatting pengguna dapat melakukan komunikasi tanpa terkendala jarak yang jauh. Pengembangan dan pengguna yang ingin melakukan aktivitas chatting harus menghubungkan diri pada sebuah komputer di internet yang berperan sebagai pusat koneksi yang disebut IRC (Internet Relay Chat).

2.2. Pengertian Kriptografi

Secara umum, kriptografi adalah suatu teknik dalam mengamankan informasi dimana text asli atau plaintext dengan menggunakan suatu kunci pada suatu metode enkripsi tertentu akan menghasilkan suatu informasi baru yang unik berupa ciphertext. Ciphertext tidak dapat dibaca secara biasa karena tulisan yang dihasilkan merupakan suatu informasi acak. Ciphertext dapat dikembalikan menjadi text asli dengan melalui proses dekripsi. Secara Umum gambaran proses kriptografi dapat dilihat pada gambar 1.

Gambar 1 Proses Kriptografi Secara Umum

2.3. Algoritma Kriptografi Caesar Cipher

Sebelum ada komputer, kriptografi dilakukan menggunakan pensil dan kertas. Algoritma kriptografi (cipher) yang digunakan dinamakan sandi klasik. Algoritma klasik adalah algoritma berbasis karakter. Di mana enkripsi dan dekripsi dilakukan pada setiap karakter pesan.

Contoh Proses enkripsi penggunaan algoritma Caesar Cipher sebagai berikut:

C = (P + K) mod (26) -> untuk huruf alphabet
C = (P + K) mod (26) -> untuk simbol
C = (P + K) mod (10) -> untuk angka
C = ?
P = skripsi ke-1 saya**.**
K = 4

a. Langkah pertama
P (plaintext) didefinisikan sebagai angka yang terdaftar dalam daftar urutan huruf alphabet atau simbol atau angka:

Tabel 1: Urutan alphabet, simbol dan angka pada plaintext yang diubah menjadi angka

P	s	k	r	i	p	s	i	k	e	-	1	s	a	y	a	.
Definisi angka	18	10	17	8	15	18	8	10	4	6	1	18	0	24	0	0

b. Langkah kedua
Pemberian Kunci (K) = 4, maka angka dari plaintext akan ditambah dengan 4. Apabila hasil melebihi atau di bawah dari mod yang telah ditentukan maka untuk huruf (hasil di bawah mod + 26) dan (hasil diatas atau sama dengan mod-26), untuk simbol (hasil di bawah mod + 25) dan (hasil diatas atau sama dengan mod-25), untuk angka (hasil di bawah mod + 10) dan (hasil diatas atau sama dengan mod-10). Untuk spasi penulis tidak melakukan proses enkripsi maupun dekripsi. Penggunaan huruf besar dan huruf kecil tidak mempengaruhi pendefinisian angka maupun proses enkripsi-dekripsi yaitu huruf besar tetap menjadi huruf besar dan huruf kecil tetap menjadi huruf kecil.

Tabel 2:Pemberian kunci pada plaintext

P	s	k	r	i	p	s	i	k	e	-	1	s	a	y	a	.
Definisi angka	18	10	17	8	15	18	8	10	4	6	1	18	0	24	0	0
Angka dengan kunci	22	14	21	12	19	22	12	14	8	10	5	22	4	2	4	4

c. Langkah ketiga
Angka dengan kunci (K) = 4 didefinisikan sebagai huruf alphabet atau simbol atau angka yang akan menjadi ciphertext.

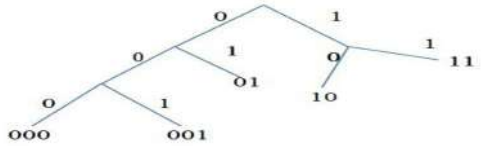
Tabel 3:Hasil perubahan plaintext ke ciphertext

P	s	k	r	i	p	s	i	k	e	-	1	s	a	y	a	.
Definisi angka	18	10	17	8	15	18	8	10	4	6	1	18	0	24	0	0
Angka dengan kunci	22	14	21	12	19	22	12	14	8	10	5	22	4	2	4	4
Cipher Text (C)	w	o	v	m	t	w	m	o	i	*	5	w	e	c	e	:

2.4. Algoritma Kompresi Huffman

Kompresi data merupakan proses mereduksi ukuran suatu data ataupun informasi dengan mengubah sekumpulan data tersebut menjadi sekumpulan kode yang dapat menghemat tempat penyimpanan dan waktu untuk transmisi data.

Proses yang terjadi dalam menggunakan algoritma huffman adalah dengan menggunakan pohon biner yang memiliki kode yang bersesuaian setiap sistemnya diberikan label 1 atau 0. Pemberian label tiap sisi haruslah sesuai dengan aturannya, yaitu setiap sisi harus memiliki nilai yang sama.

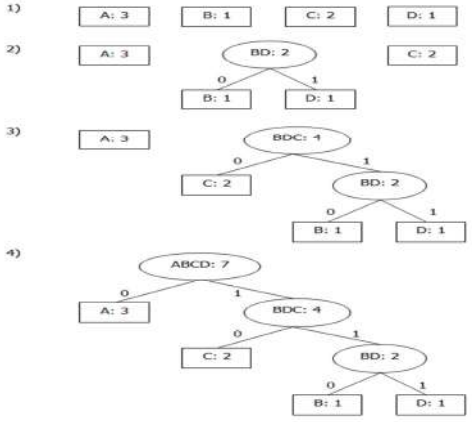


Gambar 2: Pohon Biner Kode Awalan

Contoh, dalam code ASCII string 7 huruf "ABACCDA" memiliki representasi 7 × 8 bit = 56 bit (7 byte), sebagai berikut:

A = 01000001
B = 01000010
A = 01000001
C = 01000011
D = 01000100
A = 01000001

Frekuensi kemunculan A = 3, B = 1, C = 2, dan D = 1.



Gambar 3: Pohon Huffman untuk karakter "ABACCDA"

a. Proses Encoding

Langkah-langkah untuk melakukan encoding pada suatu string biner, sebagai berikut:

1. Menentukan karakter yang akan diencoding.
2. Kemudian dari akar, baca setiap bit yang terdapat pada cabang yang bersesuaian sampai ketemu daun di mana karakter itu berada.
3. Langkah terakhir dengan melakukan pengulangan langkah 2 sampai seluruh karakter selesai diencoding.

Pada tabel di bawah ini, yang merupakan hasil encoding untuk pohon Huffman pada gambar tadi.

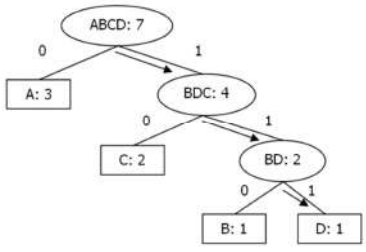
Tabel 4:Kode Huffman untuk karakter "ABCD"

Karakter *String*	Biner *Huffman*
A	0
B	110
C	10
D	111

b. Proses Decoding

Langkah-langkah dalam melakukan decoding suatu string biner pada contoh sebelumnya, sebagai berikut:

1. Langkah pertama adalah baca sebuah bit dari string biner
2. Dimulai dari akar pohon biner.
3. Pada setiap bit yang dilakukan pada langkah pertama, lakukan traversal pada cabang yang bersesuaian.
4. Kemudian Ulangi langkah 1, 2 dan 3 sampai bertemu daun pada pohon tersebut. Kodekan rangkaian bit yang telah dibaca dengan karakter di daun.
5. Proses terakhir hanya melakukan langkah pertama sampai semua bit di dalam string habis.



Gambar 4: Proses Decoding dengan Menggunakan Pohon Huffman

3. ANALISA MASALAH DAN PERANCANGAN PROGRAM

3.1. Analisa Permasalahan

pada PT. Tasindo Mandiri Indonesia, yang memiliki masalah pada saat pengiriman data-data penting melalui pesan chatting. Pesan yang terkirim dan tersimpan di database saat ini masih belum

memiliki keamanan, sehingga siapapun yang dapat mengakses database dapat melihat seluruh informasi yang ada. Hal tersebut terjadi karena proses pengiriman pesan dilakukan melalui jaringan internet di mana pesan yang dikirim tidak dilengkapi dengan pengamanan. Dengan adanya situasi tersebut, maka pengguna khawatir akan pesan yang dikirim dapat dicuri, disadap, dan diketahui oleh pihak yang tidak berkepentingan. Hal tersebut dapat berdampak pada kerugian perusahaan bila pesan yang dikirim berisi laporan-laporan penting yang seharusnya hanya bisa diketahui oleh pihak-pihak tertentu saja dicuri dan disalahgunakan oleh pihak yang tidak bertanggung jawab.

3.2. Rancangan Basis Data

Berikut adalah struktur-struktur tabel yang digunakan dalam pembuatan aplikasi ini.

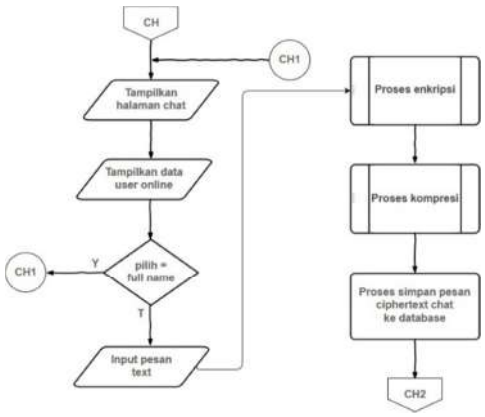
Tabel 5: Tabel users

No	Nama Field	Type	Panjang	Keterangan
1.	Users_id	Integer	5	Id Pengguna
2.	Users_nama	Varchar	100	Nama Pengguna
3.	Users_password	Varchar	100	Password Pengguna
4.	Users_confirm	Varchar	100	Konfirmasi Password
5.	Users_authorized	Enum		Admin atau User
6.	Users_flag	Tiny Int	1	Flag User Yang Online

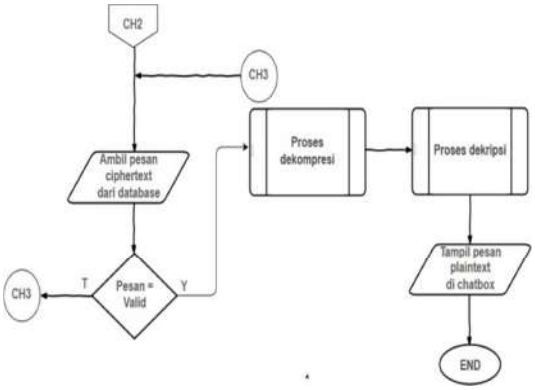
Tabel 6: Tabel Chat

No	Nama Field	Type	Panjang	Keterangan
1.	chat_id	Integer	5	Id Chat
2.	Users_from	Integer	5	Id Pengirim
3.	Chat_text	Text	255	Chat Pengguna
3.	Chat_tanggal	Timestamp		Chat Pengguna
4.	Users_to	Integer	5	Id Penerima
5.	Chat_flag	Tiny Int	1	Flag Chat yang Belum Terbaca

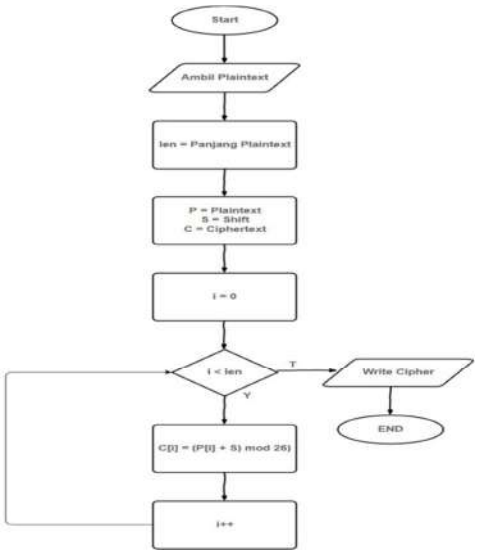
3.3. Flowchart Halaman Chat Pengirim Pesan



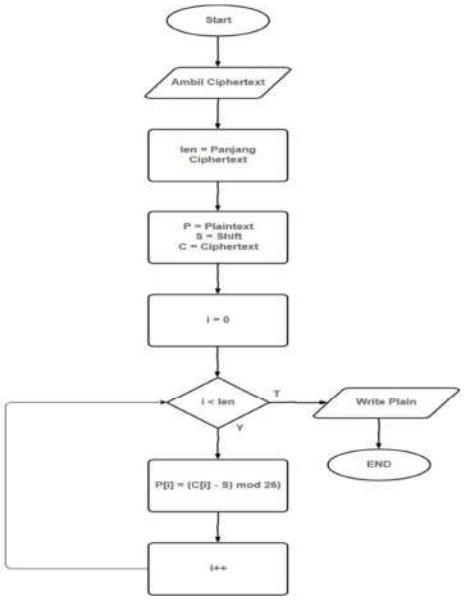
Gambar 5: Flowchart Halaman Chat Penerima Pesan



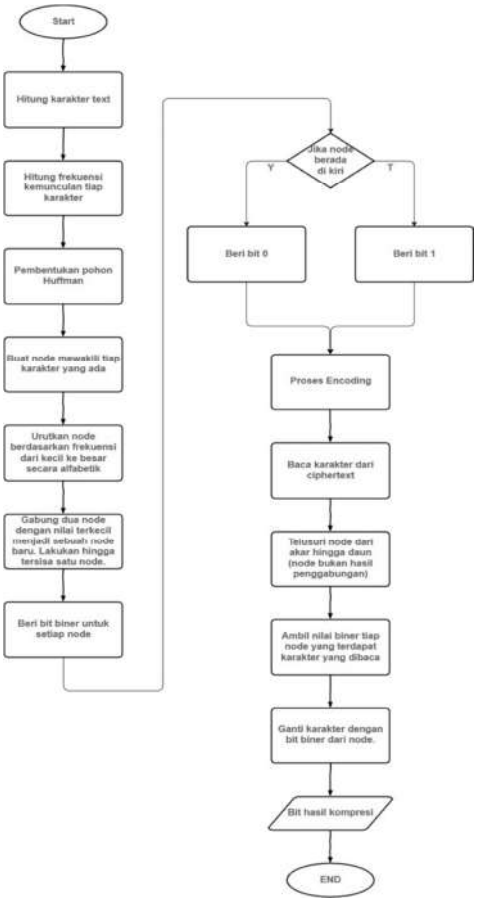
Gambar 6: Flowchart Halaman Chat Penerima Pesan



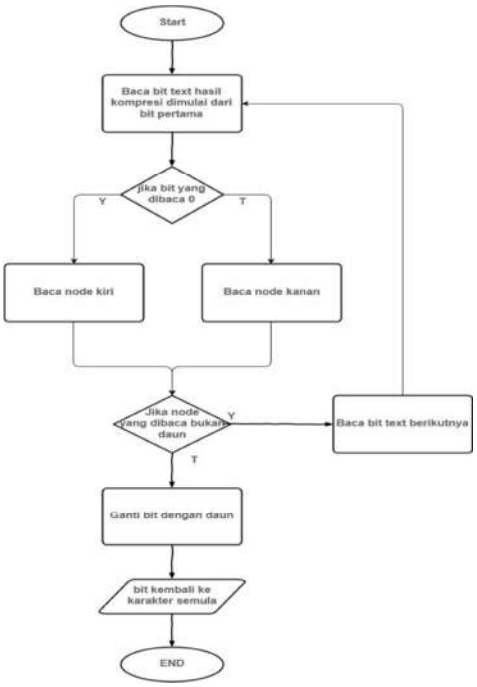
Gambar 7: Flowchart Enkripsi Caesar Cipher



Gambar 8: Flowchart Dekripsi Caesar Cipher



Gambar 9: Flowchart Kompresi Huffman

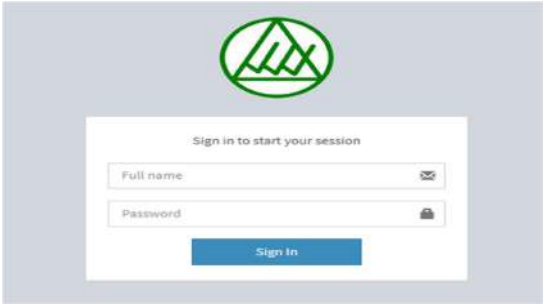


Gambar 10: Flowchart Dekompresi Huffman

4. HASIL DAN PEMBAHASAN

4.1. Tampilan Layar

a. Tampilan Halaman *Sign in*



Gambar 11: Halaman Sign In

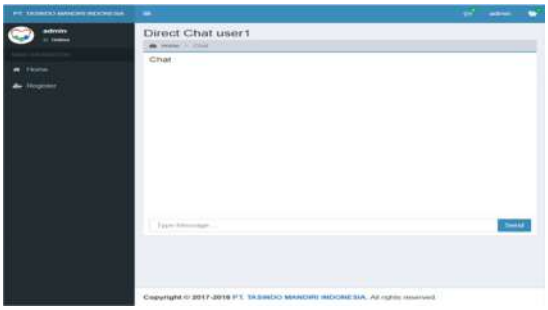
b. Tampilan Halaman *Home Level* Admin

Gambar 12: Halaman Layar Home Level Admin

c. Tampilan Halaman Home Level User

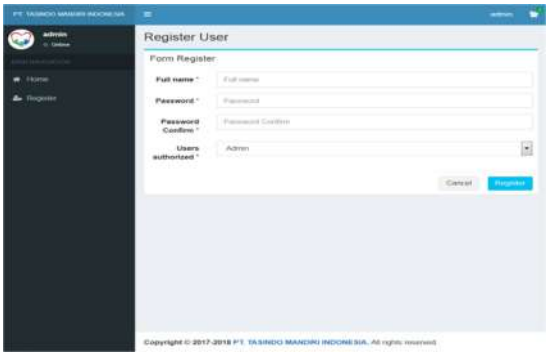
Gambar 13: Halaman Layar Home Level User

d. Tampilan Halaman Chatting



Gambar 14: Halaman Layar Chat

e. Tampilan Halaman *Register*



Gambar 15: Halaman Layar Register

4.2. Hasil Pengujian

Berikut adalah hasil dari pengujian aplikasi enkripsi *chatting*. *Text* yang terkirim dalam bentuk *plaintext* pada menu *chatbox* tersimpan dalam bentuk *ciphertext* di dalam *database*.

Tabel 7: Hasil Enkripsi

No	Pengirim	*Plaintext*	*Size*	*Ciphertext*	*Size*
1.	Admin	Uji coba chat pertama	21 B	û@ø„ª@ñ 8v¢,[˜ð	16 B
2.	Admin	Ini adalah aplikasi kriptografi	31 B	ĪPøf":C• ┼u'=◖Ù>",-³)šÅæ	24 B
3.	User1	Besok akan diadakan meeting.	28 B	è-•Q^:#©┼£Ç(tGR"e-Ñê÷F	22 B
4.	User2	Halo salam kenal	16 B	ĩ %b2:C§◖IÕ (	13 B
5.	User3	Halo, apa kabar?	16 B	ĩ %gÃ aã"9└±Š	13 B

4.3. Evaluasi Sistem

Setelah dilakukan analisa dari hasil pengujian aplikasi ini, dapat ditemukan beberapa kelebihan dan kekurangan pada aplikasi chatting ini, yaitu sebagai berikut:

a. Kelebihan Aplikasi

1) Dapat dioperasikan di semua komputer yang terhubung dengan *server* di mana aplikasi ini berada, sehingga program dapat berjalan lebih fleksibel pada segala jenis *operating sistem*.
2) Aplikasi *chatting* ini dapat melakukan pengiriman pesan secara *real time*.
3) Pada sisi klien, klien hanya membutuhkan *browser* untuk menjalankan aplikasi ini.
4) Aplikasi ini memiliki *user interface* yang sederhana sehingga mudah dimengerti oleh para pengguna.

b. Kekurangan Aplikasi

1) Aplikasi *chatting* ini hanya dapat mengirimkan pesan dalam bentuk *text*.
2) Aplikasi ini tidak menampilkan informasi pengguna seperti foto, alamat, dan nomor telepon.
3) Aplikasi ini tidak memiliki fasilitas untuk edit *fullname* dan *password*.
4) Pesan tidak dapat dikirim ke dalam bentuk *group chatting*.
5) *History* pesan di dalam *chatbox* tidak dapat dihapus.

5. KESIMPULAN DAN SARAN

5.1. Kesimpulan

a. Dengan adanya aplikasi *chatting* ini diharapkan dapat membantu PT. Tasindo Mandiri Indonesia dalam pengamanan pesan *chatting* antar divisi perusahaan sehingga pesan *chatting* akan tetap terjaga dari pihak ketiga yang tidak berhak mengakses.
b. Dengan adanya kompresi pada pesan *chatting* ini ruang penyimpanan pesan di dalam *database* menjadi lebih efisien.
c. Hasil enkripsi pesan yang dikirim oleh *user* pengirim akan selalu sama dan tidak mengalami perubahan ketika pesan didekripsi dan ditampilkan kepada *user* penerima.

5.2. Saran

a. Adanya penambahan fitur-fitur untuk melengkapi aplikasi *chatting* ini, misalnya pesan *file*, foto, dan audio.
b. Aplikasi ini dapat menampilkan informasi pengguna seperti foto, alamat, dan nomor telepon.
c. Adanya penambahan fungsi agar dapat mengedit *fullname* dan *password*.
d. Adanya pengembangan fungsi pengiriman pesan kedalam bentuk *groupchatting*.
e. Adanya penambahan fungsi untuk menghapus *history* pesan pada *chatbox*.

DAFTAR PUSTAKA

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

[2] Basri. 2016. *Kriptografi Simetris dan Asimetris Dalam Perspektif Keamanan Data dan Kompleksitas Komputasi*, Jurnal Ilmiah Ilmu Komputer, Vol. 2, No. 2.

[3] Munir, Rinaldi. 2013, *Pengantar Kriptografi*, Departemen Teknik Informatika, Institut Teknologi Bandung, Diktat Teknik Informatika Mata Kuliah IF 3058.

[4] Pradipta, Anjar. 2016. *Implementasi Metode Caesar Cipher Alphabet Majemuk Dalam Kriptografi Untuk Pengamanan Informasi*, Journal on Networking and Security, Vol. 5, No.3.

[5] Puspita, Novalinda., Nurfarahin,F. 2016. *Analisis Algoritma Huffman Statis Dalam Kompresi Teks Pada Short Message Service (SMS)*, Seminar Nasional Matematika dan Pendidikan Matematika UNY 2016.

[6] Rahayu, Tri Puji., Yakub, Irwan, L. 2012. *Aplikasi Enkripsi pesan Text (SMS) Pada Perangkat Handphone Dengan Algoritma Caesar Cipher*,

Seminar Nasional Teknologi Informasi dan Komunikasi 2012 (Sentika 2012).

[7] Rajagukguk, D. M. 2014, Analisis Perbandingan Algoritma *Huffman* Dengan Algoritma (Lempel-ZIP-Welch) pada Kompresi Gambar Menggunakan Metode Exponensial, Jurnal Teknik Informatika, Vol. VI, No. 3.

[8] Rio, Rita. 2014. *Perancangan Aplikasi Pengamanan Pesan Dengan Algoritma Caesar Cipher*, Jurnal Teknik Informatika, Vol. VI, No. 3.

[9] Sadikin, Rifki. 2012, *Kriptografi Untuk Keamanan Jaringan,* Yogyakarta, Penebit Andi.

[10] Vintana, Gratia. 2012. *Security Chatting Berbasis Dekstop dengan Enkripsi Caesar Cipher Key Random*, Jurnal TICOM, Vol. 5, No.1.

[11] Wibowo, Ari. 2012. *Kompresi Data Menggunakan Metode Huffman*, Seminar Nasional Informasi & Komunikasi Terapan 2012 (Semantik 2012).