SISTEM KEAMANAN CHAT BERBASIS WEB MENGGUNAKAN ALGORITMA ZIG ZAG STUDI KASUS : NOKTOURNAL MOTOSHOP

Muhammad Ridwan Firdaus [1)], **Sejati Waluyo, M.Kom**[2)]
Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5866369
E-mail : 1311501512@student.budiluhur.ac.id[1)], *sejati.waluyo@budiluhur.ac.id*[2)]

ABSTRAK

Aplikasi chatting merupakan suatu jenis dari perkembangan suatu teknologi. Dengan kecanggihan teknologi saat ini, fungsi aplikasi chatting tidak sebagai media komunikasi saja, tetapi dapat juga mengirimkan foto, dokumen, dan lain sebagainya. Dampak yang ditimbulkan dari penggunaan aplikasi chatting mungkin tidak disadari sama sekali. Selain memudahkan dalam berkomunikasi sebagai dampak positif yang user dapatkan, terdapat pula dampak negatif yang user dapatkan sebagai akibat dari menggunakan aplikasi chatting ini. Salah satu dampak negatifnya adalah bocornya data-data penting yang seharusnya tidak boleh diketahui oleh publik atau pihak-pihak yang tidak berkepentingan. Noktournal Motoshop bergerak dibidang penjualan aksesoris perlengkapan sepeda motor beserta pengendaranya, baik itu untuk menunjang berkendara sehari-hari maupun untuk menunjang berkendara dengan jarak jauh atau biasa disebut dengan touring. Saat ini proses jual-beli dan komunikasi antara seller dan buyer untuk aksesoris yang produk jadinya bersifat request by buyer atau bisa juga disebut produk custom, proses komunikasinya masih melalui telepon, SMS, atau datang langsung ke toko sehingga masih belum memenuhi kebutuhan komunikasi antara seller dan buyer secara efektif. Untuk mengatasi masalah diatas maka dibutuhkan suatu aplikasi chatting yang mampu mengamankan pesan yang dikirimkan penggunanya. Salah satu caranya adalah dengan mengimplementasikan suatu metode kriptografi. Metode kriptografi yang akan digunakan adalah algoritma Zig Zag Cipher. Zig Zag Cipher adalah algoritma kriptografi klasik dengan teknik transposisi kolom dan baris. Teknik transposisi ini menggunakan mutasi karakter pesan asli tidak dapat dibaca tanpa memiliki kunci untuk mengembalikan pesan tersebut ke bentuk semula. Dalam membangun aplikasi kriptografi ini, penulis menggunakan bahasa pemrograman PHP. Dengan menggabungkan algoritma kriptografi tersebut diharapkan aplikasi yang dibuat dapat memberikan keamanan tambahan terhadap pesan yang dikirim sehingga tetap terjaga kerahasiaannya.

Kata kunci : Kriptografi, *Zig Zag Cipher*, *Chatting*

1. PENDAHULUAN

Aplikasi *chatting* baik itu berbasis *website* ataupun *mobile* merupakan suatu jenis dari perkembangan suatu teknologi. Dengan kecanggihan teknologi saat ini, fungsi aplikasi *chatting* tidak hanya sebagai alat komunikasi biasa, tetapi dapat juga mengirimkan foto, dokumen, dan lain sebagainya. Dampak yang ditimbulkan dari penggunaan aplikasi *chatting* mungkin tidak disadari sama sekali oleh *user*. Selain lebih mudah dan efektif dalam berkomunikasi sebagai dampak positif yang didapatkan, terdapat pula dampak negatif yang *user* dapatkan sebagai akibat dari menggunakan aplikasi *chatting* ini. Salah satu dampak negatifnya adalah bocornya data-data penting yang seharusnya tidak boleh diketahui oleh publik atau pihak-pihak yang tidak berkepentingan. Keamanan dan kerahasiaan saat mengirim data menjadi sesuatu sangat penting dalam komunikasi data, baik untuk privasi individu ataupun untuk tujuan keamanan bersama, baik dari pihak pengirim maupun penerima pesan. Mereka yang menginginkan agar datanya tidak diketahui oleh publik atau individu yang tidak memiliki kepentingan terhadap data dikirimnya. Kebutuhan perlindungan akan kerahasiaan datapun meningkat, salah satu cara melindunginya adalah dengan menyandikan data atau enkripsi.

Noktournal Motoshop bergerak dibidang penjualan aksesoris perlengkapan sepeda motor beserta pengendaranya, baik itu untuk menunjang berkendara sehari-hari maupun untuk menunjang berkendara dengan jarak jauh atau biasa disebut dengan *touring*. Saat ini proses jual-beli dan komunikasi antara *seller* dan *buyer* masih melalui *website e-commerce* Tokopedia untuk aksesoris produksi pabrik, tetapi untuk aksesoris yang produk jadinya bersifat *request by buyer* atau bisa juga disebut produk *custom*. Proses komunikasinya masih melalui telepon, SMS, atau datang langsung ke toko sehingga masih kurang memenuhi kebutuhan komunikasi antara *seller* dan *buyer* secara mudah dan efektif.

Zig Zag Cipher adalah algoritma kriptografi klasik dengan teknik transposisi kolom dan baris. Teknik

transposisi ini menggunakan mutasi karakter yang mana pesan asli tidak dapat dibaca apabila tidak memiliki kunci untuk membuka pesan tersebut.

Dengan aplikasi *chatting* berbasis *website* diharapkan komunikasi antar pihak penjual dan pembeli menjadi lebih efektik dan lebih aman dalam hal komunikasi antara seller dan buyyer.

2. LANDASAN TEORI

2.1 Pengertian Kriptografi

Kriptografi ialah ilmu yang mempelajari bagaimana cara menjaga supaya pesan atau data tetap aman pada saat dikirimkan dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga [1]. Kriptografi adalah ilmu dan seni untuk menjaga keamanan ketika pesan dikirim dari suatu tempat ke tempat lain [2].

2.2 Sejarah Kriptografi

Kriptografi terdiri dari dua kata yang berasal dari bahasa Yunani, *Crypto* dan *graphia*. *Crypto* berarti rahasia dan *graphia* berarti tulisan. Sekitar 400 SM, kriptografi pada bidang militer digunakan oleh bangsa Spartan dalam bentuk potongan papirus atau perkamen dibungkus dengan kayu. Sistem ini disebut *Scytale* [3].

2.3 Tujuan Kriptografi

Tujuan dari kriptografi adalah bukan untuk menyembunyikan pesan, melainkan untuk menyembunyikan makna dari pesan tersebut.

2.4 Pengertian *Chat*

Chat merupakan salah satu media untuk berinteraksi antara sesama *user* sebuah *website* [4]. Komunikasi dengan orang lain secara *realtime* dengan mengetikan kata-kata, menyisipkan simbol, atau gambar.

Dengan adanya layanan *chat* memungkinkan kita untuk dapat berkomunikasi melalui internet dengan orang-orang yang berada di seluruh dunia [5].

2.5 Algoritma *Zig Zag Cipher*

Metode *Zig Zag Cipher* adalah algoritma kriptografi klasik dengan teknik transposisi kolom dan baris. Teknik transposisi kolom dan baris ini menggunakan mutasi karakter yang mana pesan yang asli tidak dapat dibaca kecuali memiliki kunci untuk mengembalikan pesan tersebut ke bentuk semula [6].

2.6 *Teknik* Pada Metode *Zig Zag Cipher*

Teknik transposisi adalah metode enkripsi dengan menyusun *plaintext* pada matriks secara baris, dan menghasilkan *ciphertext* dengan cara mengambil rangkaian karakter secara kolom. Teknik transposisi juga disebut metode permutasi. Teknik yang diterapkan pada metode *Zig Zag Cipher* adalah teknik transposisi *cipher* enkripsi dan dekripsi pesan dengan cara merubah urutan huruf-huruf yang ada di dalam *plaintext* (pesan yang belum dienkripsi) menjadi *ciphertext* dengan cara tertentu agar isi pesan tersebut tidak dimengerti kecuali oleh orang-orang tertentu. Pada dasarnya prinsip pengubahan pesan mirip dengan anagram seperti kata "melepas" diubah menjadi "saeeplm", tapi tentu saja transposisi *cipher* mempunyai rumus atau kunci tertentu yang diperlukan agar pesan bisa dimengerti. Transposisi *cipher* kolumnar atau diterapkan individual, lebih mudah untuk *cryptanalyze*. Zig zag yang terapkan dengan menggabungkan tiap pola zig zag dan kolumnar transposisi untuk menghasilkan *ciphertext* yang lebih sulit untuk *cryptanalyze*. Transposisi zig zag dapat dilakukan berturut-turut dengan cara membentuk baris atau kolom yang diatur dalam format matriks. Jika zig zag yang transposisi dilakukan baris, maka pesan dibaca dalam model zig zag berdasarkan angka dalam kunci. Jika digit dikuncinya adalah i, maka urutan posisi matriks pesan dibaca sebagai berikut:

(i, 1) (i +1, 2) (i, 3) (i +1, 4) (i, 5)

Jika transposisi kolom maka pesan dibaca

(1, i) (2, i +1) (3, i) (4, i +1) (5, i)

Setelah transposisi diproses dengan kunci pada enkripsi simetris *cipher*, kunci yang sama digunakan untuk dekripsi. Jika digit ke j dikuncinya adalah i, maka baris j teks *cipher* adalah:

(i, 1) (i +1, 2) (i, 3) (i +1, 4) (i, 5)

Jumlah digit pada kunci (*key*) yang digunakan pada algoritma *Zig Zag Cipher* tergantung pada jumlah baris jika menggunakan transposisi baris dan tergantung pada jumlah kolom jika menggunakan transposisi kolom.

2.7 *Contoh* Enkripsi *Zig Zag Cipher* Pada Proses Enkripsi *Chat*

Algoritma proses enkripsi *chat* terdiri dari langkah-langkah yang dilakukan untuk mengubah *plaintext* (pesan asli) menjadi sebuah *ciphertext* (pesan rahasia) yang tidak dapat diterjemahkan secara langsung oleh penerima pesan. Proses pembentukan *ciphertext* menjadi *plaintext* menggunakan pola zig zag yang merupakan konsep dasar dari matriks. Dalam pembentukan matriks kunci akan menbentuk berapa banyak jumlah baris dan berapa banyak jumlah karakter pada *chat* membentuk berapa banyak kolom sesuai konsep dasar dari matriks. Namun enkripsi dapat juga dilakukan dengan memulainya bukan dari baris paling atas (*offset* = 1), tetapi dapat juga dari baris lainnya berdasarkan jumlah baris yang didapat dari proses pembentukan matriks kunci. Untuk lebih jelasnya dapat dilihat gambar di bawah ini penentuan nilai *offset* berdasarkan kunci (*key*).

Nilai Kunci (*key*)	*Offset* (Baris)
2	1-2
3	1-3
4	1-4
-	-
-	-

Gambar 1: Penentuan Nilai Offset

1) Pola Enkripsi *Zig Zag Cipher Key*=2 *Offset*=1
Berikut adalah contoh pola algoritma enkripsi *Zig Zag Cipher* dengan ketentuan:
Plaintext : "KEAMANAN CHAT"
Key : 2
Offset : 1
Key = 2 dan *offset* = 1 artinya adalah dalam 2 baris, karakter pertama dimulai dari baris ke-1. Untuk banyaknya karakter terdiri dari 12, dalam pembentukan pola enkripsi ini karakter spasi tidak dihitung dalam proses pembentukan *ciphertext* (pesan rahasia). Dari ketentuan diatas maka diperoleh pola algoritma *Zig Zag Cipher* dan *ciphertext* sebagai berikut:

BARIS (*Offset*) 1	K		A		A		A		C		A	
BARIS (*Offset*) 2		E		M		N		N		H		T

Gambar 2: Pola Zig Zag Cipher key=2 offset=1

Maka *ciphertext* hasil enkripsi dengan membaca karakter yang ada tiap barisnya dimulai dari baris pertama adalah: "**KAACAEMNNHT**".

2) Pola Enkripsi *Zig Zag Cipher Key*=3 *Offset*=2
Berikut adalah contoh pola algoritma enkripsi *Zig Zag Cipher* dengan ketentuan:
Plaintext : "KEAMANAN CHAT"
Key : 3
Offset : 2
Dari ketentuan diatas (karakter spasi tidak disertakan dalam pembentukan *ciphertext*) maka diperoleh pola algoritma *Zig Zag Cipher* dan *ciphertext* sebagai berikut:

BARIS (*Offset*) 1				M				N				T
BARIS (*Offset*) 2	K		A		A		A		C		A	
BARIS (*Offset*) 3		E				N				H		

Gambar 3: Pola Zig Zag Cipher key=3 offset=2

Maka *ciphertext* hasil enkripsi dengan membaca karakter yang ada tiap barisnya dimulai dari baris pertama adalah: "**MNTKAACAENH**".

3) Pola Dekripsi *Zig Zag Cipher Key*=2 *Offset*=1
Ciphertext : "KAACAEMNNHT"
Key : 2
Offset : 1
Jumlah Karakter : 12 (Banyak Kolom)

Gambarkan urutan/baris sesuai jumlah karakter dan *key* lalu inialisasikan dengan karakter lain, atur karakter sesuai dengan spesifikasi *key* dan *offset*.

Tabel 1: Susunan Karakter

Baris 1	X		X		X		X		X		X	
Baris 2		X		X		X		X		X		X

Setelah itu masukan *ciphertext* secara urut dimulai dari baris pertama sampai akhir (parameter inialisasi karakter lain) lalu dilanjutkan dengan baris selanjutnya hingga selesai. Bila digambarkan sebagai berikut:

Tabel 2: Susunan Karakter

Baris 1	K		A		A		A		C		A	
Baris 2		E		M		N		N		H		T

Langkah terakhir tinggal baca sesuai urutan *zig zag* dimulai dari karakter pertama hingga diperoleh *plaintext* "KEAMANANCHAT" dari *ciphertext* "KAACAEMNHT"

3. RANCANGAN SISTEM DAN APLIKASI

3.1 Model Data Relasional

1) *admin_login*

Tabel 3: Tabel admin_login

admin_id	username	Password
PK		

2) *header*

Tabel 4: Tabel header

header_id	admin_id	user_id	time
PK			

3) *message*

Tabel 5: Tabel message

message_id	header_id	is_from_sender	content	time
PK				

4) *user_login*

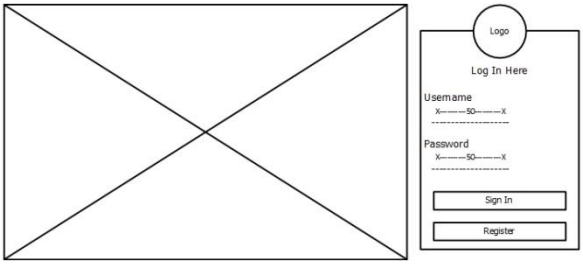
Tabel 6: Tabel user_login

user_id	Username	password	email
PK			

3.2 Rancangan Layar

1) Rancangan Layar *User Login Form*

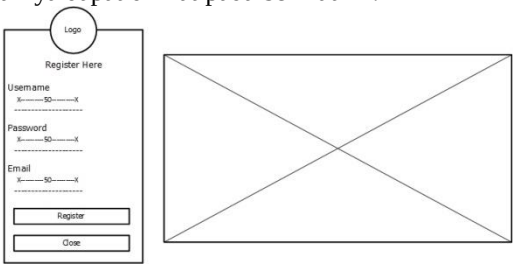
Pada rancangan layar *User Login Form* merupakan tampilan awal ketika *website* dibuka. Agar fitur *chat*-nya dapat digunakan, langkah pertama yang harus dilakukan *user* adalah melakukan proses *login* melalui tampilan *form* yang tersedia dengan mengisi *password* dan *username*, untuk rancangan layarnya bisa dilihat pada gambar berikut ini:



Gambar 4: Rancangan Layar User Login Form

2) Rancangan Layar *Register Form*

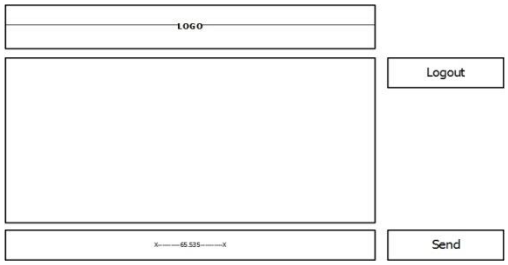
Apabila *user* belum memiliki akun, maka diharuskan untuk membuatnya terlebih dahulu dengan cara mengisi data dihalaman *Register Form*. Halaman ini dapat diakses dengan menekan tombol "*Register*" dihalaman *User Login Form*. Untuk rancangan layarnya dapat dilihat pada berikut ini:



Gambar 5: Rancangan Layar Register Form

3) Rancangan Layar *User Chat Room*

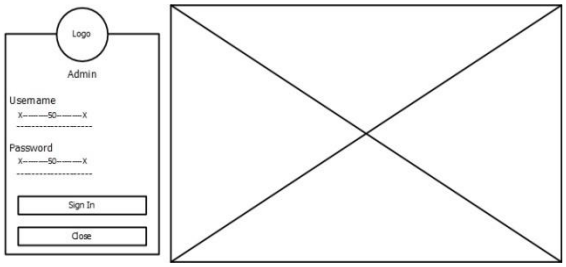
Setelah proses *login* selesai maka akan muncul tampilan *chat room*. Halaman ini berfungsi untuk melakukan proses komunikasi antara *admin* dan *user*. Untuk tampilannya dapat dilihat pada gambar di bawah ini:



Gambar 6: Rancangan Layar User Chat Room

4) Rancangan Layar *Admin Login Form*

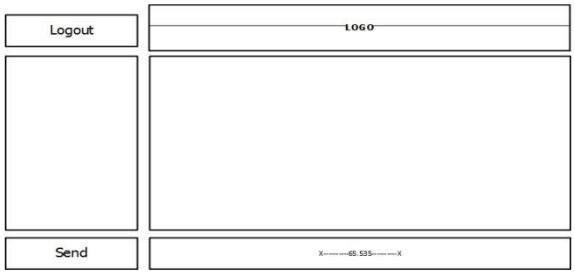
Pada rancangan layar *Admin Login Form* merupakan tampilan awal bagi *admin*. Sebelum menggunakan aplikasi ini, langkah pertama yang harus dilakukan *admin* adalah melakukan proses *login* melalui tampilan *form* yang tersedia dengan mengisi *password* dan *username*, untuk rancangan layarnya bisa dilihat pada gambar berikut ini:



Gambar 7: Rancangan Layar Admin Login Form

5) Rancangan Layar *Admin Chat Room*

Setelah proses *login* selesai maka akan muncul tampilan *chat room*. Halaman ini berfungsi untuk melakukan proses komunikasi antara *admin* dan *user*. Untuk tampilannya khusus bagian *admin* bisa dilihat pada gambar di bawah ini:

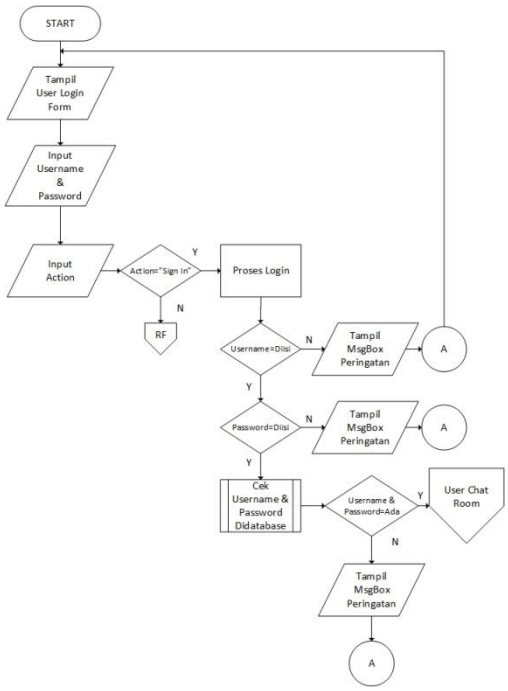


Gambar 8: Rancangan Layar Admin Chat Room

3.3 *Flowchart*

1) *Flowchart User Login Form*

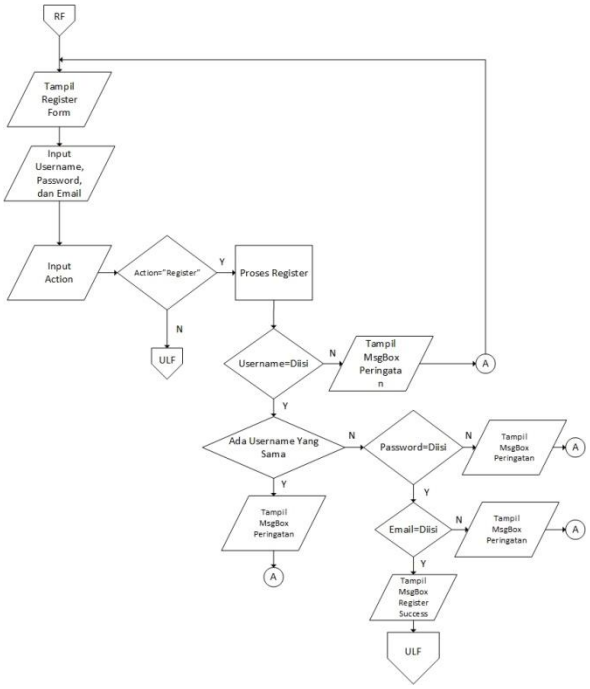
Pada saat aplikasi *chatting* ini diakses oleh pengguna, maka tampilan pertama yang dilihat oleh pengguna adalah halaman *user login form*. Pada halaman ini terdapat *form login* yang harus diisi oleh pengguna apabila ingin menggunakan fitur *chat* dari *website* ini. Pertama pengguna harus menginput *username* dan *password* lalu pengguna harus memilih tombol *Sign In*, jika *username* dan *password* cocok di*database* maka pengguna akan masuk ke halaman *user chat room*. *Flowchart* halaman *user login form* dapat dilihat pada gambar berikut:



Gambar 9: Flowchart User Login Form

2) *Flowchart Register Form*

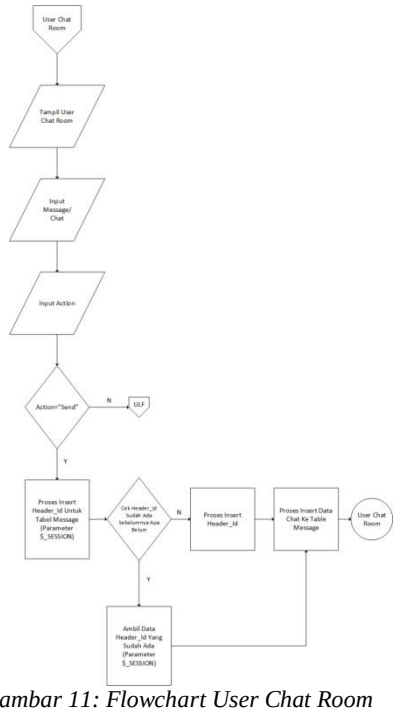
Apabila pengguna belum memiliki akun maka diharuskan membuatnya terlebih dahulu dengan cara memilih tombol *register*. Disini pengguna akan diminta mengisi data seperti *username*, *password*, dan *email* yang nantinya akan digunakan untuk *login*. Untuk *flowchart* halaman *register* bisa dilihat pada gambar di bawah ini:



Gambar 10: Flowchart Register Form

3) *Flowchart User Chat Room*

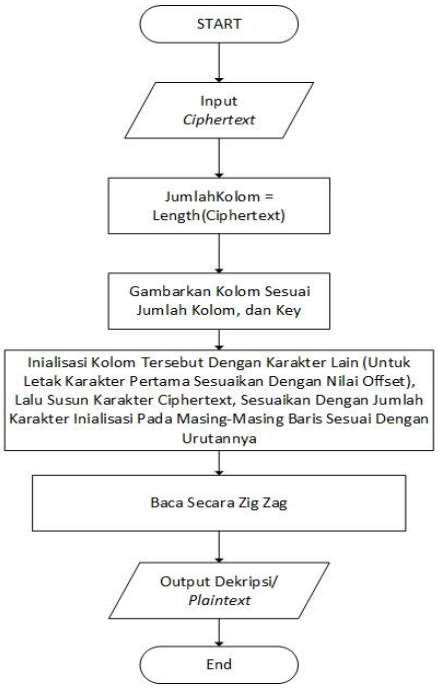
Setelah pengguna melakukan proses *login* maka dapat menggunakan fitur *chat* dari aplikasi *chatting* ini. Disini dijelaskan bagaimana proses data *chat* yang di*input* pengguna dapat masuk dan tersimpan ke dalam *database*. Untuk lebih jelasnya dapat dilihat pada gambar di bawah ini:



Gambar 11: Flowchart User Chat Room

4) *Flowchart Flowchart Enkripsi dan Dekripsi Zig Zag Cipher*

Gambar 12: Flowchart Enkripsi Zig Zag Cipher

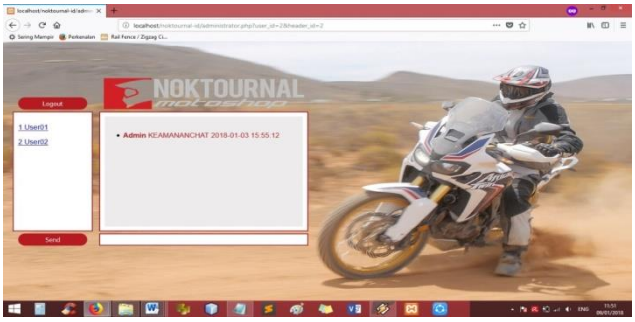


Gambar 13: Flowchart Dekripsi Zig Zag Cipher

4. IMPLEMENTASI DAN UJI COBA PROGRAM

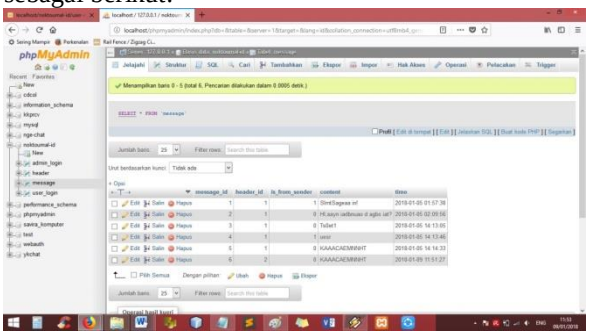
4.1 Proses Enkripsi dan Dekripsi Chat

Pengujian enkripsi ini dimulai dari sisi *admin* dimana *admin* akan mengirimkan chat kepada salah satu *user*, untuk lebih jelasnya akan diperlihatkan pada gambar di bawah ini:



Gambar 14: Uji Coba Chat dari Admin ke User-01

Dalam pengujian ini *admin* mengirimkan *chat* "KEAMANANCHAT" kepada "User02", untuk tampilan *database* dan hasil enkripsinya adalah sebagai berikut:



Gambar 15: Uji Coba Chat dari Admin ke User-02

Lalu pada tampilan *user chat room* dengan akun "User02", *chat* yang dikirim dari *admin* akan muncul dalam keadaan sudah terdekripsi.

Gambar 16: Uji Coba Chat dari Admin ke User-03

4.2 Tabel Pengujian

Dalam pengujian kali ini akan dibahas mengenai perbandingan antara proses enkripsi dan dekripsi. Pesan yang diuji meliputi nilai *key* dan *offset* yang berbeda-beda. Agar mempermudah dalam membaca

hasil tabel pengujian maka *plaintext* yang diujikan tidak menggunakan spasi.

Tabel 5: Tabel Pengujian Proses Enkripsi

Plaintext	**Jumlah Karakter**	**Nilai *Key***	**Nilai *Offset***	**Hasil Enkripsi**	**Waktu (Detik)**
KEAMAN ANCHAT	11	2	1	KAAACA EMNNHT	0,20
KEAMAN ANCHAT	11	3	2	MNTKAA ACAENH	0,30
KEAMAN ANCHAT	11	2	2	EMNNHT KAAACA	0,20
KEAMAN ANCHAT	11	4	3	AAMNHT KAACEN	0,20
KEAMAN ANCHAT	11	4	4	MHAACA ENNTKA	0,40

5. KESIMPULAN DAN SARAN

Berdasarkan perancangan, pembuatan, analisa program dan serangkaian uji coba dari aplikasi *chatting* ini, maka dapat diambil suatu kesimpulan antara lain:

1) Algoritma kriptografi *Zig Zag Cipher* dapat diimplementasikan pada aplikasi keamanan *chat.*
2) Meminimalisir kebocoran pesan yang terdapat pada aplikasi ini.
3) Proses enkripsi dan dekripsi sudah diatur oleh sistem agar berjalan secara otomatis.

Adapun saran yang mungkin diperlukan untuk membuat aplikasi *chatting* ini dapat berjalan lebih baik lagi antara lain:

1) Dapat dikembangkan menjadi aplikasi berbasis *mobile*.
2) Tidak hanya pesan *text* yang dapat dikirim dan dienkripsi, ke depannya diharapkan bisa mengirim pesan berupa gambar.
3) Bisa dikembangkan menjadi toko *online* sehingga dapat meningkatkan *branding* toko yang bersangkutan.

6. DAFTAR PUSTAKA

[1] A. Halimatusadiah and E. Insanudin, "IMPLEMENTASI KRIPTOGRAFI METODE CAESAR CHIPER PADA CHATING BERBASIS WEB," *CAESAR CIPHER CHATING*, vol. 1, no. 20, pp. 1–5, 2016.

[2] E. Sularsono, W. S. Raharjo, and Y. Lukito, "IMPLEMENTASI ALGORITMA RIJNDAEL 128 PADA APLIKASI CHATTING BERBASIS HTML5 WEBSOCKET," *J. Teknol. Komput. dan Inform.*, vol. 10, no. 2, pp. 66–79, 2014.

[3] H. Pandiangan and S. Sijabat, "Perancangan Media Pengiriman Pesan Teks Dengan Penyandian Pesan Menggunakan Algoritma RC4 Berbasis Web," *J. Matik Penusa*, vol. 19, no. 1, pp. 63–71, 2016.

[4] A. Gunawan, A. Adnan, and Bachtiar, "Perancangan Website Webchat Menggunakan PHP Dan MySQL," *J. InTekSis*, vol. 3, no. 1, pp. 70–78, 2016.

[5] F. Adinta and I. Neforawati, "Pemanfaatan Docker pada Aplikasi Chatting Berbasis Web," 2017.

[6] R. Kristianto Hondro, "APLIKASI ENKRIPSI DAN DEKRIPSI SMS DENGAN ALGORITMA ZIG ZAG CIPHER PADA MOBILE PHONE BERBASIS ANDROID," *Pelita Inform. Budi Darma*, vol. X, no. 3, pp. 122–127, 2015.