Vigenere Cipher dan Affine Cipher untuk Pengamanan Chatting Berbasis Android

Ahcmad Syahroji[1)], Rizky Pradana[2)]
[1,2)]*Program Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur*
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5866369
asyahroji96@gmail.com [1)] ,rizky.pradana@budiluhur.ac.id [2)]

ABSTRAK

Berkomunikasi merupakan salah satu kegiatan yang sering dilakukan di seluruh lapisan masyarakat, baik secara langsung maupun tidak langsung. Perubahan dalam berkomunikasi di saat ini, terpengaruhi oleh perkembangan teknologi dan informasi. Salah satu perubahannya adalah penggunaan aplikasi chatting seperti WhatApp, BBM, Line dan lain-lain untuk berkomunikasi. Dalam dunia pendidikan itu sendiri dengan menggunakan aplikasi chatting tersebut adalah salah satu cara untuk berkomunikasi bagi beberapa orang tua yang tidak dapat menemui langsung wali kelas dikarenakan kesibukkan dari beberapa orang tua tersebut. Dengan menggunakan aplikasi chatting berguna untuk menyampaikan informasi penting yang perlu disampaikan kepada orang tua/wali murid dengan cepat dibandingkan dengan menyampaikan informasi tersebut melalui siswa/siswi yang kemungkinan tidak sampai kepada orang tua. Namun, pesan yang dikirim oleh orang tua maupun wali kelas dengan aplikasi chatting tersebut tidak langsung membaca pesan tersebut dikarenakan anggapan orang tua atau wali kelas terhadap pesan tersebut bersifat broadcast atau pesan lain yang bisa dibaca di lain waktu. Selain itu pesan yang berisi informasi yang berhubungan dengan sekolah tercampur dengan pesan pribadi milik orang tua maupun wali kelas sehingga pesan tidak langsung dibaca. Tujuan dari penelitian ini untuk menghasilkan suatu aplikasi chatting berbasis Android yang digunakan untuk pertukaran pesan/informasi antara wali kelas dengan orang tua maupun sebaliknya. Kemudian pengamanan pada aplikasi chatting tersebut, menggunakan algoritma kriptografi Vigenere Cipher dan Affine Cipher sehingga pesan yang bersifat pribadi maupun pesan yang bersifat rahasia terjamin akan keamanannya. Algoritma kriptografi Vigenere Cipher dan Affine Cipher dapat mengamanakan pesan dan dapat diimplementasikan ke dalam aplikasi chatting berbasis Android dengan menggunakan database Firebase. Hasil dari pengujian pada aplikasi chatting ini, bahwa pesan yang telah dikirim berhasil dienkripsi dan dapat mengembalikkan pesan tersebut seperti semula dengan keberhasilan sebesar 100%. Aplikasi ini dapat mengirim dan menerima pesan yang dapat dilakukan oleh orang tua/wali murid maupun wali kelas secara langsung dengan pengamanan pada pesan yang dikirim.

Kata Kunci : Chatting, Vigenere Cipher, Affine Cipher, Android, Firebase.

1. PENDAHULUAN

1.1 Latar Belakang

Berkomunikasi merupakan salah satu kegiatan yang sering dilakukan di seluruh lapisan masyarakat, baik secara langsung maupun tidak langsung. Perubahan dalam berkomunikasi di saat ini, terpengaruhi oleh perkembangan teknologi dan informasi. Pengiriman pesan memalui *smartphone* seperti *chatting* adalah salah satu contoh dari perubahan dalam berkomunikasi tersebut. Hingga saat ini masyarakat menggunakan aplikasi *chatting* untuk mengirim pesan teks, *file*, berbagi gambar, dan lain-lain. Adapun dampak *negative* yang ditimbulkan penggunaan pada aplikasi ini seperti pencurian data secara ilegal yang dapat merugikan banyak pihak.

Aplikasi *chatting* telah menjadi media berkomunikasi di semua kalangan maupun diberbagai macam bidang, tidak terkecuali di dunia pendidikan. Namun, di dalam dunia pendidikan saat ini, komunikasi antara orang tua/wali murid secara langsung maupun tidak langsung masih jarang dilakukan. Seharusnya orang tua/wali murid berpartisipasi dengan cara berkomunikasi tentang perkembangan / pengawasan anaknya di sekolah. Faktor kesibukkan masing-masing orang tua/wali murid menjadi salah satu penyebab berkomunikasi antara orang tua murid dan wali kelas tidak terjadi, tidak terkecuali SMK PANCAKARYA KOTA TANGERANG. Kurangnya komunikasi antara orang tua murid dengan wali kelas, menyebabkan lemahnya perhatian/pengawasan terhadap anak atau murid di sekolah. Orang tua murid lebih mempercayakan peran wali kelas atau tidak ikut berpartisipasi dalam mengawasi terhadap anaknya di sekolah. Pada saat tertentu mengirim pesan melalui aplikasi *chatting* pada umumnya, pesan tidak langsung dibaca oleh orang tua murid dikarenakan anggapan orang tua murid terhadap pesan tersebut bersifat *broadcast* atau pesan lain yang bisa dibaca dilain waktu, sehingga tidak langsung membaca pesan tersebut. Adapun pesan informasi yang tidak melalui aplikasi *chatting*, jika

surat/pesan yang biasanya diberikan oleh guru melalui siswa/i yang bersangkutan dimana surat/pesan itu menjadi tidak tersampaikan langsung kepada orang tua murid. Maka dari itu, dibutuhkanlah suatu media khusus untuk orang tua murid dan wali kelas yaitu, aplikasi *chatting* berbasis Android yang dapat digunakan untuk berbagi informasi antara wali kelas dan orang tua murid yang berkaitan di sekolah secara khusus. Wali kelas ataupun orang tua murid dapat memprioritaskan pesan tersebut dengan tetap menjaga keamanan informasi yang dikirimkan dengan menggunakan salah satu teknik metode kriptografi.

Kriptografi merupakan ilmu atau seni yang dibuat untuk menjaga keamanan pesan/teks. Dalam pembuatan aplikasi *chatting*, keamanan adalah aspek penting yang harus menjadi perhatian dalam dunia teknologi informasi, dimana terdapat informasi yang masuk dan pesan tersebut dapat bersifat pribadi maupun rahasia, maka diperlukanlah sebuah pengamanan kriptografi pada aplikasi *chatting* berbasis Android ini menggunakan metode Vigenere Cipher dan metode Affine Cipher. Pesan/teks dienkripsi menggunakan metode Vigenere Cipher ini akan mengubah pesan/teks menjadi *ciphertext* atau pesan/teks acak. Kemudian pesan/teks yang terenkripsi tersebut dilakukan pengenkripsian kembali dengan menggunakan metode Affine Cipher, setelah itu disimpan ke media penyimpanan. Pesan/teks yang telah tersimpan tersebut memiliki keamanan yang baik dikarenakan pesan tersebut terenkripsi. Sebelum pesan/teks diterima oleh penerima pesan maka, dilakukan dekripsi menggunkan metode Affine Cipher dan setelah itu didekripsikan kembali dengan menggunakan metode Vigenere Cipher agar menjadi pesan/teks semula sehingga dapat dibaca dan diterima oleh penerima pesan. Aplikasi *chatting* berbasis Android ini, menggunakan media penyimpanan *realtime database* Firebase yang bersifat *real-time* yang cepat dan akurat.

1.2 Tujuan Penelitian

Berdasarkan dari rumusan masalah yang telah diuraikan, maka tujuan penulisan adalah sebagai berikut :

a. Membuat aplikasi *chatting* berbasis Android dengan pengamanan data/pesan.
b. Membuat aplikasi *chatting* dengan menggunakan algoritma enkripsi Vigenere Cipher dan Affine Cipher.
c. Mengubah pesan *plaintext* menjadi *ciphertext* dan mengembalikannya lagi secara otomatis.

1.3 Batasan Masalah

Dari permasalahan yang ada pada perumusan masalah, penulis memfokuskan batasan masalah sebagai berikut :

a. Algoritma yang digunakan yaitu, Vigenere Cipher dan Affine Cipher.
b. Media penyimpanan yang digunakan pada aplikasi *chatting* ini menggunakan Firebase.
c. Aplikasi dibuat berbasis Android.
d. Hanya dapat mengirim teks.

2. STUDI LITERATUR

Menggunakan algoritma Vigenere Cipher untuk aplikasi *chatting* rahasia yaitu kriptografi merupakan salah satu cara yang dapat digunakan untuk mengamankan berbagai tipe file, salah satunya berupa pesan teks [5]. Salah satu solusi untuk menjaga keamanan dan kerahasiaan pada proses pengiriman data dengan menggunakan teknik kriptografi [2]. Algoritma kriptografi berdasarkan data pengkodean informasi yang mendukung kebutuhan dua aspek keamanan informasi, yaitu kerahasiaan (perlindungan kerahasiaan data informasi) dan keaslian (perlindungan terhadap pemalsuan dan perubahan informasi yang tidak diinginkan) [3]. Penggunaan fungsi *hash* pada pengamanan data atau informasi pada sebuah *website* dirasa sudah tidak aman lagi, dan memiliki kelemahan berupa *collision* sehingga solusi yang tepat adalah memodifikasi dan mengimplementasikan algoritma atau metode yang digunakan [4]. Dengan menggunakan algoritma kriptografi Affine Cipher dan Rivest Code 4 (RC4) dapat mengenkripsikan semua jenis file baik audio maupun video dan dapat mendekripsikannya kembali sehingga menjadi file semula [1].

3. METODOLOGI PENELITIAN

3.1 Analisa Masalah

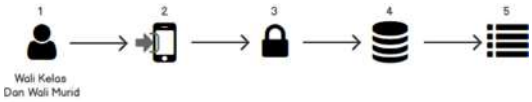
Komunikasi yang dilakukan secara langsung maupun tidak langsung antara orang tua murid dengan wali kelas ataupun sebaliknya dapat disimpulkan masih kurang baik. Dengan komunikasi yang baik antara orang tua dan wali kelas/guru dapat memberikan dampak positif terhadap perkembangan anak di sekolah. Beberapa orang tua/wali murid mempunyai aktivitas sehingga tidak adanya kesempatan untuk menemui langsung wali kelas/guru. Adapun dengan menggunakan aplikasi *chatting* yang sudah banyak digunakan oleh masyarakat seperti Whatapp, Line, BBM, dan lain-lain. Namun, dengan aplikasi tersebut tidak sedikit terjadinya pesan diabaikan atau membaca pesan tersebut di lain waktu, dikarenakan tercampurnya antara pesan pribadi orang tua/wali murid maupun wali kelas/guru dengan pesan penting yang berhubungan dengan sekolah sehingga pesan tidak langsung dibaca oleh orang tua murid.

3.2 Pemecahan Masalah

Berdasarkan masalah yang telah dijabarkan di atas maka dapat disimpulkan bagaimana membuat

komunikasi antara orang tua/wali murid dengan wali kelas/guru dapat terjalin dengan baik tanpa terkendala dengan waktu. Diperlukan suatu aplikasi *chatting* yang secara khusus untuk media komunikasi antara wali kelas dan orang tua murid agar dapat digunakan untuk berbagi informasi yang berkaitan di sekolah. Disamping itu, untuk menjaga keamanan data dikarenakan pesan tersebut bersifat rahasia atau pribadi maka sebelum pesan dikirim digunakan metode kriptografi Vigenere Cipher dan Affine Cipher pada pesan yang akan dikirim. Setelah itu pesan tersebut disimpan di media penyimpanan yaitu *realtime database* Firebase, lalu pesan tersebut dilakukan dekripsi atau mengembalikan pesan yang telah diacak sehingga menjadi pesan dapat dibaca kembali seperti semula kepada penerima pesan.

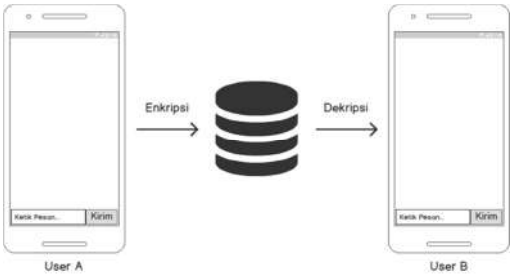
3.3 Skema Proses Sistem Aplikasi



Gambar 1 : Skema Inti Aplikasi

Pada aplikasi dapat dijelaskan inti dari proses aplikasi *chatting* wali kelas / wali murid dapat. Adalah sebagai berikut :

a. Pengguna yang dapat menggunakan pada aplikasi ini adalah wali kelas atau wali murid.
b. Pengguna wali kelas ataupun wali murid harus mengisi data untuk *login* pada aplikasi ini sebelum menggunakannya.
c. Data diisikan tersebut dilakukan proses enkripsi menggunakan metode Vigenere Cipher dan Affine Cipher.
d. Setelah proses enkripsi selesai data tersebut ke dalam *realtime database* Firebase.
e. Jika proses registrasi berhasil, wali kelas dan wali murid langsung masuk ke *chat room*. Untuk melakukan *chatting* atau mengirim pesan, wali kelas atau wali murid dapat memilih salah satu *chat room* dan akan masuk ke *chatting room*. Penjelasan pada pengiriman pesan dapat dilihat berikut ini :



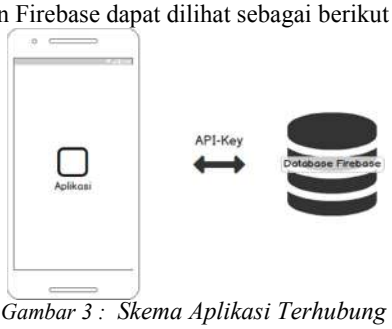
Gambar 2 : Proses Chatting

Dalam proses pengiriman pesan terdapat 2 poin penting dalam skema proses pengiriman pesan yaitu :

1) Pada tahap mengirim pesan, pesan tersebut dienkripsi menggunakan metode algoritma Vigenere Cipher dan Affine Cipher. Kemudian, disimpan di dalam *database* Firebase secara *real-time*.
2) Sebelum penerima pesan mendapatkan pesan. Pesan yang tersimpan di *database* Firebase akan dibaca oleh program dan didekripsi menggunakan metode algoritma Vigenere Cipher dan Affine Cipher, kemudian ditampilkan pada penerima pesan.

3.4 Skema Aplikasi Terhubung ke Firebase

Sebelum aplikasi dapat menyimpan sebuah data ke dalam *realtime database* Firebase, maka dalam proses pembuatan aplikasi diperlukan suatu sinkronisasi antara aplikasi yang dibuat melalui editor Android Studio dengan Firebase. Dalam tahap sinkronisasi tersebut dibutuhkan API-key dan sebuah file .json yang secara otomatis dibuatkan oleh Firebase. Skema proses aplikasi terhubung dengan Firebase dapat dilihat sebagai berikut :



Gambar 3 : Skema Aplikasi Terhubung ke Database Firebase

Sebelum menggunakan layanan yang ada pada Firebase ada beberapa tahapan yang harus dilakukan pengguna, sebelum aplikasi tersebut dapat berfungsi untuk menyimpan data ke dalam layanan Firebase. Skema proses tersebut dapat dilihat sebagai berikut :

Gambar 4 : Skema Menggunakan Firebase

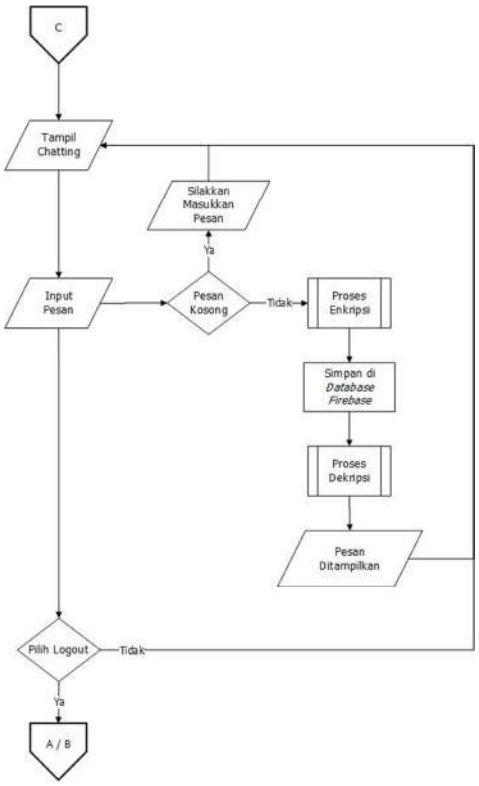
a. Tahap pertama yang dilakukan oleh *developer* adalah *login* dengan menggunakan akun Google. Pada halaman konsol Firebase, *developer* dapat membuat *project* dengan cara menekan tombol "Tambahkan proyek" dan diisikan nama *project* dan negara.
b. Pilih *platform* yang akan digunakan, setelah itu lakukan sinkronisasi aplikasi yang dibuat melalui Android Studio dengan tahapan yang ada pada Firebase. Setelah berhasil pada tahapan tersebut maka, layanan yang ada pada Firebase dapat digunakan.

3.5 *Flowchart*

Berikut ini adalah beberapa alur pada aplikasi yang dijalankan dengan menggunakan diagram *flowchart*. Berikut ini adalah *flowchart chatting* :

a. *Flowchart Chatting*

Pada saat pengguna wali kelas atau wali murid memilih salah satu *chat room* yang ada, maka pengguna langsung dapat mengirim dan menerima pesan pada *chatting* (C). Untuk aktivitas *chatting* digunakan metode kriptografi Vigenere Cipher dan Affine Cipher untuk melakukan enkripsi pada pesan yang dikirim, sehingga pada *database* Firebase pesan tersebut terenkripsi atau menjadi *ciphertext*. Untuk menampilkan agar pesan *ciphertext* tersebut agar dapat dilihat oleh pengguna, maka pesan tersebut diambil pada *database* Firebase lalu dilakukan proses dekripsi. Pada *flowchart* ini, wali kelas jika *logout* maka akan ke *login* wali kelas (A) dan wali murid jika *logout* maka akan ke *login* wali murid (B). Berikut ini adalah *flowchart chatting* wali kelas



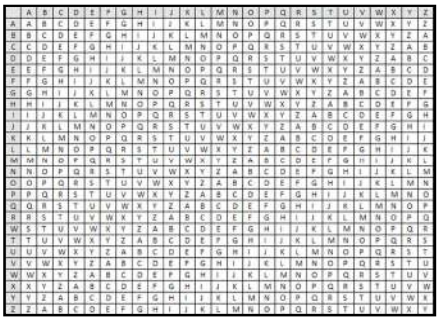
dan wali murid :

Gambar 5 : Flowchart Chatting

Enkripsi :

1) Proses Enkripsi Vigenere Cipher

Vigenere Cipher dapat menggunakan sebuah tabel Vigenere untuk mengenkripsikan sebuah *plaintext* yang terdiri dari 26 baris dan



kolom alfabet, dimana pada masing-masing baris tersebut digeser satu huruf ke kiri.

Gambar 6 : Tabel Vigenere

Sebagai contoh, teks asli (*plaintext*) yang akan dienkripsikan adalah "TEKNIK INFORMATIKA", sedangkan kata untuk kunci adalah "BUDI LUHUR". Jika panjang kunci lebih pendek dari teks asli (*plaintext*), maka kunci diulang secara periodik sehingga kunci menjadi "BUDILU HURBUDILUHU". Pada tabel Vigenere gambar 2.4 menunjukkan, jika huruf "T" ditemukan dengan huruf "B" maka akan menghasilkan huruf "U", lalu huruf "E" bertemu dengan huruf "U" menghasilkan huruf "Y", dan seterusnya. Sehingga hasil seluruhya dapat dilihat sebagai berikut ini :

Teks Asli : TEKNIK INFORMATIKA
Kunci : BUDILU HURBUDILUHU
Teks Acak : UYNVTE PHWPLPIECRU

Dapat disimpulkan, bahwa huruf yang sama di dalam teks asli tidak selalu dienkripsikan dengan huruf chipertext yang sama pula. Sehingga Vigenere Cipher termasuk ke dalam algoritma yang aman. Model matematika pada Vigenere Cipher dapat ditulis sebagai berikut ini :

$C_i = (P_i + K_i) \bmod 26$

Keterangan :
C_i = Nilai desimal karakter teks acak ke-i
P_i = Nilai desimal karakter teks asli ke-i
K_i = Nilai desimal karakter kunci ke-i
Nilai desimal karakter = A=0, B=1, C=2, ... Z=25.

Contoh :

Huruf Asli : T=19
Huruf Kunci : B=1
$C_i = (P_i + K_i) \bmod 26$
$C_i = (19+1) \bmod 26$
$C_i = (20) \bmod 26$
$C_i = 20$ (20 = huruf U)

Huruf Asli : E=4
Huruf Kunci : U=20
$C_i = (P_i + K_i) \bmod 26$
$C_i = (4+20) \bmod 26$

C_i = (24) mod 26
C_i = 24 (24 = huruf Y)

2) Proses Enkripsi Affine Cipher

Pada proses enkripsi algoritma Affine Cipher menggunakan 2 buah kunci yaitu 1 (a) dan 1 kunci (b) untuk menghasilkan sebuah *ciphertext* atau pesan acak. Plaintext (P_i) akan dikonversikan menggunakan tabel konversi sehingga menjadi angka desimal, kemudian ciphertext (C_i) akan diperoleh dengan mengenkripsi plaintext dengan persamaan :

$$C_i = (a\ P_i + b) \bmod 26 \quad \ldots\ldots\ldots (1)$$

Keterangan :
C_i = *ciphertext* dari pergeseran karakter yang terdapat pada *plaintext*.
P_i = pergeseran karakter pada *plaintext*.
a = bilangan bulat yang relatif prima dengan 26.
b = pergeseran relatif prima dari a.

Adapun hasil yang didapatkan pada (1) maka, dari bilangan desimal tersebut akan dikonversikan menggunakan tabel menjadi ciphertext yang diinginkan.

Dekripsi :

1) Proses Dekripsi Affine Cipher

Proses dekripsi algoritma Affine Cipher digunakan dua buah kunci yang mana kedua kunci tersebut haruslah sama dengan kunci yang digunakan dalam proses enkripsi. Agar dapat memperoleh plaintext maka kunci 1 (a) akan dirubah dalam bentuk invers a (mod 26), dinyatakan dengan a^{-1} :

$$P_i = a^{-1}(C_i - b) \bmod 26 \quad \ldots\ldots\ldots (2)$$

Keterangan :
P_i = plaintext dari pergeseran karakter yang terdapat pada ciphertext.
C_i = pergeseran karakter pada ciphertext.
a dan b = kunci yang sama dengan kunci yang digunakan pada proses enkripsi.

Sebelum melakukan perhitungan pada (2) maka, C_i harus dikonversikan terlebih dahulu ke dalam bentuk desimal menggunakan tabel konversi. Hasil dari konversi bilangan desimal tersebut kemudian akan dikonversikan kembali menggunakan tabel konversi untuk memperoleh *plaintext*.

2) Proses Dekripsi Vigenere Cipher

Untuk melakukan dekripsi pada Vigenere Cipher, dapat menggunakan kebalikan dari fungsi enkripsinya. Model matematika untuk dekripsi *pada* Vigenere Cipher dapat ditulis sebagai berikut :

$$P_i = (C_i - K_i) \bmod 26$$

Keterangan :
C_i = Nilai desimal karakter teks acak ke-i
P_i = Nilai desimal karakter teks asli ke-i
K_i = Nilai desimal karakter kunci ke-i
Nilai desimal karakter = A=0, B=1, C=2 .... Z=25.

Contoh :

Huruf Acak : U=20
Huruf Kunci : B=1
$P_i = (C_i - K_i) \bmod 26$
$C_i = (20 - 1) \bmod 26$
$C_i = (19) \bmod 26$
C_i = 19 (19 = huruf T)

Huruf Acak : P=15
Huruf Kunci : H=7
$P_i = (C_i - K_i) \bmod 26$
$C_i = (15 - 7) \bmod 26$
$C_i = (8) \bmod 26$
C_i = 8 (8 = huruf I)

4. HASIL DAN PEMBAHASAN

4.1 Implementasi Antarmuka

a. Tampilan Menu Utama

Pada saat aplikasi ini dijalankan, pengguna langsung diarahkan untuk memilih tipe *user* yaitu wali kelas dan wali murid. *Login* sebagai wali kelas dikhususkan untuk wali kelas dan *login* sebagai wali murid dikhususkan untuk orang tua/wali murid. Berikut ini adalah tampilan menu utama :

Gambar 7 : Tampilan form menu utama

b. Tampilan *Chat Room* Wali Kelas

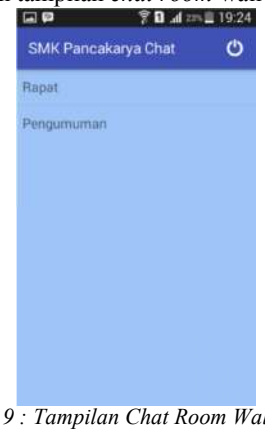
Tampilan *chat room* akan tampil, jika pada saat *login* atau registrasi wali kelas

berhasil maka akan langsung menuju ke tampilan *chat room* wali kelas. Pada tampilan ini terdapat sebuah *field* untuk memasukkan "nama *room*" dan terdapat *button* untuk membuat *room* baru. Hak akses untuk membuat *room* baru hanya terdapat pada *user level* wali kelas. Berikut ini adalah tampilan dari *chat room* wali kelas :

Gambar 8 : Tampilan Chat Room Wali Kelas

c. Tampilan *Chat Room* Wali Murid

Tampilan *chat room* wali murid adalah *chat room* yang tersedia dan telah dibuatkan oleh *user level* wali kelas. Dikarenakan *user level* wali murid tidak bisa membuat *chat room* baru, tetapi wali murid bisa melihat dan milih *chat room* sehingga muncul tampilan *chatting* untuk mengirim dan menerima pesan. Di bawah ini adalah tampilan *chat room* wali murid :



Gambar 9 : Tampilan Chat Room Wali Murid

d. Tampilan *Chatting* Wali Kelas dan Wali Murid

Tampilan *chatting* ini adalah digunakan oleh wali kelas/wali murid jika ingin mengirim dan menerima pesan. Setelah wali kelas dan wali murid memilih salah satu *chat room* maka tampilan

Gambar 10 : Tampilan Chatting Wali Kelas dan Wali Murid

4.2 Tabel Pengujian

Dalam tabel pengujian pada aplikasi ini, akan diuji mengenai waktu yang mengenai proses enkripsi, dekripsi, dan aktivitas pada aplikasi. Berikut ini adalah beberapa tabel yang memperlihatkan hasil dari pengujian tersebut :

a. Tabel Hasil Pengujian Proses di Dalam Ruangan

Berikut ini adalah hasil dari pengujian proses yang ada pada aplikasi ini. Proses-proses yang dilakukan pengujian pada lokasi *indoor* atau di dalam ruangan yang dapat dilihat sebagai berikut :

Tabel 1 : Tabel Hasil Pengujian Proses di Dalam Ruangan

No.	Proses	Jaringan	Lokasi	Waktu (Detik)		
				Proses	Enkripsi	Dekripsi
1	Daftar	Wifi	Di dalam ruangan	2	0.5	-
2	Daftar	Paket Data	Di dalam ruangan	11	0.5	-
3	Login	Wifi	Di dalam ruangan	2	0.5	-
4	Login	Paket Data	Di dalam ruangan	4	0.5	-
5	Kirim Pesan	Wifi	Di dalam ruangan	0.5	0.5	0.5
6	Kirim Pesan	Paket Data	Di dalam ruangan	0.5	0.7	0.7
7	Buat Chat Room	Wifi	Di dalam ruangan	1	-	-
8	Buat Chat Room	Paket Data	Di dalam ruangan	2	-	-

b. Tabel Pengujian di Luar Ruangan

Berikut ini adalah hasil dari pengujian proses yang ada pada aplikasi ini Proses-proses yang dilakukan pengujian pada lokasi *outdoor*

atau di luar ruangan yang dapat dilihat sebagai berikut :

Tabel 2 : Tabel Hasil Pengujian Proses di Luar Ruangan

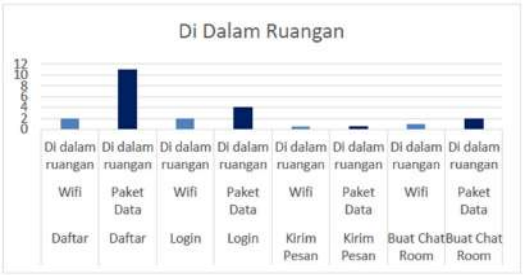
No.	Proses	Jaringan	Lokasi	Waktu (Detik)		
				Proses	Enkripsi	Dekripsi
1	Daftar	Wifi	Di Luar Ruangan	3	0.5	-
2	Daftar	Paket Data	Di Luar Ruangan	7	0.5	-
3	Login	Wifi	Di Luar Ruangan	2	0.5	-
4	Login	Paket Data	Di Luar Ruangan	3	0.5	-
5	Kirim Pesan	Wifi	Di Luar Ruangan	0.5	0.6	0.6
6	Kirim Pesan	Paket Data	Di Luar Ruangan	0.5	0.6	0.6
7	Buat Chat Room	Wifi	Di Luar Ruangan	1	-	-
8	Buat Chat Room	Paket Data	Di Luar Ruangan	2	-	-

1.3 Diagram Pengujian

Untuk mempermudah melihat hasil dari tabel pengujian dibuatlah diagram yang menampilkan hasil dari pengujian tersebut. Berikut ini adalah beberapa diagram dari hasil tabel pengujian :

a. Diagram Hasil Pengujian Proses di Dalam Ruangan

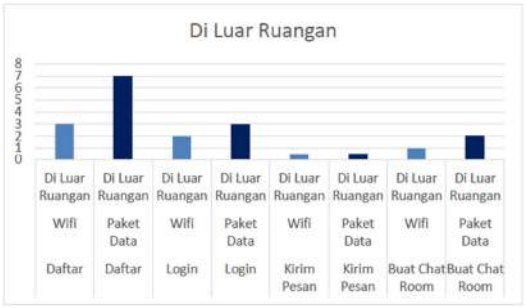
Hasil pengujian proses di dalam ruangan terdapat perbedaan waktu yaitu pada proses daftar dengan menggunakan wifi lebih cepat dibandingkan dengan menggunakan paket data, dengan *wifi* hanya butuh 2 detik sedangankan paket data butuh waktu 11 detik. Berikut ini adalah diagram dari pengujian proses di dalam ruangan yang menggunakan jaringan *wifi* dan paket data :



Gambar 11 : Diagram Hasil Pengujian Proses di Dalam Ruangan

b. Diagram Hasil Pengujian Proses di Luar Ruangan

Hasil pengujian proses di luar ruangan, juga terjadi berbedaan yaitu dengan menggunakan paket data lebih lama dibandingkan dengan *wifi* yang mempunyai waktu 3 detik sedangkan paket data 7 detik pada proses daftar. Berikut ini adalah diagram dari pengujian proses di luar ruangan yang menggunakan jaringan wifi dan paket data :



Gambar 12 : Diagram Hasil Pengujian Proses di Luar Ruangan

1.4 Evaluasi Program

Evaluasi program dimaksudkan untuk menganalisa hasil dari aplikasi yang telah dibuat yang dijabarkan dalam bentuk kelebihan dan kekurangan. Adapun kelebihan dan kekurangan tersebut dapat dilihat sebagai berikut :

a. Kelebihan Aplikasi *Chatting*
   1. Pengguna dapat menggunakan aplikasi ini, dimanapun dan kapanpun dengan menggunakan akses internet.
   2. Pengguna dapat saling mengirim dan menerima pesan, baik pesan tersebut bersifat urusan di sekolah maupun hanya komunikasi biasa.
   3. Aplikasi *chatting* ini, menggunakan Vigenere Cipher dan Affine Cipher untuk mengamankan pesan pada media penyimpanan yang digunakan yaitu *database* Firebase.

b. Kekurangan Aplikasi *Chatting*
   1. Aplikasi ini hanya dapat mengenkripsi pesan teks.
   2. Tidak adanya pengecekan *email* untuk memastikan *email* tersebut valid.
   3. Pengguna diminta *password* jika ingin mendaftar sebagai *user* wali kelas, namun *password* tersebut tidak dilakukan pengacakan kepada setiap user yang ingin mendaftar sehingga *password* tersebut dapat tersebar selain wali kelas.
   4. Tidak adanya *password* pada setiap *chat room* sehingga pengguna dapat masuk secara bebas.

5. KESIMPULAN DAN SARAN

Bedasarkan hasil analisis dari tabel pengujian, maka dapat ditarik kesimpulan dan saran yang diperlukan untuk pengembangan pada aplikasi ini menjadi lebih baik dari segala aspek.

5.1 Kesimpulan

Berdasarkan dari uraian yang telah dijabarkan pada bab-bab sebelumnya terhadap permasalahan yang ada dan menyelesaikan permasalahan tersebut, maka dapat disimpulkan sebagai berikut :

a. Aplikasi ini dapat mengirim dan menerima pesan yang dapat dilakukan oleh orang tua/wali murid maupun wali kelas secara langsung.
b. Pengamanan pada aplikasi ini, menggunakan 2 (dua) metode kriptografi yaitu, Vigenere Cipher dan Affine Cipher yang dapat mengamankan pesan/informasi.
c. Dengan menggunakan algoritma kriptografi Vigenere Cipher dan Affine Cipher secara otomatis dapat mengekripsi dan mendekripsi pesan tersebut.
d. Pada Vigenere Cipher menggunakan kunci yang telah ditentukan untuk proses enkripsi dilanjutkan dengan enkripsi Affine Cipher yang menggunakan dua kunci yang telah ditentukan. Untuk mendekripsi menggunakan Affine Cipher dengan kunci yang sama pada proses enkripsi, kemudian dekripsi dengan menggunakan Vigenere Cipher dengan kunci yang sama pada proses enkripsi.
e. Pada aplikasi ini, *user level* wali kelas dapat membuat *chat room* yang berguna untuk memfokuskan topik pembicaraan berdasarkan dengan nama *chat room* yang dibuat.
f. Pada aplikasi *chatting* ini, mempunyai keberhasilan sebesar 100% dapat mengenkripsi dan mendekripsi pesan yang dikirim oleh pengguna.
g. Hasil dari pengujian proses pada aplikasi *chatting* ini, dengan menggunakan *wifi* lebih cepat dibandingkan dengan menggunakan paket data pada lokasi di dalam ruangan maupun di luar ruangan.
h. Waktu yang diperlukan untuk proses enkripsi dan dekripsi cukup cepat.

5.2 Saran

Selain kesimpulan, terdapat juga saran-saran dapat dijadikan bahan pertimbangan dalam pengembangan aplikasi agar menjadi lebih baik lagi, antara lain sebagai berikut :

a. Format yang dapat diamankan tidak hanya teks, tetapi dapat mengamankan berupa gambar, file, video dan audio.
b. Menambahkan *personal chat* supaya antara pengguna wali kelas ataupun wali murid dapat berkomunikasi lebih pribadi.
c. Penerapan validasi pada *email*.
d. Seharusnya menerapkan *password* pada setiap *chat room* yang dibuat oleh wali kelas agar isi *chat room* lebih bersifat pribadi dari orang-orang yang tidak berkepentingan.

DAFTAR PUSTAKA

[1] Agung, H., dan Budiman, 2015. Implementasi Affine Cipher dan RC4 Pada Enkripsi File Tunggal. *Prosiding SNATIF*, hal. 243-250.

[2] Anwar, S., Nugroho, I., dan Ahmadi, A., 2015. Implementasi Kriptografi Dengan Enkripsi Shift Vigenere Cipher Serta Checksum Menggunakan CRC32 Pada Data Text. *Jurnal Sistem Informasi*, vol. 2, hal. 51-58.

[3] Efrandi, Asnawati, dan Yupiyanti, 2014. Aplikasi Kriptografi Pesan Menggunakan Algoritma Vigenere Cipher. *Jurnal Media Infotama*, vol. 10, no. 2, hal. 120-128.

[4] Nugroho, S., P., dan Aribowo, E., 2014. Pengembangan Modul Enkripsi Dan Dekripsi Pada PHP Dengan Modifikasi Metode Kriptografi Vigenere Cipher Dan Cipher Block Chaining (Studi Kasus Pada geekybyte.com). *Jurnal Sarjana Teknik Informatika*, vol. 2, no. 1, hal. 1004-1012.

[5] Yulianingsih, P., Hamdani, dan Maharani, S., 2014. Aplikasi Chatting Rahasia Menggunakan Algoritma Vigenere Cipher. *INFORMATIKA Mulawarman*, vol. 9, no. 1, hal. 19-22.