IMPLEMENTASI METODE BLOWFISH, *RC6*, DAN AFFINE CIPHER PADA APLIKASI *CHATTING* BERBASIS *ANDROID*

Muhammad Fahri Ramadhan[1)], Purwanto[2)]
[1]Program studi, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Jakarta Selatan 12260
E-mail : fahriramadh4n@gmail.com[1)], purwanto@budiluhur.ac.id[2)]

ABSTRAK

Berkomunikasi menjadi hal yang penting bagi setiap individu dalam melakukan sosialisasi. Setiap individu berkomunikasi dengan teknologi canggih tanpa mengenal waktu dan tempat, salah satunya itu dengan menggunakan Instant Messenger. Penggunaan Instant Messenger dapat dilakukan untuk berkomunikasi dengan mengirimkan pesan teks langsung dengan orang yang berada pada list kontak kita. Pejabat Pembuat Akta Tanah dan Notaris, pejabat umum yang memiliki kewenangan atas pembuatan pada akta otentik tentang hukum yang ditentukan hak atas tanah dan rumah. Komunikasi bagi Pejabat Pembuat Akta Tanah sangat penting dikarenakan sifat nya yang rahasia oleh karena itu diperlukannya aplikasi chatting yang cepat,aman,dan sifat nya realtime.Cara untuk mengamankan sebuah data yang sifat nya rahasia yaitu dengan metode kriptografi. Kriptografi adalah penerapan matematika dan logika kompleks untuk merancang proses enkripsi dan dekripsinya. Untuk mengamankan percakapan antara notaris dan client dibuatlah aplikasi chatting yang menggunakan metode kriptografi. Dalam penulisan penelitian ini penulis akan menggunakan metode Kriptografi dengan Algoritma Blowfish,RC6 untuk mengenkrip pesan text dan metode kriptografi algoritma Affine Cipher pesan lampiran gambar berupa URL. Dengan menggunakan ketiga metode tersebut diharapkan percakapan antara notaris dan client tidak dapat disadap oleh pihak yang tidak bertanggung jawab dan terhindar dari manipulasi data yang menyebabkan kerugian bagi pihak notaris dan pihak client.

Kata kunci : *Instant Messenger*, Kriptografi, *Blowfish, RC6, Affine Cipher*

1. PENDAHULUAN

1.1. Latar Belakang

Berkomunikasi menjadi hal yang penting bagi setiap individu dalam melakukan sosialisasi. Setiap individu berkomunikasi dengan teknologi canggih tanpa mengenal waktu dan tempat, salah satunya itu dengan menggunakan i*nstant messenger*. Penggunaan *instant messenger* dapat dilakukan untuk berkomunikasi dengan mengirimkan pesan teks langsung dengan orang yang berada pada list kontak kita. Pejabat Pembuat Akta Tanah dan Notaris pejabat umum yang memiliki kewenangan atas pembuatan pada akta otentik tentang hukum yang ditentukan hak atas tanah dan rumah. Komunikasi bagi Pejabat Pembuat Akta Tanah sangat penting dikarenakan sifat nya yang rahasia oleh karena itu diperlukannya aplikasi *chatting* yang cepat,aman,dan sifat nya realtime. Cara untuk mengamankan sebuah data yang sifat nya rahasia yaitu dengan metode kriptografi. Kriptografi adalah ilmu yang menerapkan matematika dan logika kompleks untuk merancang proses enkripsi dan dekripsinya. Setiap saat teknik yang digunakan untuk memecahkan *ciphertext* juga berkembang dengan pesat. Dengan ini, adalah sangat dibutuhkan teknik-teknik yang mendukung kekuatan untuk memperkuat keamanan dari *ciphertext*. Untuk mengamankan percakapan antara notaris dan client dibuatlah aplikasi *chatting* yang menggunakan metode kriptografi. Dalam penulisan penelitian ini penulis akan menggunakan metode kriptografi dengan Algoritma Blowfish, RC6 untuk mengenkrip pesan text dan metode kriptografi algoritma Affine Cipher pesan lampiran gambar berupa *URL*. Dengan menggunakan ketiga metode tersebut diharapkan percakapan antara notaris dan client nya tidak dapat disadap oleh pihak yang tidak bertanggung jawab dan juga terhindar dari manipulasi data yang dapat menyebabkan kerugian bagi pihak notaris dan pihak client.

1.2. Permasalahan

Berdasarkan latar belakang diatas maka dapat ditarik kesimpulan permasalahan yang dimiliki pada notaris adalah bagaimana cara agar pesan asli dan lampiran berupa gambar yang terenkripsi dan diamankan tidak akan mengubah isi dari pesan.

1.3. Tujuan Penulisan

Penelitian ini memiliki maksud dan tujuan untuk mengamankan pesan teks. Aplikasi *chatting* dibuat agar mencapai komunikasi menjadi aman dan memudahkan penggunaan antara notaris dan *client*. Dengan digunakanya metode algoritma enkripsi Blowfish dan RC6 digunakan untuk mengamankan pesan teks, sedangkan pada pengamanan *URL* gambar menggunakan metode algoritma Affine Cipher.

2.METODE PENELITIAN

Pembuatan pada sistem ini menggunakan metode *waterfall* pada implementasinya agar proses bisa mudah dilakukan dan dibuat :

1) Melakukan tahapan *requirment* pada tepat riset untuk mengetahui apa yang dibutuhkan pada penelitian ini, mengetahui apa yang harus diamankan pada notaris tersebut, serta mengetahui algoritma yang cocok untuk di gunakan dalam enkripsi aplikasi *chatting.*
2) Setelah melakukan tahapan riset serta mencari metode yang cocok, selanjutnya menganalisa dari kebutuhan sistem yang akan dikembangkan.
3) Apabila kita telah selesai dalam tahapan analisa dan mengetahui akan kebutuhan sistem, maka dilanjutkan kepada tahapan desain sistem yang akan dibuat, *database* yang akan digunakan secara *realtime,* rancangan layar yang akan dibuat untuk memudahkan pada tahap pengkodingan.
4) Tahap keempat, apabila kita telah selesai membuat desain, database yang akan digunakan, dan rancanganya, bisa dilanjutkan pada tahap pengkodingan. Dalam tahap ini pengkodingan bahasa yang digunakan menggunakan java dengan *platform* berbasis Android, untuk penggunaan metode algoritma menggunakan tiga algoritma diantaranya : Blowfish, RC6, Affine Cipher pada implementasi kriptografi di aplikasinya, serta database *realtime* nya menggunakan *firebase console*.
5) Apabila semua tahapan telah terpenuhi dan dalam proses pengkodingan telah selesai, maka dilanjutkan dengan implementasi dan uji coba pada sistem pada aplikasi yang telah dibuat. Melalui tahapan ini apakah telah memenuhi kebutuhan dan masih adakah kekurangan dalam proses pada aplikasinya, agar aplikasinya bisa di implementasi dan digunakan secara langsung.

3. HASIL DAN PEMBAHASAN

3.1. Analisa Masalah

Informasi perpesanan menjadi sebuah hal yang sangat penting pada notaris dan PPAT Pejabat Pembuat Akta Tanah oleh karena itu pesan yang terkandung bersifat penting dan diharapkan rahasia pesan tidak akan diketahui oleh pihak yang tidak bersangkutan. Pengacara dan pelanggan melakukan pertukaran informasi menggunakan media aplikasi *chatting.* Penggunaan pada aplikasi *chatting* itu sudah sangat populer setiap orang pasti menggunakan nya sebagai media pertukaran informasi teks dan khusunya pada instansi seperti notaris dan PPAT.

Aplikasi *chatting* yang sering digunakan pada saat ini mempunyai banyak kegunaan, namun pada isi pesan aplikasi *chatting* belum diadakan nya pengamanan pada pesan. Sebab dari permasalah tersebut jika *server* pada aplikasi diretas, seluruh informasi pesan yang terdapat pada aplikasi *chatting* akan mudah terbaca dan tercuri oleh pihak yang tidak berkepentingan atau *cracker*.

3.2. Penyelesaian Masalah

Dalam mengatasi permasalahan yang telah diuraikan di atas, dibuatlah aplikasi *chatting* yang diadakannya fitur keamanan pada pesan teks . Dalam pembuatan aplikasi *chatting* tersebut, menggunakan metode kriptografi. Dalam metode kriptografi proses yang umum dilakukan yaitu enkripsi dan dekripsi. Enkripsi memiliki fungsi untuk mengubah pesan teks biasa (*plaintext*) yang di manipulasi menjadi *ciphertext* atau teks acak yang tidak bisa terbaca. Proses dekripsi memiliki fungsi untuk mengembalikan *ciphertext* langsung menjadi *plaintext* seperti semula. Dalam penerapan kriptografi pada aplikasi *chatting* ini, diharapkan pihak yang tidak bertanggung jawab tidak memiliki kesempatan untuk mendapatkan informasi pada pesan yang telah dikirimkan dari aplikasi *chatting* ini. Semua akun *user* dan isi pesan atau percakapan yang terenkripsi pada penerima dan pengirim akan disimpan melalui *firebase console* .

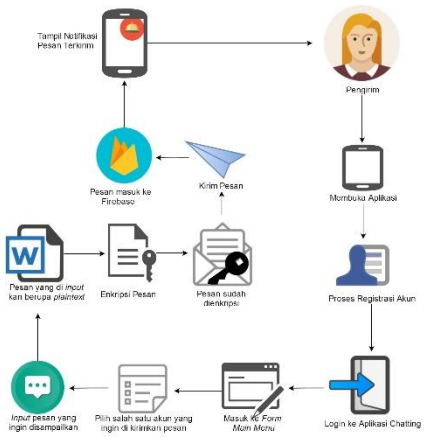
Pengunaan algoritma pada aplikasi ini menggunakan tiga metode diantaranya adalah algoritma Blowfish, RC6, dan Affine Cipher. Ketiga algoritma ini memiliki sifat simetris, yang pada implementasi nya menggunakan kunci yang sama saat proses enkripsi dan dekripsi. Penggunaan untuk mengamankan pada pesan berupa teks menggunakan dua algoritma Blowfish dan RC6, sedangkan untuk mengamankan pesan berupa link pada gambar digunakan algoritma Affine Cipher.

3.3. Skema Proses Keseluruhan Aplikasi

Dalam penyelesaian masalah di atas, dibuatlah proses skema pada semua aplikasi. Berikut ini adalah tahapan pesan pengirim :

1) Pengirim diharuskan meng-*install* lalu mebuka aplikasi *chatting* yang terinstall pada perangkat android .
2) Jika pengirim belum memiliki akun, maka pengirim di haruskan melalukan *register* terlebih dahulu pada aplikasi. Pengirim diharuskan mengisi data berupa *email, password, dan repeat password*.
3) Bila pengirim sudah terdaftar dan menjadi *user*, pengirim dapat langsung melaksanakan proses *login* dengan menggunakan *email* dan *password* dan sudah terdaftar pada *server firebase console* dan terhubung pada *internet*.
4) Apabila sudah *login* dan masuk. Lalu pengirim akan masuk ke *form* utama dan pilihlah salah satu akun yang ingin dikirimkan dilanjut dengan proses pengiriman pesan enkripsi, aplikasi pengirim akan masuk ke *form chat*.
5) Setelah itu pengirim dapat meng-*input* pesan kepada penerima yang dipilih.
6) Proeses dari pengiriman pesan akan melalui proses enkripsi.
7) Pada pesan teks yang di-*input* kan akan menjadi *ciphertext* dan kunci nya akan diatur oleh sistem.

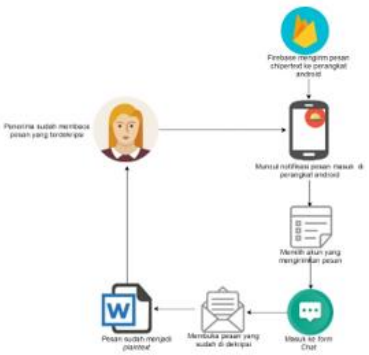
8) Bila proses pada enkripsi telah selesai, pesan akan diteruskan ke *Firebase Console* dan dilanjutkan kepada akun penerima pesan lalu ditampilkan pada penerima.
9) Notifikasi akan diberikan kepada pengirim untuk memastikan apakah pesan terkirim atau tidak.
10) Pada *ciphertext* yang dikirim kepada penerima akan terdekripsi secara otomatis pada sistem.



Gambar 1 Proses Saat Pengiriman Pesan

Setelah proses pengiriman, berikut dijelasakan proses penerimaan pesan :

1) Notifikasi berupa pesan masuk akan diterima oleh penerima yang dikirim.
2) Penerima bisa memilih akun yang mengirimkan pesan yang telah ditampilkan pada *form main* dan membaca isi pesannya . Lalu otomatis penerima masuk pada *form chat*.
3) Maka pesan yang diacak tidak ditampilkan pada *form chat* penerima. Namun *Chipertext* sendiri disimpan pada *Firebase Console*.
4) *Ciphertext* akan melalui proses dekripsi pesan.
5) *Ciphertext* yang melalui proses dekripsi akan dirubah menjadi teks biasa.
6) *Plaintext* yang akan ditampilkan pada *form chat* adalah pesan asli atau murni dari pengirim pesan tanpa merubah isi asli pesan.



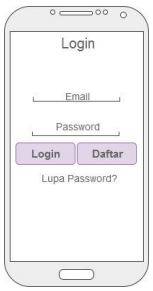
Gambar 2 proses pada penerimaan pesan

3.4 Rancangan Layar

Rancangan layar sangat diperlukan dalam membuat sebuah program. Oleh karena itu rancangan layar harus mudah di mengerti oleh *user* sehingga *user* tidak akan mengalami kesulitan dalam menggunakan aplikasi. Pada aplikasi yang dibuat akan digambarkan meliputi *form register, form login, main menu dan form chat.* Selain itu terdapat from akun untuk mensetting foto profil anda agar mudah dikenali. *Menu form about* dan *help* yang terdapat pada *dropdown menu*. Berikut rancangan layar pada masing-masing *form* :

a. Rancangan Layar Pada *Form Login*

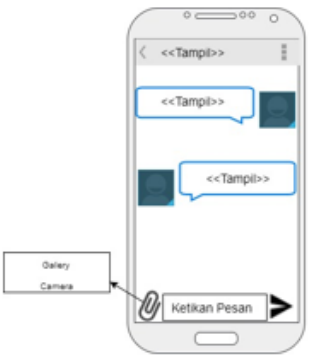
Form login adalah hal yang pertama kali muncul pada aplikasi *chatting* ini bila belum memiliki akun maka harus mendaftar terlebih dahulu dengan memilih *button* daftar, tetapi apabila sudah memiliki akun maka hanya megisi email dan *password* lalu *button login* .



Gambar 3 Rancangan *Form Login*

b. Rancangan Layar *Form Chat*

Form chat adalah *form* yang digunakan dalam melalukan aktivitas *chatting* dengan *user* lain yang sudah terdaftar dan dipilih melalui *form main menu.* Percakapan pada pesan akan di enkripsi dengan menggunakan metode Blowfish dan RC6, sedangkan bila pengirim ingin mengirim pesan berupa *link* gambar, maka pesan tersebut akan di enkripsi menggunakan metode Blowfish. Pada pesan selama pengiriman akan aman karena telah melaui proses enkripsi. Pesan yang masuk ke perangkat android akan langsung terdekripsi otomatis tanpa user repot-repot dalam memasukan kunci.



Gambar 4 Rancangan *Form Chat*

c. Rancangan Layar *Form* Akun

Form akun merupakan *form* yang memiliki fitur untuk mengganti foto *profil* mengganti nama pengguna, ubah *password*, dan keluar aplikasi, *form akun akan* tampil apabila mengklik *fragment* akun anda pada *fragment main menu* .

Gambar 5 Rancangan *Form* Akun

3.5 *Flowchart* Program

Pada *form chat*, pengguna bisa mengirimkan pesan teks ke *user* yang sudah dituju dari *Form Main Menu*. Pesan yang dikirimkan selalu melewati proses enkripsi dan pesan yang diterima selalu melewati proses dekripsi

Gambar 6 *Flowchart Form Chat*

3.6 Algoritma Alur Proses

Pada algoritma ini menjelaskan bagaimana terjadi nya *form chat*.

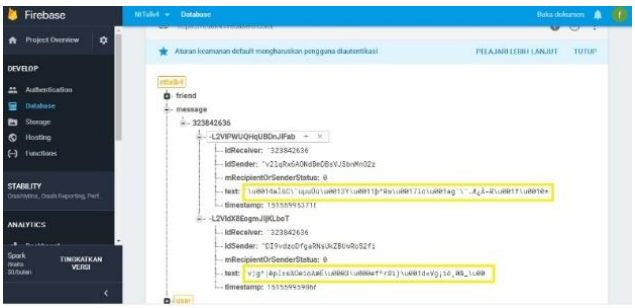
1. Buka Tampilan Form Chat
2. Tampilkan semua Teks pada pesan Pengirim dan Penerima
3. Input PesanText
4. If Pilih = Kirim then
5. If pesan terdapat “teks” then
6. Enkrip dengan Blowfish
7. Enkrip dengan RC6
8. Kirim ke Firebase Console
9. End If
10. Else if Pesan terdapat “Gambar” then
11. Enkrip dengan Affine Cipher
12. Kirim Ke Firebase Console
13. End if
14. Tampilkan laporan pengiriman “Pesan Terkirim”
15. Pesan di lanjutkan ke Penerima
16. else
17. Kembali ke baris 1
18. EndIf

3.7. Tampilan Layar

Tampilan layar selalu menjadi aspek yang penting bagi pengguna untuk bisa memahami dalam menjalankan suatu program dan juga agar pengguna merasa nyaman dalam penggunaanya.

a. Tampilan Layar *Database Firebase Console*

Pesan yang telah dikirimkan akan dikirimkan melalui database dengan menggunkan *firebase console*. Dapat di lihat pada gambar 7



Gambar 7 Tampilan Pada *Firebase Console* dikirim dan terenkripsi otomatis

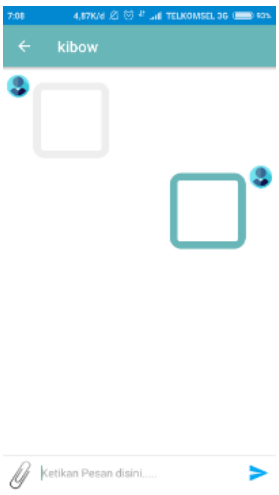
b. Tampilan Layar Pesan Terenkripsi

Pesan yang dikirimkan akan melalui proses enkripsi, pesan yang terenkripsi tersebut akan diambil melalui *firebase console* dan pada *form main menu* di penerima pesan akan tampil pesan terenkripsi sebelum di buka pesan tersebut, Dapat dilihat pada gambar 8

Gambar 8 Tampilan layar pesan terenkripsi

c. Tampilan Layar Pesan Terenkripsi

Apabila pengguna mengirimkan pesan berupa gambar, maka tampilan gambar pada *form chat* hanya berupa *blank message* karena *link* gambar masih terenkripsi. Pengguna hanya perlu mengklik gambar untu bisa melihat gambar tersebut, Dapat dilihat pada gambar 9



Gambar 9 Tampilan layar *link* gambar terenkripsi

3.8 Evaluasi Hasil Uji Coba Program

Setelah proses perangkat keras dan perangkat lunak terpenuhi, penulis telah mencoba uji coba program. Mengetahui hasil dari uji coba pada program adalah hal penting guna mengevaluasi aplikasi yang terlah dicapai tersebut. Adapaun dari hasil uji coba tersebut penulis menemukan beberapa batasan-batasan dari masalah, diantaranya adalah :

Kelebihan Pada Program

1) Pada aplikasi *chatting* ini hanya memiliki besar *memory* 6MB.
2) Pada aplikasi *chatting* memiliki fitur pengiriman pesan secara *realtime*.
3) Database pada aplikasi ini menggunakan *firebase*.
4) Pada chatting sendiri dapat mengirimkan pesan teks dan gambar.
5) Apabila sedang membuka aplikasi lain, aplikasi ini bisa mengirimkan pesan notifikasi.
6) Pada aplikasi chatting ini setiap pesan yang dikrimkan akan terenkripsi pada 2 algoritma, 1 algoritma untuk *link* pada gambar .
7) Sistem aplikasi ini sudah menyiapkan *key* pada sistem untuk proses enkripsi nya .

Kelemahan Pada Program

1) Pada Aplikasi *chatting* ini tidak di berikan nya fungsi untuk *group chat* dan *broadcast message*.
2) Fitur pada aplikasi chatting ini sendiri belum memiliki fitur diantaranya pesan suara, dokumen, dan maps.
3) Aplikasi ini tidak dapat dijalankan pada system operasi Android di bawah versi 5.0 *Lolipop*.
4) Aplikasi ini tidak bisa melakukan percakapan baik melalui panggilan telepon ataupun *video call*.

4. KESIMPULAN

Melalui analisa permasalahan dan penyelesaian yang dapat disimpulkan pada aplikasi *chatting* dengan metode *Blowfish*, Rivest Code 6(RC6) untuk mengenkripsi pesan teks dan untuk mengkripsi link pada gambar dengan metode Affine Cipher berbasis *Android* pada Notaris dibutuhkan diantaranya karena:

a. Karena adanya aplikasi ini pesan teks maupun gambar dapat terjaga kerahasiaanya.
b. Pengamanan pada pesan sendiri cukup terjaga, pesan pada saat pengiriman pun tidak rusak dan pada saat dikembalikan sesuai dengan apa yang dikirim.
c. Aplikasi nya memiliki ruang memory yang ringan hanya 6 MB.

Karena waktu yang diberikan tidak banyak dalam menyelesaikan penelitian ini, penyelesaian masalahnya pun masih jauh dari pada sempurna, maka dari itu perlu dikembangkan dari sisi *software* maupun *hardware* nya. Untuk saran pada pengembangannya antara lain:

a. Dapat Ditambahkan fitur yang melengkapi aplikasi ini untuk kirim *file*, penarikan pada pesan , *voice call*, dan *map.*
b. Dapat dilakukan update berkala untuk versi android terupdate.
c. autentifikasi melalui alamat *email* untuk setiap pengguna yang masuk dapat di cek pada *system*.

5. DAFTAR PUSTAKA

[1]. Riadi, M., 2017. *kajianpustaka.com.* [Online] Available at: <http://www.kajianpustaka.com/2014/01/pengertian-sejarah-dan-jenis kriptografi.html> [Accessed 5 November 2017].

[2]. Wardoyo, S., Imanullah, Z. & Fahrizal, R., 2016. Enkripsi Dan Dekripsi File Dengan Algoritma Blowfish Pada Perangkat Mobile Berbasis Android. *Jurnal Nasional Teknik Elektro*, 5(1), pp. 37-44.

[3]. Rahmayun, I. & Defni, 2014. enkripsi sms (short message service) pada telepon selular berbasis android dengan metode RC6. *Jurnal Momentum*, 16(1), pp. 1-11.

[4]. Wibowo, S., Nilawati, F. E. & Suharnawi, 2014. Implementasi Enkripsi Dekripsi Algoritma Affine Cipher Berbasis Android. *Techno.COM*, 13(4), pp. 215-221.

[5]. Gea, F., 2016. Perancangan Aplikasi Enkripsi Pesan Singkat Dengan Menggunakan Algoritma Affine Cipher Dan Vigenere Cipher Berbasis Android. *Jurnal INFOTEK*, 1(3), pp. 30-39.

[6]. Hariady, M. M., Suyatno, A. & Astuti, I. F., 2016 . Keamanan Dan Penyisipan Pesan Rahasia Pada Gambar Dengan Enkripsi Blowfish Dan Steganografi End Of File. *Jurnal Informatika Mulawarman*, 11(2), pp. 1-10.

[7]. Musfiroh, A., 2017. *masktekno.* [Online] Available at: https://www.mastekno.com/id/pengertian-tujuan-dan-jenis-jenis-kriptografi-rumus-penyelesaian/ [Accessed 1 November 2017].