PENGAMANAN APLIKASI CHATTING PADA PERANGKAT ANDROID MENGGUNAKAN KRIPTOGRAFI DENGAN METODE ADVANCED ENCRYPTION STANDARD (AES) 128 PADA PT. SALAM MEDINA INDONESIA

Wahyu Krishna Hadi[1)], Sri Mulyati M.Kom[2)]
[1,2]Program studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
Telp.(021) 5853753 ext.303, Fax. 5853489
E-mail : wahyukrishna.tkj1@gmail.com[1)], sri.mulyati@budiluhur.ac.id[2)]

Abstract

Perkembangan teknologi informasi khususnya perangkat Android saat ini sangat pesat terutama dalam masalah komunikasi. Informasi penting dikirimkan setiap harinya lewat berbagai jenis media, contohnya aplikasi chatting. Seiring dengan banyaknya aplikasi chatting, kejahatan cybercrime seperti penyadapan dan manipulasi pesan juga banyak terjadi karena tidak adanya sistem keamanan untuk melindungi pesan. Hal tersebut dikhawatirkan oleh staf karyawan dan customer PT. Salam Medina Indonesia sebagai pengguna aktif aplikasi chatting. Para staf dan customer bertukar data dan informasi rahasia tanpa adanya jaminan keamanan pesan pada aplikasi chatting yang digunakan selama ini. Pada penelitian ini akan dibuat sebuah aplikasi chatting yang menggunakan kriptografi Advanced Encryption Standard(AES) untuk mengamankan pesan yang dikirim. Pesan yang awalnya berupa teks biasa(plaintext), melalui proses enkripsi menjadi teks acak yang tak bisa dibaca(chipertext). Pesan hanya dapat dibaca melalui proses dekripsi pada aplikasi chatting ini sehingga kerahasiaan pesan tetap terjaga. Dengan adanya kriptogragi AES yang diimplementasikan pada aplikasi chatting ini, pengguna khususnya staf karyawan dan customer PT. Salam Medina Indonesia dapat mengirim pesan dengan aman tanpa khawatir pesan disadap atau dimanipulasi oleh pihak yang tidak bertanggung jawab.

***Kata kunci** : Android, Aplikasi Chatting, Kriptografi, AES*

Abstrak

The development of information technology especially Android devices is currently very rapid, especially in communication problems. Important information is sent every day through various types of media, for example chat applications. Along with the many chat applications, cybercrime crimes such as wiretapping and messaging manipulation also occur due to the lack of a security system to protect messages. It is feared by staff employees and customers of PT. Salam Medina Indonesia as an active user of chat application. Staff and customers exchange confidential data and information without any guarantee of message security on the chat apps used so far. In this research will be made a chat application that uses Advanced Encryption Standard cryptography (AES) to secure messages sent. Messages that were originally plain text (plaintext), through the encryption process into random text that can not be read (chipertext). Messages can only be read through the decryption process in this chat application so that the confidentiality of the message is maintained. With the existence of AES cryptography which is implemented in this chat application, user especially staff of employees and customer PT. Regards Medina Indonesia can send messages safely without worry of messages being tapped or manipulated by irresponsible parties.

Keywords: Android, Chatting Application, Cryptography, AES

1. PENDAHULUAN

Pengiriman pesan melalui internet dengan menggunakan aplikasi chatting merupakan salah satu metode komunikasi yang bersifat real-time. Selama ini aplikasi tersebut belum bisa menjamin privasi diantara pengirim dan penerima pesan, karena data yang dikirim berupa pesan langsung dan dapat langsung dibaca (plaintext).

Aplikasi *chatting* dilakukan dengan melakukan transaksi paket antara *client* dengan *server*. Penggunaan teknologi ini memiliki suatu kelebihan dibandingkan surat elektronik (*email*), yaitu komunikasi dapat terjalin secara langsung

dan lebih cepat. Hal tersebut merupakan salah satu penyebab pertumbuhan pada jumlah penggunaan pengirim pesan instan untuk berkomunikasi.

PT. Salam Medina Indonesia merupakan salah satu lembaga di bidang pelayanan Tour dan Travel yang cukup aktif dalam menggunakan aplikasi chatting untuk berkomunikasi, baik dengan konsumen maupun sesama karyawan. Aplikasi chatting sebagai sarana pengiriman pesan yang meningkat telah menimbulkan kekhawatiran mengenai keamanannya, khususnya bagi PT. Salam Medina Indonesia. Teks pesan yang dikirim melalui pengirim pesan dapat diganggu oleh pihak-pihak yang ingin tahu tentang isi percakapan tersebut dengan mudah karena tidak melalui proses pengamanan dalam perjalanannya. Untuk mengatasi ancaman-ancaman tersebut, diperlukanlah suatu cara agar teks pesan dalam aplikasi chatting tersebut tidak dapat diketahui oleh pihak lain. Salah satu caranya adalah dengan menggunakan kriptografi. Kriptografi sudah dikenal sejak ribuan tahun yang lalu. Kriptografi terus-menerus dikembangkan hingga saat ini. Pengembangannya dilakukan oleh berbagai pihak dari berbagai negara. Karena banyaknya jumlah algoritma yang digunakan, diperlukanlah standar algoritma sehingga dapat dipergunakan dalam berbagai aplikasi. Dengan demikian, teknik Kriptografi cukup membantu dalam pengamanan aplikasi chatting, karena semua teks pesan yang dikirimkan akan disamarkan sehingga orang akan sulit untuk membaca teks pesan yang terenkripsi tersebut. Salah satu metode yang dapat digunakan untuk mengimplementasikan teknik kriptografi adalah metode Advanced Encryption Standard (AES) 128.

Dengan melihat latar belakang diatas maka dapat diambil kesimpulan beberapa pokok permasalahan yang dimiliki oleh PT. Salam Medina Indonesia. Yaitu bagaimana membuat sebuah pengamanan untuk aplikasi *chatting* yang bersifat rahasia agar tidak dicuri oleh orang yang tidak bertanggung jawab. Pengamanan tersebut dibutuhkan karena isi percakapan dalam aplikasi *chatting* tersebut berisikan percakapan internal karyawan maupun konsumen PT. Salam Medina Indonesia.

Adapun maksud dan tujuan penelitian ini adalah sebagai berikut:

- Mengimplementasikan algoritma Advanced Encryption Standard (AES) 128 bit pada aplikasi *chatting* dan kerahasiaan isi percakapan dapat terlindungi dengan baik.
- Mengubah isi percakapan menjadi kode-kode yang sulit di mengerti.

Dalam penulisan Penelitian ini, beberapa metode digunakan untuk memperoleh informasi yang diperlukan dan menyelesaikan masalah yang ditemui. Adapun metode-metode itu sebagai berikut :

- Studi Literatur
  Melalui studi literatur diperoleh data atau informasi dengan mengumpulkan, mempelajari dan membaca berbagai referensi baik itu dari buku, jurnal, makalah, dan *internet* mengenai algortima *Advanced Encryption Standard* (AES) 128, konsep matematis yang mendasarinya, dan beberapa referensi lainnya.
- Analisa Data
  Metode ini digunakan untuk menganalisa algortima *Advanced Encryption Standard* (AES) 128.
- Perancangan Sistem
  Metode ini dilakukan dengan cara merancang sistem aplikasi yang akan dibangun dan mengimplementasikan langsung algortima *Advanced Encryption Standard* (AES) 128 ke dalam sebuah aplikasi berbasis Android.
- Pengujian Sistem
  Metode ini dilakukan dengan menguji dan mengecek jalannya program yang telah dirancang serta menyimpulkan hasil dari pengujian.

2. LANDASAN TEORI

2.1 Kriptografi

Kriptografi berasal dari bahasa Yunani, yaitu Kryptos (tersembunyi, rahasia) dan Graphein (tulisan). Jadi kriptografi didefenisikan sebagai ilmu seni untuk menjaga kerahasiaan pesan dengan cara menyandikan ke bentuk yang tidak dapat dimengerti.[1]

Kriptografi merupakan bidang pengetahuan yang menggunakan persamaan matematis untuk melakukan proses enkripsi (encrypt) maupun dekripsi (decrypt) pesan. Teknik ini digunakan untuk mengubah pesan kedalam kode-kode tertentu sehingga informasi yang disimpan atau ditransmisikan melalui jaringan yang tidak aman (misalnya saja internet) tidak dapat dibaca oleh pihak manapun kecuali orang-orang yang berhak. Algoritma dari enkripsi adalah fungsi-fungsi yang digunakan untuk melakukan fungsi enkripsi dan dekripsi. Algoritma yang digunakan menentukan kekuatan dari enkripsi, dan ini biasanya dibuktikan dengan basis matematika. Berdasarkan cara memproses teks (plaintext), cipher dapat dikategorikan menjadi dua jenis:[1]

Blok cipher dan stream cipher. Blok cipher bekerja dengan memproses data secara blok, dimana beberapa karakter/data digabungkan menjadi satu blok. Setiap proses satu blok menghasilkan keluaran satu blok juga. Sementara

itu stream cipher bekerja memproses masukan (karakter atau data) secara terus menerus dan menghasilkan data pada saat yang bersamaan.[1]

2.2 Algoritma AES

AES atau Advanced Encryption Standard merupakan standar enkripsi kunci simetri yang pada awalnya diterbitkan dengan algoritma Rijndael. Algoritma ini dikembangkan oleh dua kriptografer Belgia, Joan Daemen dan Vincent Rijmen. Advanced Encryption Standard (AES) dipublikasikan oleh NIST (National Institute of Standard and Technology) pada tahun 2001. AES merupakan blok kode simetris untuk menggantikan DES (Data Encryption Standard). Algoritma AES merupakan algoritma simetris yaitu menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Algoritma AES memiliki tiga pilihan kunci yaitu tipe : AES-128, AES-192, dan AES-256. Masing-masing tipe menggunakan kunci internal yang berbeda yaitu round key untuk setiap putaran.[1]

AES mendukung panjang kunci 128 bit sampai 256 bit. Panjang kunci dan ukuran Blok dapat dipilih secara independen dan setiap blok dienkripsi sejumlah putaran tertentu.[2]

AES mempunyai panjang kunci paling sedikit 128 bit, maka AES tahan terhadap serangan exhaustive key search dengan teknologi saat ini. Dengan panjang kunci 128 bit, maka terdapat sebanyak: 2128 = 3,4 × 1038 kemungkinan kunci. Jadi Jika digunakan komputer tercepat yang dapat mencoba 1 juta kunci setiap detik, maka akan dibutuhkan waktu 5,4 × 1024 tahun untuk mencoba seluruh kemungkinan kunci. Jika digunakan komputer tercepat yang dapat mencoba 1 juta kunci setiap milidetik, maka akan dibutuhkan waktu 5,4 × 1018 tahun untuk mencoba seluruh kemungkinan kunci.[2]

2.3 Chatting

Chatting adalah teknologi dalam sebuah jaringan untuk mengirim dan menerima pesan ke pengguna lain yang tersambung dalam suatu jaringan LAN atau internet.[3]

Setelah penggunaan email yang mengubah cara orang berkomunikasi dari cara konvensional untuk mengirimkan surat, teknologi pengiriman pesan singkat (instant messaging) diciptakan untuk menutupi kelemahan email yang kadang-kadang kurang cepat dan tidak waktu nyata (real-time).[3]

Sekarang banyak aplikasi chatting yang bermunculan dari berbasis web, desktop maupun mobile. Chatting bukan lagi hal yang diminati, melainkan bagian dari kebutuhan sosial manusia. Kebutuhan itu sendiri membuat kita mudah dalam melakukan komunikasi baik jauh maupun dekat.[3]

3. RANCANGAN SISTEM DAN APLIKASI

3.1 Analisa Masalah

Informasi berupa pesan menjadi sesuatu yang pokok pada PT. Salam Medina Indonesia. Ditambah lagi pesan tersebut bersifat penting atau rahasia yang tidak boleh diketahui oleh sembarang orang. Tidak jarang staf karyawan maupun customer PT. Salam Medina Indonesia melakukan pertukaran informasi menggunakan media yang praktis dan user friendly, media tersebut adalah aplikasi chatting. Aplikasi chatting merupakan media pertukaran informasi berupa pesan teks yang paling banyak digunakan oleh individu maupun pada suatu instansi seperti PT. Salam Medina Indonesia.

Beberapa aplikasi chatting yang paling sering digunakan saat ini hanya terdapat fitur keamanan seperti user password pada menu login, tidak ada fitur keamanan untuk isi pesan yang dikirim pada aplikasi chatting tersebut. Maka apabila saat proses pengiriman pesan tidak ada pengamanan, seluruh isi percakapan pengguna dapat dibaca dengan mudah oleh hacker sehingga dapat terjadi pencurian serta manipulasi data.

3.2 Penyelesaian Masalah

Untuk mengantisipasi permasalahan yang telah diuraikan, dibutuhkanlah sebuah aplikasi chatting yang memiliki fitur keamanan dalam pengiriman pesan teks. Untuk membuat aplikasi tersebut, digunakanlah teknik yang disebut kriptografi. Pada kriptografi terdapat dua proses yaitu enkripsi dan dekripsi. Proses enkripsi berfungsi untuk mengubah pesan teks yang berisi plaintext atau teks biasa yang terbaca menjadi ciphertext atau teks acak yang tak terbaca. Sedangkan proses dekripsi berfungsi untuk mengembalikan ciphertext tersebut menjadi plaintext seperti semula. Maka dengan penerapan kriptografi pada aplikasi ini, hacker pun tidak mempunyai kesempatan untuk mengetahui isi pada pesan yang dikirim dari aplikasi chatting ini. Seluruh akun pengguna dan isi percakapan yang terenkripsi antara pengirim dan penerima akan disimpan pada Firebase Console.

Algoritma yang digunakan pada aplikasi ini adalah algoritma AES 128 bit. Algoritma ini termasuk dalam jenis algoritma Kriptografi yang sifatnya simetris, jadi kunci yang digunakan pada enkripsi sama dengan dekripsi.

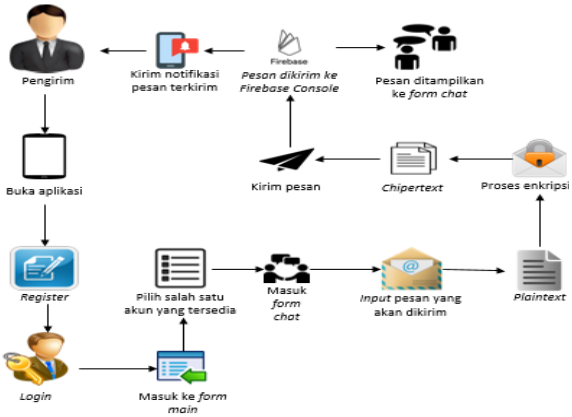
3.3 Skema Proses Keseluruhan Aplikasi

Untuk melengkapi penyelesaian masalah di atas, maka diuraikanlah skema proses keseluruhan pada aplikasi. Berikut adalah tahapan dan rich picture pada proses pengiriman pesan:

- Langkah awal untuk menggunakan aplikasi ini adalah pengirim terlebih

dahulu membuka aplikasi telah ter-install di perangkat Android.

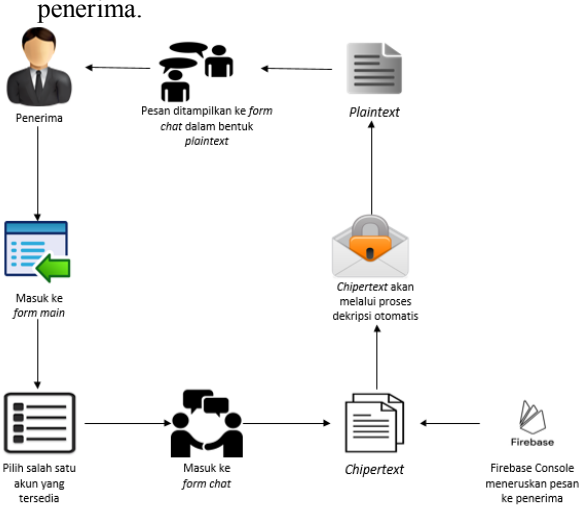
- Apabila pengirim belum memiliki akun aplikasi ini, pengirim dapat membuat akun baru dengan melakukan register. Pengirim mengisi data berupa username, email, dan password.
- Jika pengirim telah terdaftar sebagai user, pengirim dapat melakukan login dengan email dan password dan harus terkoneksi dengan internet.
- Setelah login pada aplikasi ini berhasil dan masuk ke dalam form utama aplikasi, pengirim memilih salah satu akun penerima yang tersedia untuk melakukan pengiriman pesan. Lalu aplikasi ini akan masuk ke form chat.
- Pengirim meng-input isi pesan sebelum melakukan pengiriman pesan.
- Pada saat proses pengiriman, aplikasi akan melakukan proses enkripsi terlebih dahulu.
- Plaintext yang didapat akan diubah menjadi ciphertext dengan menggunakan kunci yang telah diatur oleh sistem.
- Pesan dikirim ke Firebase Console dan akan diteruskan lalu ditampilkan ke dalam form chat penerima.
- Pengirim akan mendapatkan notifikasi berupa alert dialog yang berisi pesan telah terkirim.
- Chipertext yang telah dikirim akan ditampilkan pada form chat.



Gambar 1 : Rich Picture proses pengiriman pesan

Setelah proses pengiriman, berikut ini adalah tahapan dan pada proses penerimaan pesan :

- Penerima memilih salah satu akun pada form main. Setelah itu penerima akan masuk form chat.
- Pesan berbentuk ciphertext akan ditampilkan pada form chat. Ciphertext yang ditampilkan pada form chat berasal dari Firebase Console.
- Ciphertext akan melalui dekripsi otomatis.
- Ciphertext yang telah didekripsi akan berubah menjadi plaintext atau teks murni yang isinya sama saat pesan tersebut dikirim oleh pengirim pesan.
- Plaintext ditampilkan pada form chat milik penerima.



Gambar 2 : Rich Picture proses penerimaan pesan

4. HASIL DAN PEMBAHASAN

4.1 Spesifikasi Hardware dan Software

Agar aplikasi kriptografi chatting dapat berjalan dengan baik maka diperlukan perangkat yang mempunyai spesifikasi yang mendukung. Spesifikasi perangkat yang digunakan dalam pembuatan aplikasi ini, antara lain yaitu :

a. Perangkat Keras (Hardware)

Dalam pembuatan aplikasi ini, perangkat keras yang digunakan pada saat implementasi aplikasi ini sebagai berikut :

1) Laptop Processor Intel Core i3
2) Memory 4GB RAM
3) Harddisk 500GB
4) Touchpad dan Keyboard
5) Smartphone Android dengan sistem operasi versi 4.4 Kitkat

b. **Perangkat Lunak (*Software*)**

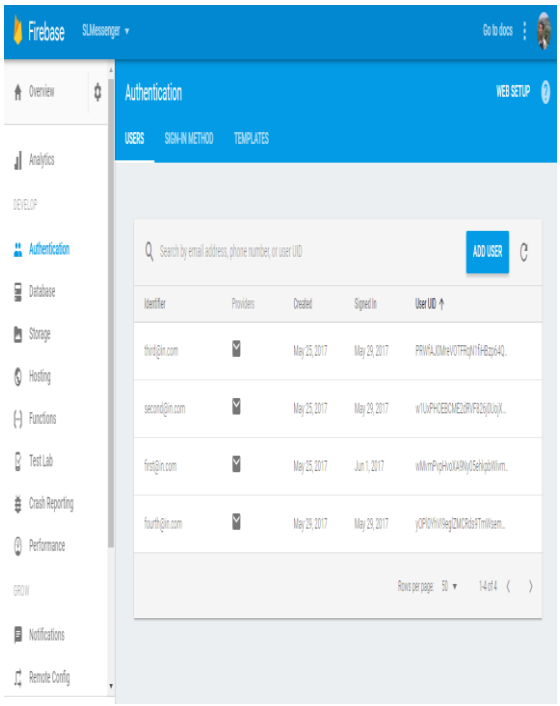
Dalam pembuatan aplikasi ini, perangkat lunak yang digunakan untuk implementasi aplikasi ini sebagai berikut :

1) Windows 10
2) Android Studio
3) Nox App Player
4) Google Chrome
5) Gradle
6) Adobe Photoshop CS5
7) Android Virtual Device
8) JDK

4.1 Tampilan Program

Tampilan Layar Akun Terdaftar

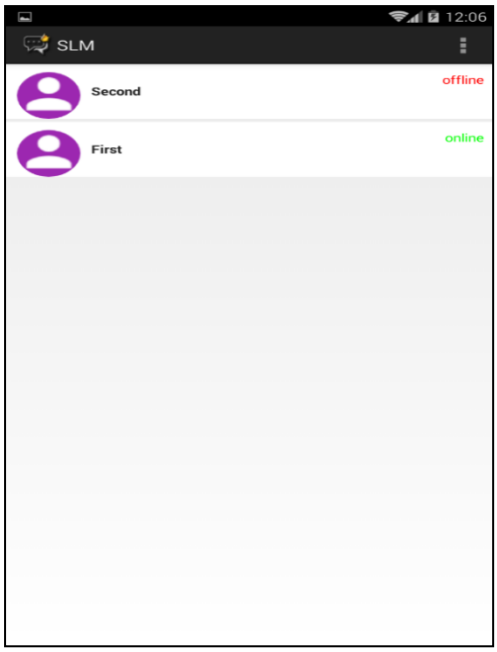
Jika seluruh *field* terisi dan *user* klik tombol *register*, aplikasi akan menyimpan akun di Firebase Console. Dan akun yang telah terdaftar dapat digunakan pada saat *login*. Untuk lebih jelasnya berikut adalah gambar tampilan layar akun terdaftar:



Gambar 3 Tampilan layar akun terdaftar

Tampilan Layar *Form Main*

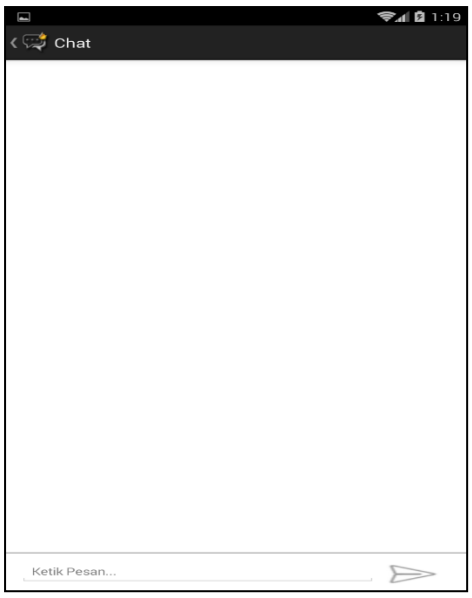
Form main adalah *form* yang digunakan *user* untuk memilih penerima untuk mengirimkan teks pesan. *User* penerima akan muncul apabila terdapat lebih dari satu akun di Firebase Console.



Gambar 4 Tampilan layar *form main*

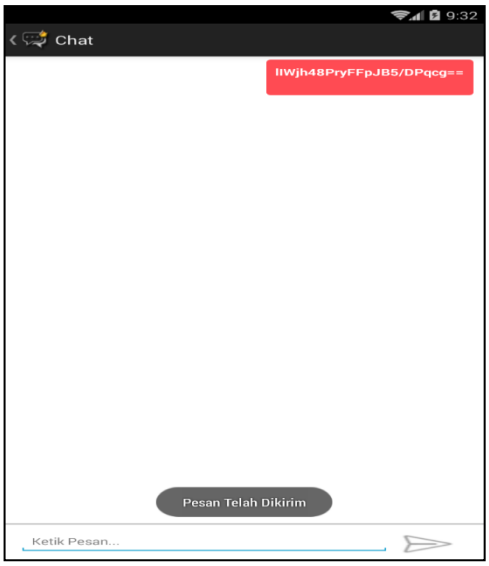
Tampilan Layar *Form Chat*

Form chat adalah *form* yang menampilkan proses pertukaran pesan, baik dari pengirim maupun penerima. *Form chat* ini akan muncul apabila *user* memilih salah satu penerima yang tersedia pada *form main.* Berikut ini adalah tampilan layar *form chat.*



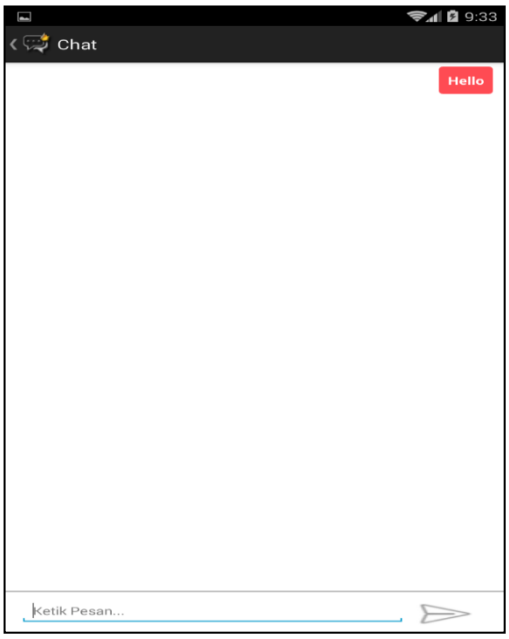
Gambar 5 Tampilan layar *form chat*

User dapat mengetik pesan yang diinginkan pada bagian bawah *form chat.* Setelah itu *user* dapat mengirim pesan dengan menekan tombol kirim yang ada dibagian bawah kanan *form chat.* Pesan yang dikirim akan melalui proses enkripsi AES 128 bit dan akan ditampilkan pada *form chat.*



Gambar 6 Tampilan layar pesan dikirim dan terenkripsi

Pesan yang ditampilkan saat dikirim berupa *chiphertext* lalu otomatis mengalami proses dekripsi AES 128 bit. *Chipertext* tersebut dapat berubah menjadi *plaintext* sehingga dapat dibaca oleh penerima maupun pengirim.

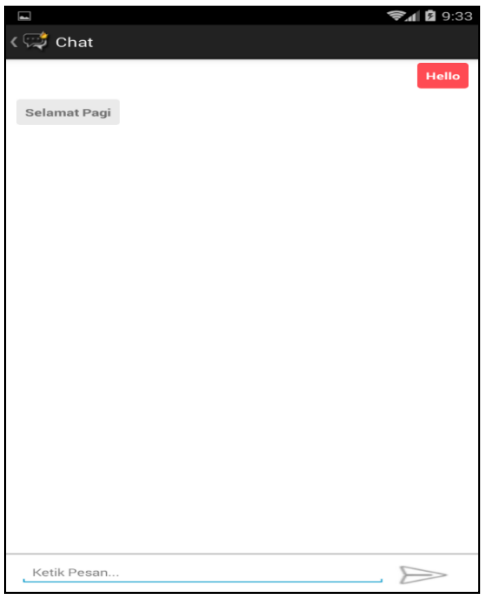


Gambar 7 Tampilan layar pesan terdekripsi

Jika ada pesan baru yang dikirim dari *user* lain yang merupakan pesan balasan akan ditampilkan disisi kiri layar. Pesan tersebut juga mengalami proses enkripsi dari aplikasi yang sama yang digunakan *user* lain.

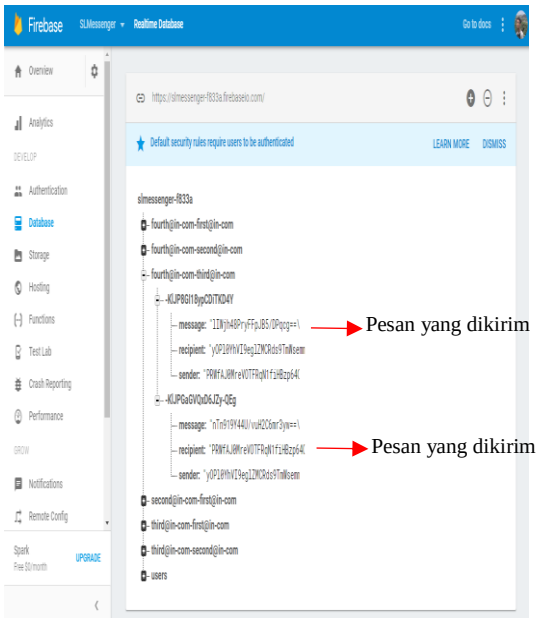
Gambar 8 Tampilan layar pesan balasan terenkripsi

Seperti pesan yang dikirim, pesan balasan dari *user* lain tersebut akan melalui proses dekripsi AES 128 bit agar *chipertext* dapat berubah menjadi *plaintext* dan dapat dibaca.



Gambar 9 Tampilan layar pesan balasan terdekripsi

Sama halnya dengan penyimpanan akun *user*, Seluruh percakapan antara pengirim dan penerima disimpan pada Firebase Console. Isi percakapan yang ada pada Firebase Console merupakan *chipertext*, sehingga pesan tetap aman dan hanya bisa dibaca pada aplikasi.



Gambar 10 Tampilan layar pesan disimpan pada *firebase console*

4.3 Uji Coba Program

Setelah spesifikasi perangkat keras dan perangkat lunak terpenuhi, maka aplikasi dapat dilakukan uji coba.

Pengujian Proses Enkripsi

Pengujian proses enkripsi merupakan pengujian untuk mengubah *plaintext* menjadi *ciphertext*. *Key* yang digunakan untuk melakukan enkripsi ini telah ditentukan oleh sistem yaitu 16s4laMind0ne5iA. Hasil berupa *chipertext* akan ditampilkan pada Firebase Console.

Tabel 1 Pengujian proses enkripsi

Plaintext	Key	Hasil pada Firebase Console (Chipertext)
San Marino’	16s4laMind0ne5iA	+kDaOQWSzoW/qLokYnQx7w==\n
Pukul 16.30	16s4laMind0ne5iA	8nXyeoDPOK6zkyIPJOWXPA==\n
Selamat siang	16s4laMind0ne5iA	O4hqgGlsy7Yqe6LpfV6eEw==\n
apa kabar?	16s4laMind0ne5iA	7xIgXqBG9EeespYk0PkK+g==\n

Pengujian Proses Dekripsi

Pengujian proses dekripsi merupakan pengujian untuk merubah *ciphertext* menjadi *plaintext*. Proses dekripsi bersifat otomatis sehingga *user* tidak perlu melakukan *input* apapun. *Key* yang digunakan untuk melakukan dekripsi ini telah ditentukan oleh sistem yaitu 16s4laMind0ne5iA. Hasil berupa *plaintext* akan ditampilkan pada *form chat* penerima.

Tabel 2 Pengujian proses dekripsi

Hasil pada Firebase Console (Chipertext)	Key	Plaintext
So8BJsVg7OIJj5JGhq83yA==\n	16s4laMind0ne5iA	network
zsKPu+dNThN9kISBJfXeDw==\n	16s4laMind0ne5iA	Penting!!!
QUhBVHf1vl9560gB0k3WkA==\n	16s4laMind0ne5iA	Berhasil
fKQ8NEMlnTV3OLQLjA5/7Q==\n	16s4laMind0ne5iA	Sukses

4.4 Evaluasi Program

a. Kelebihan

- Aplikasi kriptografi chatting ini mudah digunakan karena tampilannya dibuat secara user friendly.
- Ukuran aplikasi ini kurang lebih hanya sebesar 2 MB saat proses install, sehingga tidak terlalu banyak mengisi penyimpanan internal pada smartphone Android pengguna.
- Dalam pengoperasiannya, aplikasi ini berjalan sangat ringan dan tidak membebani kinerja smartphone Android pengguna.
- Pengguna tidak perlu menulis atau menginput key, karena sudah diatur oleh sistem.
- Aplikasi kriptografi chatting dapat berjalan dengan baik selama ada koneksi internet.
- Aplikasi ini dapat berjalan dengan baik pada sistem operasi Android versi 4.4 ke atas.
- Isi pesan akan lebih aman, karena pesan yang dikirim telah dienkripsi. Dan pesan hanya dapat dibaca pada aplikasi ini.

b. Kekurangan

- Fitur-fitur yang ada pada aplikasi kriptografi chatting masih sedikit.
- Kelancaran proses pengiriman pesan tergantung pada ukuran pesan serta koneksi internet yang digunakan. Semakin besar ukuran pesan, maka semakin lama proses enkripsi dan dekripsinya.
- Aplikasi tidak akan berjalan pada sistem operasi Android di bawah versi 4.4.
- Pengguna hanya bisa mengirim pesan berupa teks.

5. KESIMPULAN

Berdasarkan analisa permasalahan dan penyelesaian masalah pada bab-bab sebelumnya, maka dapat disimpulkan bahwa program aplikasi *chatting* dengan metode *Advanced Encryption*

Standard (AES) 128 berbasis Android pada PT. Salam Medina Indonesia sangat diperlukan karena:

- Dengan adanya aplikasi ini maka isi dari pesan teks terjaga kerahasiaannya dari pihak yang tidak bertanggung jawab, yang tidak berkepentingan, dan yang tidak berhak untuk mengetahui apa isi dari pada pesan teks tersebut.
- Tingkat keamanan pesan setelah dienkripsi cukup terjaga, dengan kata lain pesan tidak berkurang atau mengalami kerusakan setelah proses enkripsi pesan dilakukan.
- Seluruh pesan yang dikirimkan tidak akan hilang walaupun aplikasi dihapus dari *smartphone* pengguna, karena pesan-pesan yang telah dikirimkan dan terenkripsi akan disimpan pada Firebase Console.

Dengan terbatasnya waktu yang diberikan untuk menyelesaikan penelitian ini, penyelesaian masalah yang telah dikembangkan masih jauh dari sempurna, sehingga perlu dilakukan penyempurnaan baik disisi *hardware* maupun *software*. Saran yang dapat dikembangkan antara lain:

- Ditambahkannya fitur-fitur untuk melengkapi aplikasi ini seperti kirim *file*, foto, pengaturan profil pengguna, grup *chatting*, tambah teman secara *manual*, penghapusan pesan, dan *voice call*.
- Ditambahkannya kompatibilitas pada sistem operasi Android di bawah versi 4.4. agar aplikasi ini dapat berjalan di seluruh versi sistem operasi Android.
- Membuat autentifikasi melalui *email* untuk mengecek *email* pengguna yang dimasukkan apakah *email* tersebut aktif atau tidak.

6. DAFTAR PUSTAKA

[1] Arif, A. dan Mandarani, P., 2016. Rekayasa Perangkat Lunak Kriptografi Menggunakan Algoritma Advanced Encryption Standard (AES) 128 Bit Pada Sistem Keamanan Short Message Service (SMS) Berbasis Android. Jurnal TEKNOIF Institut Teknologi Padang. hal. 84-93.

[2] Hanafi, J.I. dan Patombongi, A, 2016. Aplikasi Sms Kriptografi Menggunakan Metode Aes Berbasis Android. Jurnal Sistem Informasi dan Teknik Komputer Catur Sakti Vol.1, No. 1. hal. 69-75.

[3] Hardianto, F. dan Handaga, B., 2015. Aplikasi Grupchat Di Android Menggunakan Websocket. Informatika Universitas Muhammadiyah Surakarta.

[4] Rahmayunita, Isnawaty, dan Sutardi, 2015. Penyadapan Sms Dan Gps Berbasis Android Menggunakan Algoritma Advanced Encryption Standard (AES). semanTIK Universitas Halu Oleo Kendari. hal. 11-22.

[5] Saefudin, dan Syamsudin, 2016. Aplikasi Enkripsi Pesan Teks Dengan Metode Advanced Encryption Standard Pada Ponsel Berbasis Android. Jurnal Sistem Informasi Universitas Serang Raya. hal. 25-28.