IMPLEMENTASI KRIPTOGRAFI DENGAN ALGORITMA CAESAR CIPHER, AES 192 dan DES UNTUK APLIKASI PESAN INSTAN BERBASIS ANDROID

Adi Rahmad Nugroho[1)],Wahyu Pramusinto, M.Kom[2)]
[1]Program studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : arnstark12@gmail.com[1)], wahyu.pramusinto@budiluhur.ac.id[2)]

ABSTRAK

Perkembangan teknologi komputer dan komunikasi makin pesat membuat kegiatan manusia makin mudah, salah satunya mengirim informasi dengan cepat dan tepat. Proses pengiriman informasi antara satu pihak kepada pihak lain perlu memperhatikan kerahasiaan data dan informasi agar terjamin kerahasiaannya. Pada penelitian ini akan dibuat sebuah aplikasi chatting yang menggunakan metode kriptografi Advanced Encryption Standard (AES) 192 bit, dan Data Encryption Standard (DES) untuk mengamankan pesan yang dikirm. Sedangkan ketika user mengirimkan pesan berupa lampiran gambar, url gambar yang dikirimkan nantinya akan diamankan dengan metode kriptografi Caesar Cipher. Dengan adanya metode kriptografi AES 192, DES, dan Caesar Cipher yang diimplementasikan pada aplikasi chatting ini, dan user dapat mengirim pesan dengan aman tanpa khawatir pesan dan data lampiran gambar disadap atau dimanipulasi oleh pihak yang tidak bertanggung jawab.

Kata kunci: Kriptografi, AES, DES, Caesar Cipher

1. PENDAHULUAN

Perkembangan teknologi komputer dan komunikasi makin pesat membuat kegiatan manusia makin mudah, salah satunya mengirim informasi dengan cepat dari satu tempat ketempat lain. Proses pengiriman informasi antara satu pihak kepada pihak lain perlu memperhatikan kerahasiaan data dan informasi agar terjamin kerahasiaannya. Untuk mengatasi permasalahan kerahasiaan data dan informasi maka dianggap perlu memanfaatkan kriptografi sebagai pengamanan data dan informasi.

Kriptografi sudah ada sejak jaman dahulu, namun seiring dengan berkembangnya teknologi,maka kriptografi ini juga semakin berkembang. Perkembangan kriptografi ini dimaksudkan supaya tidak ada yang bisa memecahkannya. Seiring dengan berkembangnya teknologi informasi dunia, berkembang pula teknologi komunikasi. Mulai dari surat, telepon, hingga sekarang yang paling banyak digunakan adalah internet. Internet semakin banyak diminati karena mudah digunakan, dan dapat diakses setiap orang dari berbagai kalangan. Salah satu hasil dari perkembangan teknologi dan informasi pada saat ini adalah aplikasi instant messaging atau yang dikenal saat ini adalah aplikasi chatting.

Aplikasi chatting merupakan aplikasi yang mengijinkan penggunanya dapat mengirimkan pesan secara satu waktu atau real time yang membuat jarak yang jauh seolah-olah tidak berarti di dunia internet. Dengan memafaatkan layanan internet, aplikasi chatting dapat berjalan dengan mudah dan cepat.

Perkembangan aplikasi chatting pun berkembang sangat pesat sampai saat ini. Banyak aplikasi chatting yang terkenal seperti Whatsapp, BBM, LINE, Telegram dan lainnya yang memiliki keunggulan masing-masing.Tetapi aplikasi chatting tersebut masih memiliki kekurangan pada pengamanan pengiriman pesan, karena pada dasarnya aplikasi tersebut digunakan oleh umum dan di akses dari seluruh penjuru dunia. Resiko yang timbul dari hal tersebut adalah informasi yang ada di dalam pesan tersebut dapat dicuri, diketahui, disadap oleh pihak yang tidak bertanggung jawab yang berdampak kerugian bagi pengguna dan khususnya bagi perusahaan atau lembaga.

1.2. Batasan Masalah

Mengingat besarnya ruang lingkup pembuatan aplikasi *chatting*, maka dibuat batasan-batasan dari permasalahan sebagai berikut :

a. Bagaimana cara mengamankan pesan pada aplikasi *chatting* yang dikirimkan dengan cara mengenkripsi pesan tersebut lalu mendekripsikannya kembali tanpa merubah isi dari pesan tersebut agar tidak bisa dibaca oleh pihak yang tidak bertanggung jawab ?

b. Bagaimana cara mengenkripsi pesan berupa lampiran gambar lalu mendekripsikannya kembali tanpa harus merubah isi dari gambar yang dikirimkan ?

1.3. Tujuan Penulisan

Penelitian ini memiliki beberapa tujuan antara lain :

a. Membuat aplikasi *chatting* berbasis android.
b. Membuat aplikasi *chatting* yang mampu menjaga kerahasiaan isi informasi pesan yang disampaikan dengan menggunakan enkripsi pada pesan yang dikirimkan.
c. Menerapkan enkripsi Caesar Cipher, AES 192 *bit*, DES, dan pada saat mengenkrip dan mendekrip pesan.

2. LANDASAN TEORI

2.1. Pengertian Android

Android adalah suatu sistem operasi yang berjalan pada *smartphone* saat ini dan menyesuaikan spesifikasi di kelas *low-end* hingga *high-end*. Hampir semua *vendor* saat ini mengembangkan produknya dengan sistem operasi Android, karena peminatnya yang semakin meningkat tajam. (Hplover, 2017)

2.2. Kriptografi

Kriptografi adalah ilmu mengenai teknik enkripsi dimana "naskah asli" (*plaintext*) diacak menggunakan suatu kunci enkripsi menjadi "naskah acak yang sulit dibaca" (*ciphertext*) oleh seseorang yang tidak memiliki kunci dekripsi. Dekripsi menggunakan kunci dekripsi bisa mendapatkan kembali data asli. Probabilitas mendapat kembali naskah asli oleh seseorang yang tidak mempunyai kunci dekripsi dalam waktu yang tidak terlalu lama adalah sangat kecil.

Teknik enkripsi yang digunakan dalam kriptografi klasik adalah enkripsi simetris dimana kunci dekripsi sama dengan kunci enkripsi. Untuk public key cryptography, diperlukan teknik enkripsi asimetris dimana kunci dekripsi tidak sama dengan kunci enkripsi. Enkripsi, dekripsi dan pembuatan kunci untuk teknik enkripsi asimetris memerlukan komputasi yang lebih intensif dibandingkan enkripsi simetris, karena enkripsi asimetris menggunakan bilangan – bilangan yang sangat besar. (Andika, 2017)

2.3 Algoritma AES

AES ini merupakan algoritma block cipher dengan menggunakan sistem permutasi dan substitusi (P-Box dan S-Box) bukan dengan jaringan Feistel sebagaiman block cipher pada umumnya. Jenis AES terbagi 3, yaitu :

1) AES-128
2) AES-192
3) AES-256

Pengelompokkan jenis AES ini adalah berdasarkan panjang kunci yang digunakan. Angka-angka di belakang kata AES menggambarkan panjang kunci yang digunakan pada tipa-tiap AES. Selain itu, hal yang membedakan dari masing-masing AES ini adalah banyaknya round yang dipakai. AES-128 menggunakan 10 round, AES-192 sebanyak 12 round, dan AES-256 sebanyak 14 round. AES memiliki ukuran block yang tetap sepanjang 128 bit dan ukuran kunci sepanjang 128, 192, atau 256 bit. Tidak seperti Rijndael yang block dan kuncinya dapat berukuran kelipatan 32 bit dengan ukuran minimum 128 bit dan maksimum 256 bit. Berdasarkan ukuran block yang tetap, AES bekerja pada matriks berukuran 4x4 di mana tiap-tiap sel matriks terdiri atas 1 byte (8 bit). Sedangkan Rijndael sendiri dapat mempunyai ukuran matriks yang lebih dari itu dengan menambahkan kolom sebanyak yang diperlukan. Blok chiper tersebut dalam pembahasan ini akan diasumsikan sebagai sebuah kotak. Setiap plainteks akan dikonversikan terlebih dahulu ke dalam blok-blok tersebut dalam bentuk heksadesimal. Barulah kemudian blok itu akan diproses dengan metode yang akan dijelaskan. (Goernia, 2013)

2.4 Algoritma DES

DES (Data Encryption Standard) adalah algoritma cipher blok yang populer karena dijadikan standard algoritma enkripsi kunci-simetri, meskipun saat ini standard tersebut telah digantikan dengan algoritma yang baru, AES, karena DES sudah dianggap tidak aman lagi. Sebenarnya DES adalah nama standard enkripsi simetri, nama algoritma enkripsinya sendiri adalah DEA (Data Encryption Algorithm), namun nama DES lebih populer daripada DEA. Algoritma DES dikembangkan di IBM dibawah kepemimpinan W.L. Tuchman pada tahun 1972. Algoritma ini didasarkan pada algoritma Lucifer yang dibuat oleh Horst Feistel. Algoritma ini telah disetujui oleh National Bureau of Standard (NBS) setelah penilaian kekuatannya oleh National Security Agency (NSA) Amerika Serikat.DES termasuk ke dalam sistem kriptografi simetri dan tergolong jenis cipher blok. DES beroperasi pada ukuran blok 64 bit. DES mengenkripsikan 64 bit plainteks menjadi 64 bit cipherteks dengan menggunakan 56 bit kunci internal (internal key) atau upa-kunci (subkey). Kunci internal dibangkitkan dari kunci eksternal (external key) yang panjangnya 64 bit. (Suhardono, 2015)

2.5 Algoritma Caesar Cipher

Dalam kriptografi , sebuah Caesar cipher, juga dikenal sebagai cipher Caesar, cipher pergeseran, kode Caesar atau pergeseran Caesar, adalah salah satu yang paling sederhana dan paling dikenal luas enkripsi teknik. Ini adalah jenis cipher substitusi dimana setiap

huruf pada plaintext digantikan oleh beberapa surat tetap jumlah posisi down alfabet. Misalnya, dengan pergeseran tiga, A akan digantikan oleh D, B akan menjadi E, dan sebagainya.

Cara kerja sandi ini dapat diilustrasikan dengan membariskan dua set alfabet; alfabet sandi disusun dengan cara menggeser alfabet biasa ke kanan atau ke kiri dengan angka tertentu (angka ini disebut kunci).

Alfabet Biasa : ABCDEFGHIJKLMNOPQRSTUVWXYZ
Alfabet Sandi : DEFGHIJKLMNOPQRSTUVWXYZABC

Untuk menyandikan sebuah pesan, cukup mencari setiap huruf yang hendak disandikan di alfabet biasa, lalu tuliskan huruf yang sesuai pada alfabet sandi. Untuk memecahkan sandi tersebut gunakan cara sebaliknya.

Contoh penyandian sebuah pesan adalah sebagai berikut.

Plain Teks : kirim pasukan ke sayap kiri
Cipher Teks : NLULP SDVXNDQ NH VDBDS NLUL

Jika pergeseran yang dilakukan sebanyak tiga kali, maka kunci untuk dekripsinya adalah 3. Pergeseran kunci yang dilakukan tergantung keinginan pengiriman pesan.

3.ANALISA MASALAH DAN PERANCANGAN PROGRAM

3.1. Analisa Masalah

Aplikasi *chatting* merupakan media pertukaran informasi berupa pesan teks yang sering digunakan oleh setiap orang. Aplikasi *chatting* yang sering digunakan pada saat ini memiliki banyak fitur seperti *user password* pada *menu login*, enkripsi dan tidak ada fitur keamanan untuk mengamankan pesan yang telah terkirim dan tersimpan ke database *server* aplikasi *chatting* tersebut. Apabila *server* tersebut diretas, maka seluruh isi percakapan yang tersimpan di *database* dapat dibaca dan dicuri dengan mudah oleh pihak yang tidak berkepentingan sehingga dapat terjadi pencurian dan manipulasi data.

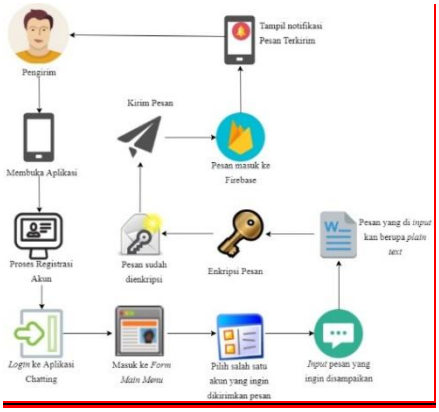
3.2. Penyelesaian Masalah

Dari permasalahan yang telah diuraikan di atas, dibuatlah aplikasi *chatting* yang sesuai dengan kebutuhan dan memiliki keamanan pada pengiriman pesan. Keamanan pengiriman pesan dilakukan dengan cara menggunakan teknik enkripsi. Metode enkripsi yang dipilih adalah Caesar Cipher, AES 192, dan DES. Aplikasi yang dibuat berbasis Android yang dapat diakses menggunakan jaringan internet

3.2. Skema Proses Keseluruhan Aplikasi

Untuk menyelesaikan masalah diatas, maka diuraikanlah skema proses keseluruhan aplikasi *chatting*. Berikut adalah tahapan dan *rich picture* pada proses pengiriman pesan :

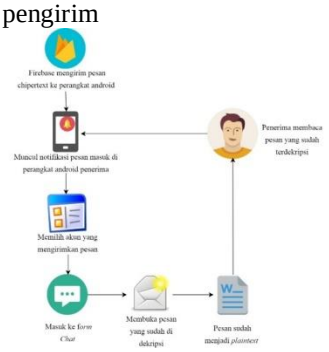
1) Untuk menggunakan aplikasi *chatting* ini , pengirim harus membuka aplikasi yang telah diinstal di perangkat android.
2) Apabila pengirim belum memiliki akun aplikasi ini, pengirim dapat membuat akun baru dengan melakukan *register*. Pengirim harus mengisi data berupa *username, email, password.*
3) Bila pengirim sudah mendaftar sebagai *user*, pengirim dapat melakukan proses *login* dengan *email* dan *password* yang sudah terhubung ke internet.
4) Setelah *login* pada aplikasi *chatting* dan berhasil masuk. Maka pengirim masuk ke dalam *form* utama dan pengirim memilih salah satu akun penerima yang sudah tersedia untuk melakukan proses pengiriman pesan enkripsi. Lalu setelah memilih akun untuk dikirimkan pesan enkripsi, pengirim masuk ke *form chat.*
5) Setelah itu pengirim meng-*input* isi pesan yang ingin dikirim ke penerima yang sudah di pilih.
6) Pada saat proses pengiriman, aplikasi akan melakukan proses enkripsi terlebih dahulu.
7) Pesan teks yang di-*input* akan dirubah menjadi *chipertext* dengan menggunakan kunci yang sudah diatur oleh sistem.
8) Setelah proses enkripsi selesai, pesan dikirim ke *Firebase Console* lalu diteruskan ke akun penerima pesan dan ditampilkan didalam *form chat* penerima.
9) Pengirim akan mendapatkan notifikasi berupa laporan pengiriman bahwa pesan berhasil terkirim atau tidak.
10) *Chipertext* yang telah dikirim akan ditampilkan pada *form chat* penerima yang otomatis sudah didekripsi terlebih dahulu oleh aplikasi.



Gambar 1 : *Rich Picture* proses Pengiriman Pesan

Setelah proses pengiriman pesan, berikut ini adalah proses penerimaan pesan :

1) Penerima mendapatkan notifikasi berupa pesan masuk dari pengirim.
2) Setelah itu penerima memilih salah satu akun yang mengirimkan pesan yang ditampilkan di *form main menu* dan membuka isi pesan tersebut. Setelah pesan dibuka maka penerima akan masuk ke *form chat*.
3) Ketika pesan dibuka, maka pesan yang awalnya berbentuk *chipertext* tidak ditampilkan pada *form chat* penerima. *Chipertext* yang ambil berasal dari *Firebase Console*.
4) *Chipertext* akan melalui proses dekripsi pesan.
5) *Chipertext* yang telah di dekripsi akan berubah menjadi *plaintext* atau teks biasa.
6) *Plaintext* ditampilkan pada form chat penerima yang isinya adalah pesan murni yang dikirim oleh pengirim

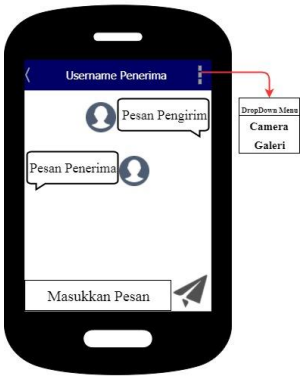


Gambar 2 : Rich Picture proses Penerimaan Pesan

3.3 Rancangan Layar

a. Rancangan Layar *Form Chat*

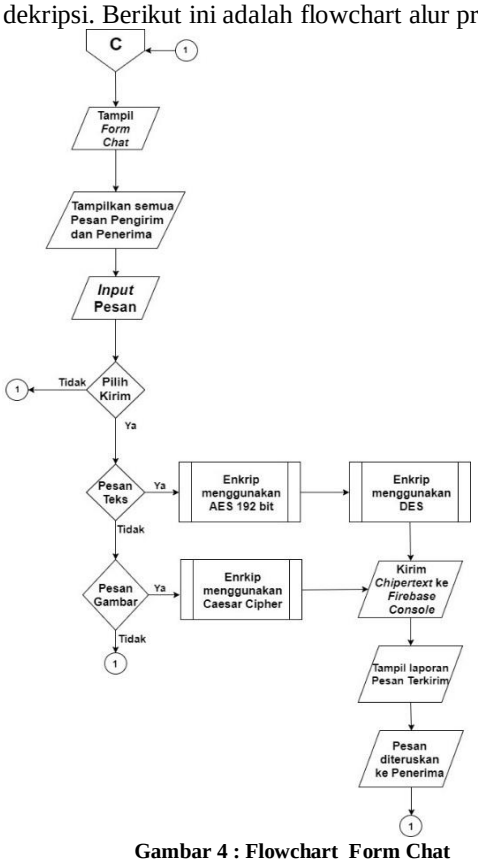
Form chat adalah *form* yang digunakan untuk melakukan aktivitas *chat* atau percakapan dengan *user* lain yang sudah terdaftar dan dipilih dari *form Main Menu*. Pesan percakapan yang kita kirim ke *user* lain akan di enkripsi dengan menggunakan metode AES 192 *bit* dan DES, sedangkan bila pengirim ingin mengirim pesan berupa gambar, maka pesan tersebut akan di enkripsi menggunakan metode Caesar Cipher. Semua pesan selama pengiriman akan aman karena telah terenkripsi. Pada saat pesan masuk ke perangkat android penerima pesan, maka pesan yang semula terenkripsi akan langsung didekripsi pada *form chat* penerima agar dapat langsung dibaca. Tampilan *form* ini bisa dilihat di Gambar berikut :



Gambar 3 : Rancangan Layar Form Chat

3.4 Flowchart Alur Proses

Dalam penggunaan form chat , user dapat mengirim pesan teks ke user yang sudah dituju dari Form Main Menu. Pesan yang dikirim akan melalui proses enkripsi dan pesan yang diterima akan melalui proses dekripsi. Berikut ini adalah flowchart alur proses chat.



Gambar 4 : Flowchart Form Chat

3.5 Algoritma Alur Proses

Algoritma ini menjelaskan tentang alur proses yang terjadi ketika user mengirimkan pesan di form chat :

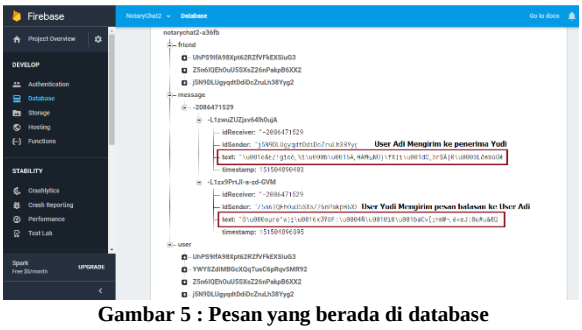
1. Tampil Form Chat
2. Tampil semua Teks pesan Pengirim dan Penerima
3. Input Pesan
4. If Pilih Kirim then
5. If pesan “teks” then
6. Enkrip AES 192 bit
7. Enkrip DES
8. Kirim ke Firebase Console
9. Else if Pesan “Gambar” then
10. Enkrip Caesar Cipher
11. Kirim Ke Firebase Console
12. End if
13. Tampil laporan pengiriman “Pesan Terkirim”
14. Pesan diteruskan ke Penerima
15. Else
16. Kembali ke baris 1
17. End If

4. HASIL DAN PEMBAHASAN

4.1 Hasil Uji Coba Program

Setelah dijelaskan mengenai alur kerja program diatas ketika pesan yang dikirimkan secara otomatis akan disimpan kedalam database firebase sebagai pesan yang sudah terenkripsi.

Untuk lebih jelasnya bisa dilihat pada gambar dibawah ini :



Gambar 5 : Pesan yang berada di database

4.2 Analisa Hasil Uji Coba Program

Setelah proses perangkat keras dan perangkat lunak terpenuhi, penulis melakukan uji coba program. Analisa hasil uji coba program merupakan salah satu hal yang perlu dilakukan dalam setiap pengembangan aplikasi guna menganalisa dan mengetahui hasil yang telah dicapai oleh aplikasi yang dikembangkan tersebut. Dari hasil uji coba program penulis menemukan beberapa batasan program yang dilihat dari beberapa kondisi dan situasi. Adapun batasan program pada aplikasi ini adalah sebagai berikut :

a. Kelebihan Program

1) Aplikasi ini tergolong pada aplikasi yang ringan karna hanya memerlukan *space memory* sebesar 8MB saat proses instalasi.
2) Aplikasi ini dapat mengirimkan pesan secara *real time*.
3) Aplikasi ini menggunakan database yaitu *firebase* untuk meringankan penggunaan data seluler. Jadi ketika aplikasi ini ditutup dan dibuka kembali tanpa menggunakan koneksi, pesan yang ada masih bisa dilihat.
4) Pesan yang dikirim dapat berupa teks dan gambar.
5) Pada saat aplikasi sedang tidak dibuka, program dapat memberikan notifikasi pada pengguna selama koneksi tetap tersambung.
6) Setiap pesan yang dikirimkan terenkripsi oleh tiga algorima.
7) Pengguna tidak perlu meng-*input key* serta melakukan penyimpanan kunci, karena sudah diatur oleh sistem.

b. Kelemahan Program

1) Aplikasi ini tidak bisa melakukan *group chat* dan *broadcase message.*
2) Fitur pada aplikasi *chatting* ini masih sedikit, diantaranya tidak bisa mengirim pesan berupa suara, dokumen dan dan tidak ada *setting* penggunaan data.
3) Aplikasi ini tidak dapat dijalankan pada system operasi android dibawah versi 5.0.
4) Aplikasi ini tidak bisa melakukan percakapan baik melalui panggilan *voice call* ataupun *video call*.
5) Aplikasi ini tidak bisa melakukan *load* pesan ketika tidak ada koneksi internet.

5. KESIMPULAN

Berdasarkan analisa permasalahan dan penyelesaian masalah pada bab-bab sebelumnya, maka dapat disimpulkan bahwa program Kriptografi dengan Algoritma Caesar Cipher, AES 192, DES untukAplikasi Pesan Instan Berbasis Android sangat diperlukan karena:

a. Dengan adanya aplikasi ini maka isi dari pesan teks dan isi dari gambar yang dikirimkan melalui *url* terjaga kerahasiaannya dari pihak yang tidak bertanggung jawab dan yang tidak berhak untuk mengetahui apa isi dari pada pesan teks dan juga gambar tersebut.
b. Tingkat keamanan pesan setelah dienkripsi menggunakan tiga buah algoritma enkripsi cukup terjaga, dengan kata lain pesan tidak

berkurang atau mengalami kerusakan setelah proses enkripsi pesan dilakukan.

c. Dari hasil pembuatan sistem enkripsi dan dekripsi pesan diperlukan kunci standar yang diatur oleh sistem dan ditambah dengan *roomID* yang setiap saat berubah ubah tergantung user berkomunikasi dengan user lain.

Program Kriptografi dengan Algoritma Caesar Cipher, AES 192, DES untukAplikasi Pesan Instan Berbasis Android masih memiliki banyak kekurangan dan diperlukan pengembangan lebih lanjut guna mencapai hasil pengamanan maksimal. .

Berikut ini saran yang dijadikan acuan untuk pengembangan aplikasi selanjutnya:

a. Ditambahkannya fitur-fitur untuk melengkapi aplikasi ini sesuai kebutuhan *user*
b. Ditambahkannya kompatibilitas pada sistem operasi android dibawah versi 5.0 agar aplikasi ini dapat berjalan di seluruh versi sistem operasi android.
c. Membuat autentikasi melalui *email* untuk mengecek *email* pengguna yang dimasukkan.

6. DAFTAR PUSTAKA

[1] Andika, D., 2017. Pengertian dan Sejarah Kriptografi. [Online] Available at: https://www.it-jurnal.com/pengertian-dan-sejarah-kriptografi/ [Accessed 19 Oktober 2017].

[2] Goernia, H., 2013. Herwin Blog. [Online] Available at: http://herwingoernia19.blogspot.co.id/2013/12/kriptografi-metode-algoritma-aes.html[Accessed 19 Oktober 2017].

[3]Hplover, 2017. Pengertian Apa itu Android, s.l.: http://hplover.com/pengertian-apa-itu-android.html.

[4]Suhardono, Z., 2015. http://ilmu-kriptografi.blogspot.co.id. [Online] Available at: http://ilmu-kriptografi.blogspot.co.id/2009/05/algoritma-des-data-encryption-standart.html [Accessed 20 Oktober 2017].