APLIKASI ANDROID UNTUK PENGAMAN TEKS MENGGUNAKAN KRIPTOGRAFI BERLAPIS DENGAN ALGORITMA CAESAR, BLOWFISH DAN AES *(ADVANCED ENCRYPTION STANDAR)*

Fernanda Fitriansyah[(1)], **Ery Safrianti**[(2)]
[1)]Mahasiswa Teknik Elektro Universitas Riau, [2)]Dosen Jurusan Teknik Elektro Universitas Riau
Laboratorium Jaringan dan Komputer
Program Studi Teknik Elektro S1, Fakultas Teknik Universitas Riau
Kampus Binawidya Jl. HR. Soebrantas Km 12,5 Simpang Baru, Panam, Pekanbaru 28293Email: fernanda.fitriansyah@gmail.com

ABSTRACT

Rapid technological developments in the telecommunications sector provide benefits that can facilitate communication from one place to another. Technological developments are also required to improve security. Along with that the security of the information exchanged is also very necessary to avoid things that are not desirable. One method of securing information and messages is to use data encryption and description, which is studied in the field of cryptography. To overcome the security problems mentioned above, this research makes an Android Application for Text Safeguards Using Layered Cryptography with Caesar, Blowfish and AES Algorithms (Advanced Standard Encryption). This application can be run on the Android 5.0 (lollipop) or above, which can be used to encrypt and decrypt text messages..

Keywords: Security, Cryptology, Caesar, Blowfish, AES.

PENDAHULUAN

Perkembangan teknologi saat ini mengalami peningkatan yang sangat pesat dalam segala bidang agar bisa mempermudah semua aktifitas manusia. Pada bidang telekomunikasi memberikan manfaat yang dapat mempermudah komunikasi dari suatu tempat ke tempat yang lainnya, bahkan jarak dan waktu bukan lagi menjadi sebuah kendala yang berarti. Salah satu hasil teknologi yang berperan besar dalam perkembangan telekomunikasi yaitu ditemukannya telepon, dan berkembang menjadi telepon selular (Ponsel). Mulai dari ponsel yang hanya bisa digunakan untuk bicara dan SMS (*Short Message Service*) hingga ponsel cerdas(*smartphone*) yang memiliki berbagai fungsi seperti *multimedia*, *multiplayer games*, transfer data, video *streaming* dan lain-lain. Perkembangan teknologi juga dituntut untuk meningkatkan keamanan. Seiring dengan itu keamanan informasi yang dipertukarkan juga sangat diperlukan guna menghindari hal-hal yang tidak diinginkan.

Saat ini berbagai macam aplikasi sosial media sangat banyak beredar dikalangan masyarakat untuk mempermudah berkomunikasi dan berinteraksi satu individu ke individu lain ataupun satu individu kebanyak individu sekaligus yang dilakukan didunia maya. Semakin banyak orang melakukan komunikasi melalui media sosial maka akan semakin banyak pula peluang tindakan yang bisa merugikan. Seperti penyadapan, pembajakan, pembocoran informasi melalui pihak ketiga, ataupuan kejahatan lainnya. Hal tersebut akan menyebabkan kerugian kepada pihak pengirim ataupun penerima.

Ada beberapa teknik yang digunakan untuk menjaga keamanan informasi maupun pesan. Salah satu metode pengamanan informasi maupun pesan adalah dengan menggunakan enkripsi dan deskripsi data, yang dipelajari dalam bidang ilmu kriptografi. Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan atau informasi yang dapat dibaca. Pesan biasanya disebut juga *plaintext* dan hasil dari enkripsi disebut *ciphertext*. Ada dua jenis algoritma kriptografi yaitu algoritma kriptografi klasik dan algoritma kriptografi modern. Dalam pengoperasiannya, algoritma kriptografi klasik bekerja menggunakan mode karakter seperti: *Hill Cipher, Vigenere Cipher, Caesar Cipher, Affine Cipher* dan lain-lain, sedangkan algoritma kriptografi modern bekerja menggunakan mode bit seperti: AES *(Advanced Encryption Standar), Blowfish*, DES *(Data Encryption Standard),* IDEA

(International Data Encryption Algorithm), RSA*(Rivest Shamir Adleman)* dan lain-lain.

Dalam mengatasi permasalahan tersebut maka pada penelitian ini yang berjudul ”Aplikasi Android Untuk Pengaman Teks Menggunakan Kriptografi Berlapis Dengan Algoritma Caesar, Blowfish dan AES *(Advanced Encryption Standar)”* yang akan merancang sebuah aplikasi berbasis Android untuk pengaman teks menggunakan kriptografi berlapis dengan algoritma Caesar, Blowfish dan AES. Agar aplikasi ini dapat menyandikan teks penting menjadi teks dalam bentuk acak yang akan dikirim atau dibagikan melalui layanan komunikasi sosial media seperti WhatsApp, Line, SMS dan lainnya dengan maksud melindungi informasi tersebut dari pihak yang tidak berhak. Dan informasi atau teks acak tersebut masih bisa dikembalikan kebentuk semula dengan menggunakan kata kunci yang sama saat menyandikan.

TINJAUAN PUSTAKA

1. Kriptografi

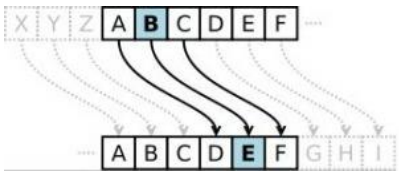
Kriptografi berasal dari bahasa Yunani, crypto dan graphia. Crypto berarti secret (rahasia) dan graphia berarti writing (tulisan). Kriptografi menurut terminologinya adalah sebuah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain. Secara istilah kriptografi didefinisikan sebagai ilmu sekaligus seni untuk menjaga kerahasiaan pesan baik berupa data maupun informasi yang mempunyai arti atau nilai dengan cara menyamarkan (mengacak) menjadi bentuk yang tidak dapat dimengerti menggunakan suatu algoritma tertentu (Roharjo T, 2018).

Proses kriptografi diawali dengan mengubah data dalam bentuk plaintext (tulisan atau pesan awal yang dapat dibaca) menjadi chipertext (tulisan atau pesan rahasia yang tidak dapat lagi dibaca dengan mudah) dengan menggunakan algoritma yang mentransposisikan (mengubah posisi) tiiap-tiap karakter / bit pada plaintext dan dengan cara mensubstitusikan (mengganti) tiap-tiap karakter / bit pada plaintext sehingga dihasilkan tulisan atau data yang berbeda sama sekali dengan data awal. Metode pengubahan plaintext menjadi chipertext di tempat pengirim atau pembuat data dinamakan dengan Metode Enkripsi, dengan menggunakan kunci enkripsi. Di tempat penerima atau pembaca data, chipertext yang diterima kemudian diubah kembali menjadi plaintext dengan menggunakan Metode Dekripsi, yang membalikkan kembali posisi ataupun isi dari data yang diterima dalam keadaan tidak dapat dibaca, kembali menjadi data yang mudah untuk dibaca, dengan menggunakan kunci dekripsi (Roharjo T, 2018).

Secara umum, berdasarkan kesamaan kunci algoritma kriptografi dapat dibedakan menjadi dua, yaitu algoritma simetrik dan algoritma asimetrik. Algoritma simetrik merupakan algoritma yang menggunakan kunci enkripsi sama dengan kunci dekripsi, algoritma ini disebut juga *single-key* algorithm. Contoh algoritma simetrik yaitu algoritma DES, AES, *Rijndael*, *Blowfish* dan lain-lain. Sedangkan algoritma asimetrik adalah suatu algoritma yang memiliki kunci enkripsi dan dekripsi tersendiri, yaitu menggunakan kunci publik dan kunci privat. Contoh algoritma asimetrik antara lain RSA, El Gamal dan Rabin (Roharjo T, 2018).

2. Caesar

Caesar Cipher adalah salah satu metode yang paling lama dan paling sederhana yang banyak digunakan. Metode ini ditemukan di abad ke19 oleh Julius Caesar. Dimana cara kerjanya melakukan pergeseran pada plaintext digantikan dengan huruf lain sesui berpakali jumlah pergeseran yang tetap pada posisi alfabet (Basuki A, 2016).



Gambar 1. Ilustrasi pergeseran 3 pada Caesar Cipher (Basuki A,2016)

Misal ingin melakukan enkripsi plaintext yang berisi TEKNIK ELEKTRO dengan kunci 3, maka huruf T diganti dengan huruf W, huruf E diganti dengan huruf H, huruf K diganti dengan huruf N dan seterusnya. Hasil ciphertext akan berisi WHNQLN HOHNWUR.

3. Blowfish

Algoritma *Blowfish* diciptakan oleh Bruce Schneier, seorang *Cryptanalyst* dan Presiden perusahaan Counterpane Internet Security, Inc (Perusahaan konsultan tentang kriptografi dan keamanan komputer) dan dipublikasikan tahun 1994. Dibuat untuk digunakan pada komputer yang mempunyai microposesor besar (32-bit keatas dengan cache data yang besar). Blowfish merupakan algoritma yang tidak dipatenkan dan tersedia secara gratis untuk berbagai macam kegunaan. Blowfish bekerja dengan membagi pesan menjadi blok-blok bit dengan ukuran sama panjang,yaitu 64-bit dengan panjang kunci

bervariasi yang mengenkripsi data dalam 8 byte blok. Pesan yang bukan merupakan kelipatan 8 byte akan ditambahkan bit-bit tambahan (padding)sehingga ukuran untuk tiap blok sama (Parasetiyo B, 2017).

Enkripsi blowfish adalah sebuah jaringan Feistel yang mempunyai 16 round. Inputnya adalah element data 64-bit (x). Untuk mengenkripsi x maka proses enkripsi bisa dilakukan dengan cara berikut(Parasetiyo B, 2017):

- Pertama bagi x dalam dua bagian 32-bit menghasil (XL) dan (XR).
- Setelah XL dan XR lanjutkan untuk iterasi(i) 1 sampai 16 maka

  $XL = XL \oplus Pi$

  $XR = F(XL) \oplus XR$

  Tukar XL dan XR , lanjutkan dari i =1 samai i= 16

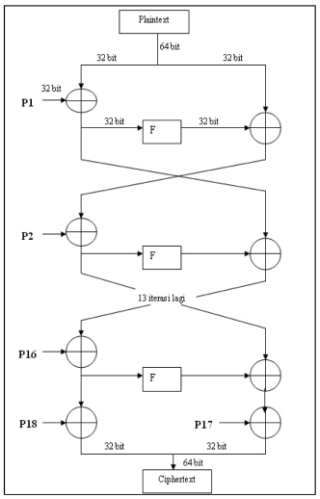
  Fungsi F adalah membagi XL menjadi empat bagian 8-bit: a,b,c dan d, maka dapat dirumuskan

  $$F(XL) = \left((S1, a + s2, b \bmod 2^{32}) \oplus S3, c\right) + S4, d \bmod 2^{32}$$
- Setelah iterasi ke-16, tukar XL dan XR lagi untuk melakukan membatalkan pertukaran terakhir.

  $XR = XL \oplus P17$

  $XL = XL \oplus P18$
- Terakhir, gabungkan kembali XL dan XR untuk mendapatkan *ciphertext (*hasil enkripsi*)*.

Cara enkripsi diatas juga bisa dijelaskan dalam blok diagram algoritma enkripsi *Blowfish*, yang ditunjukkan pada Gambar 2



Gambar 2.5 Blok diagram algoritma enkripsi *Blowfish*(Parasetiyo B, 2017).

Proses dekripsi memiliki langkah sama persis dengan proses enkripsi, hanya saja urutan Pbox digunakan dengan urutan terbalik.

4. AES (*Advanced Encryption Standar)*

Advanced Encryption Standard (AES) merupakan pemenang dalam sayembara pencarian pengganti algoritma DES yang dianggap sudah tidak aman lagi. National Institute of Standards and Technology (NIST) telah memilih system penyandian *Rijndael* yang dikembangkan oleh Joan Daemen dan Vincent Rijment sebagai system penyandian AES pada tahun 2000.

AES sampai saat ini masih dianggap aman untuk digunakan. Keamanan sistem AES salah satunya disebabkan oleh penggunaan kunci yang besar (128 *bit*, 192 *bit*, dan 256 *bit*) apabila dibandingkan dengan sistem DES yang hanya menggunakan 64 *bit*. Jadi *bruce attack* terhadap sistem AES 256 *bit* memiliki ruang kunci 2^{256} yang merupakan nilai yang sangat besar.

AES adalah system penyandian blok yang bersifat *non-Fiestel* karena menggunakan komponen yang selalu memiliki invers dengan panjang blok 128 *bit*. Kunci AES dapat memiliki panjang kunci 128, 192 dan 256 *bit*. AES menggunakan 5 unit ukuran data, yaitu: *bit, byte, word*, blok dan *state*. *Bit* merupakan satuan data terkecil, yaitu nilai digit sistem biner, *byte* berukuran 8 *bit*, *word* berukuran 4 *byte* (32 *bit*), blok berukuran 16 *byte* (128 *bit*), dan *state* adalah blok yang membentuk matriks *byte* berukuran 4x4 (Roharjo T, 2018).

5. Android

Android adalah sistem operasi untuk telepon seluler yang berbasiskan Linux. Android menyediakan platform terbuka bagi para pengembang untuk menciptakan aplikasi mereka sendiri sehingga dapat digunakan oleh bermacam peranti penggerak. Awalnya Google Inc. membeli Android Inc. pendatang baru yang membuat software (perangkat lunak) untuk telepon genggam. Kemudian untuk mengembangkan Android di bentuklah Open Handset Alliance yang merupakan gabungan dari 34 perusahaan peranti keras, peranti lunak dan telekomunikasi termasuk Google, HTC, Intel, Motorola, Qualcomm, TMobile, dan Nvidia (Defni, 2014).

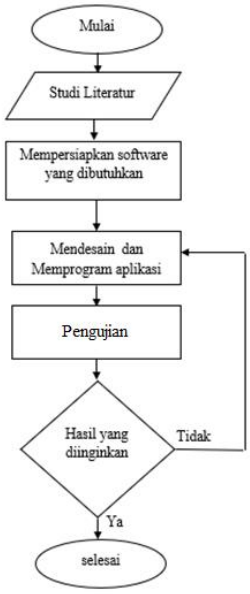
Sejak April 2009, versi Android dikembangkan dengan nama kode yang dinamai berdasarkan makanan pencuci mulut dan penganan manis. Masing-masing versi dirilis sesuai urutan alfabet. Berikut adalah rangkaian perjalanan android (Daveloper, 2018):

1. Android Beta (2007)
2. Android Versi 1.0 *Astro (*2008*)*
3. Android Versi 1.1 *Bender(*2009*)*
4. Android Versi 1.5 *Cupcake*(2009)
5. Android Versi 1.6 *Donut(*2009*)*
6. Android Versi 2.0/2.1 *Eclair*(2009)
7. Android Versi 2.2 *Froyo*(2010)
8. Android Versi 2.3 *Gingerbread*(2010)
9. Android Versi 3.0 *Honeycomb(*2011)
10. Android Versi 4.0 *ICS (2011)*
11. Android Versi 4.1-4.3 *Jelly Bean (2013)*
12. Android Versi 4.4 *KitKat(2013)*
13. Android Versi 5.0 *Lollipop*(2014)
14. Android Versi 6.0 Marshmallow (2015)
15. Android Versi 7.0 Nougat(2016)
16. Android Versi 8.0 Oreo(2017)
17. Android Versi 9.0 Pie(2018)

Untuk keamanan Android biasanya ada pada perangkat Android baru pada media *SandBox* yang diciptakan Google, dimana pada saat setiap *user* ingin menginstall aplikasi pada market maka akan muncul beberapa perizinan yang sebelumnya harus disetujui oleh *user* sebelum menginstall aplikasi tersebut pada perangkatnya.

METODE PENELITIAN

Metode perancangan aplikasi adalah dengan menggunakan *software* Android Studio.



Gambar 2. Alur Sistem Perancangan

Pada gambar 2 dijelaskan aliran kerja perancangan secara umum. Pada studi literatur yaitu mencari dan mempelajari teori yang terkait penelitian. Setelah itu dilanjutkan oleh mempersiapkan *software* yang dibutuhkan, disini *software* yang digunakan adalah android studio dan emulator android dengan sistem operasi android 5.0 atau diatasnya. Selanjutnya melakukan desainer atau membentuk tampilan yang diinginkan dan memprogram tampilan tersebut seperti yang diinginkan. Setelah program dimasukan dan selesai baru bisa dilakukan pengujian untuk enkripsi dan dekripsi teks. Jika ada error atau hasi yang diinginkan tidak tercapai maka proses akan kembali pada saat mendesain dan memprogram ulang. Jika hasil yang diinginkan telah tercapai maka aplikasi telah selesai.

Aplikasi yang dirancang hanya bisa melakukan enkripsi pesan teks dengan algoritma caesar, hasil caesar akan dienkripsi kembali dengan algoritma blowfist. Dan hasil blowfish akan dienkripsi lagi dengan algoritma aes yang merupakan hasil akhir dari aplikasi.

Untuk penggunaan dekripsi prose yang dilakukan hampir sama dengan proses dekripsi tetapi melakukannya dengan cara sebaliknya yaitu dengan mlakukan aes dahulu setelah itu blowfis dan terakhir baru caesar. Hasil caesar merupakan pesan teks semula yang belum tersandikan.

HASIL DAN PEMBAHASAN

Hasil dari aplikasi memiliki 4 tampilan utama yaitu: tampilan menu utama, tampilan enkripsi, tampilan dekripsi dan tampilan informasi..

1. Tampilan Menu awal

Tampilan menu utama merupakan tampilan awal saat aplikasi dibuka. Pada menu utama ini pengguna memiliki 4 pilihan button yaitu: button enkripsi, button dekripsi, button informasi, dan button keluar.

Gambar 3. Tampilan Menu Utama

Pada gambar 3 dilihat hasil tampilan menu utama aplikasi yang dirancang. Dalam tampilan tersebut terdapat 4 pilihan button yang memiliki fungsi:

- Button enkripsi yang akan memanggil tampilan enkripsi.
- Button dekripsi yang akan memanggil tampilan dekripsi.
- Button informasi yang akan memanggil tampilan informasi.
- Button keluar untuk keluar dari aplikasi.

2. Tampilan Enkripsi

Tampilan enkripsi merupakan sebuah tampilan yang akan terpanggil saat button enkripsi ditampilan menu awal dipilih.

Gambar 4. Tampilan Enkrip

Pada gambar 4.3 diperlihatkan tampilan enkripsi yang merupakan tampilan yang akan terpanggil saat button enkripsi pada menu utama dipilih. Pada tampilan enkripsi pesan akan diproses untuk disandikan. Dan pada tampilan ini memiliki beberapa edit teks, teks view dan button yang memiliki fungsi :

- Dua masukan edit teks yaitu masukan plain text yang merupakan pesan teks yang akan disandikan, masukan key yang merupakan kata kunci untuk pesan yang akan disandikan.
- Teks view disini adalah kluaran yang merupakan hasil pesan teks yang telah disandikan(cipher teks).
- Tiga button untuk memproses pesan, button enkripsi disini merupakan button untuk melakukan proses penyandian terhadap pesan teks diantaranya button enkripsi memilki fungsi menyadikan input plain teks dengan metode caesar. Button enkripsi blfs memilki fungsi menyadika hasil caesar dengan metode blowfish. Button enkripsi aes memilki fungsi menyadika hasil blowfish dengan metode aes.
- Button bagikan(share) untuk membagikan pesan yang telah tersandi melalui aplikasi sosial media yang tedapat pada smart phone pengguna.
- Button salin(copy) untuk menyalin pesan yang telah tersandi dan dapat dipaste kembali.
- Button simpan(save) untuk menyimpan pesan yang telah terandi pada perangkat pengguna dalam format .txt.
- Dua button untuk kembali diantaranya button home yang akan memanggil

tampilan menu utama. Button dekripsi untuk memanggil tampilan dekripsi.

3. Tampilan Dekripsi

Tampilan dekripsi merupakan sebuah tampilan yang akan terpanggil saat button dekripsi ditampilan menu awal dipilih.

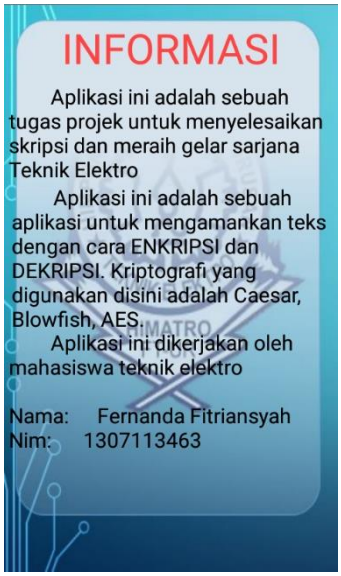
Gambar 5. Tampilan Enkrip

Gambar 5 Merupakan tampilan dekripsi yang merupakan tampilan yang akan terpanggil saat button dekripsi pada menu utama dipilih. Pada tampilan dekripsi pesan tersandi akan diproses untuk dikembalikan kedalam bentuk awal. Dan pada tampilan ini memiliki beberapa edit teks, teks view dan button yang memiliki fungsi :

- Dua masukan edit teks yaitu masukan cipher tekt yang merupakan pesan teks tersandi yang akan dikembalian seperti pesan asli, dan masukan key yang merupakan kata kunci untuk pesan yang disandikan agar pesan bisa dikambalikan seperti pesan asli.
- Teks view disini adalah keluaran yang merupakan pesan teks asli (plain text) yang telah dikembalikan dari pesan tersandi.
- Dua untuk masukan yaitu button load yang akan meload atau membuka pesan dalam forma .txt yang tersimpan pada perangkat pengguna. Dan button paste yang akan mempaste atau menempel pesan yang telah disalin.
- Tiga button untuk memprose pesan, button dekripsi disini merupakan button untuk melakukan proses pengembalian penyandian terhadap pesan teks tersandi yatitu button enkripsi aes memilki fungsi mengembalikan penyadian dari input cipher teks dengan metode aes. Button enkripsi blfs memilki fungsi mengembalikan penyadian dari hasil aes dengan metode blowfish. Button enkripsi memilki fungsi mengembalikan penyadian dari blowfish dengan metode caesar, sehingga menjadi pesan awal yang tidak tersandikan.
- Dua button untuk kembali diantaranya button home yang akan memanggil tampilan menu utama. Button enkripsi untuk memanggil tampilan enkripsi.

4. Tampilan Informasi

Tampilan informasi merupakan sebuah tampilan yang akan terpanggil saat button informasi ditampilan menu awal dipilih.



Gambar 6. Tampilan Informasi

Gambar 6 Merupakan tampilan informasi yang merupakan tampilan yang akan terpanggil saat button informasi pada menu utama dipilih. Pada tampilan informasi ini mencantumkan rincian mengenai aplikasi dan biodata mahasiswa yang mengerjakan.

Pengujian Aplikasi

Pengujian Aplikasi android untuk pengaman teks menggunakan kriptografi berlapis

dengan algoritma caesar, blowfish, dan AES dilakukan dengan cara menjalankan pada sistem operasi android dan melakukan proses enkripsi dan proses dekripsi.

Gambar 7. Proses Enkripsi

Gambar 7 memperlihatkan proses enkripsi. Proses enkripsi dapat dilakukan dengan mengisi masukan terlebih dahulu dari gambar kita melihat masukan plain teks adala “Teknik Elektro, Fakultas Tekni” dan kata kunci adalah “12345”. Prose enkripsi berlangsung dengan tiga lapis algoritma kriptografi yaitu caesar, blowfish dan AES. Proses caesar melakukan penggeseran pada plain teks sebanyak 3 kali penggeseran. Proses blowfis melakukan penyadian hasil caesar dengan membagi bit – bit pesan dan menggabungkan kembali setelah dilakukan pencampuran dengan kata sandi. AES melakukan proses berulang sebanyak 14 kali setelah itu barulah didapat hasil enkripsi. Maka hasil dari plainteks diatas adalah “ZppT0DyIG1KG0BhmsTUU5fA hckn5z+5zP/qyuqkLIgMp2squ7 qBj5yGQFiE6KwuI”.

Untuk memulai prose dekripsi maka pesan cipher teks harus diisi terlebih dahulu bisa dengan mengetikan manual, membuka file tersimpan, atau menempel pesan yang telah disalin. Setelah pesan terisi baru masukan kata kunci yang sama dengan sewaktu melakukan enkripsi. Contoh disini cipher teks dimasukan dengan membuka file yang telah tersimpan dan untuk kata kunci adalah “12345”.

Gambar 8. Proses Dekripsi

Gambar 8 memperlihatkan proses dekripsi. Pada gambar dapat kita lihat bahwasanya kata yang telah tersandi dikembalikan lagi kebentuk smula sebelum disandikan yaitu “Teknik Elektro, Fakultas Teknik”.

Setelah dilakukan pengujian maka didapat hasil enkripsi pada tabel 4.1 dan dekripsi pada tabel 4.2berikut:

Tabel 4.1 Hasil Pengujian Enkripsi

NO	Masukan plain teks	Kata kunci	Hasil Enkripsi
1	Teknik Elektro, Fakultas Teknik	12345	ZppT0DyIG1KG0BhmsTUU5fAhckn5z+5zP/qyuqkLIgMp2squ7qBj5yGQFiE6KwuI
2	aA bB cC dD eE fF gG hH iI jJ kK lL mM nN oO	abcd	bIakSC24GgX0ObxMqtpm+jRBRKsxX8KaEdmo5sJK49YmzRfJxX+V0F++Opt2mePfPwRZjujSOMFtVtq+0P46v+n5MOxiIpjQTjKuTqvAX2U=
3	!@#$%^&*()_+~{}[]<>/?.,	++--?	61DWGhX0Y16FkCJNGqXEw51FFeyAG7wF+WK1AO0VA5OHvF6dXS505gXUOfcPHue8
4	Fernanda.fitriansyah@gmail.com	Maret04	LaIJbPigf6huhyrCPAP5QfVNnel7p2+XEZiVVRzkQqcewX1V7TUiwj1zNX457M31
5	NIM: 1307113463	1995	lYyuppOyApSBjutZzBlgJozHSqb/s0JSAzkZJDYXlFw=

Tabel 4.2 Hasil Pengujian dekkripsi

NO	Masukan cipher teks	Kataku nci	Hasil Dekripsi	Kesalahan
1	ZppT0DyIG1KG0BhmsTUU5fAhckn 5z+5zP/qyuqkLIgMp2squ7qBj5yG QFiE6KwuI	12345	Teknik Elektro, Fakultas Teknik	Tidak ada
2	bIakSC24GgX0ObxMqtpm+ jRBRKsxX8KaEdmo5sJK49YmzRf JxX+V0F++Opt2mePfPwRZjujSO MFtVtq+0P46v+n5MOxiIpjQTjKu TqvAX2U=	abcd	aA bB cC dD eE fF gG hH iI jJ kK lL mM nN oO	Tidak ada
3	61DWGhX0Y16FkCJNGqXEw51F FeyAG7wF+WK1AO0VA5OHvF6 dXS505gXUOfcPHue8	+-?	!@#$%^ &*()_+~{ }[]<>/?.,	Tidak ada
4	LaIJbPigf6huhyrCPAP5QfVNnel7p 2+XEZiVVRzkQqcewX1V7TUiwj 1zNX457M31	Maret04	Fernanda. fitriansyah@gmail. com	Tidak ada
5	lYyuppOyApSBjutZzBlgJozHSqb/s 0JSAzkZJDYXlFw=	1995	NIM: 1307113463	Tidak ada

Pada tabel 4.1 diperlihatkan hasil enkripsi dan tabel 4.2 diperlihatkan hasil dekripsi. Enkripsi merupakan penyandian dan dekripsi merupakan pengembalian. Dari dua tabel tersebut dapat dilihat bahwa hasil teks awal yang tersandi dapat dengan aman dikembalikan kedalam teks semula seperti sedia kala tampa kehilangan atau kekurangan sedikitpun. Pada proses dekripsi tidak memiliki kesalah, dilihat dari dekripsi pesan yang telah tersandi berhasil dikembalikan kedalam bentuk yang sama dengan teks asli baik itu huruf kapital, angka, dan tanda baca dapat dienkripsi dan dekripsi secara sempurna. Jadi setelah melihat hasil tersebut dapat dibuktikan bahwa aplikasih telah berjalan dengan semestinya.

KESIMPULAN

Ada beberapa kesimpulan yang diperoleh dari hasil aplikasi android pengaman teks menggunakan kriptografi berlapis dengan algoritma Caesar, Blowfish dan AES, diantaranya adalah sebagai berikut:

1. Aplikasi android pengaman teks yang rancang berhasil digunakan dan dijalankan pada sistem operasi android 5.0 (lollipop) keatas untuk versi dibawahnya aplikasi akan error saat diinstal.
2. Pengujian hasil enkripsi pada aplikasi android pengaman teks yang dirancang berhasil melakukan enkripsi tiga lapis dan menghasilkan teks rahasiah.
3. Pengujian hasil dekripsi pada aplikasi android pengaman teks yang dirancang berhasil mengembalikan pesan yang tersandi kembali kebentuk semula saperti sebelum disandikan.
4. Pengujian hasil enkripsi pada aplikasi android pengaman teks yang dirancang hanya bisa didekripsi dengan aplikasi yang sama, tidak akan bisa didekripsi dengan aplikasi lain kecuali dengan koding android studio yang sama.
5. Pengujian hasil enkripsi dan dekripsi pada aplikasi android pengaman teks yang dirancang dapat melakukan enkripsi dan dekripsi dengan berbagai plainteks seperti berbagi huruf kapital, angka, dan tanda baca dapat terenkripsi dan terdekripsi tampa ada kesalahan.

DAFTAR PUSTAKA

Basuki. A., Upik. P., Restu. H., 2016. Perancangan Aplikasi Kriptografi Berlapis Menggunakan Algoritma Caesar, Transposisi, Vigenere, Dan Blok Chiper Berbasis Mobile. Seminar Nasional Teknologi Informasi dan Multimedia *ISSN : 2302-3805*. Yogyakarta

Defni, Indri. R. (2014). Enkripsi Sms (Short Message Service) Pada Telepon Selular Berbasis Android Dengan Metode Rc6. Jurnal Momentum Vol.16 No.1. Februari 2014 ISSN : 1693-752X. Padang.

Developer. A., 2018. https://developer.android.com /studio .

Prasetiyo. B., Muslim. M.A., Susanto. H., (2017). Penerapan Kriptografi Algoritma Blowfish pada Pengamanan Pesan Data Teks. *Techno.COM*, *16*(4), 358–366.

Roharjo, T., 2018. Skripsi thesis: *Aplikasi* Pengamanan Pesan Teks Menggunakan RC6 dan AES Berbasis Android, *Yogyakarta Universitas Mercu Buana.*