JEJARING (Jurnal Teknologi dan Manajemen Informatika) p-ISSN : 2527-3930, e-ISSN : 2614-5448
Volume 5 Nomor 2, November 2020 https://journal.uniku.ac.id/index.php/jejaring

IMPLEMENTASI ALGORITMA AES 128 BIT SEBAGAI PENGAMAN TEKS DI APLIKASI NOTE BERBASIS ANDROID

Aji Permana[1], Elan jaelani[2]
[1,2]Universitas Kuningan
Jl.Cut Nyak Dhien no.36A kuningan
Aji.permana@uniku.ac.id[1], elan.jaelani@gmail.com[2]

***Abstrak** : Disemua bidang kehidupan dari semua kalangan memanfaatkan teknologi untuk pertukaran informasi. Salah satu media yang dimiliki oleh banyak orang adalah perangkat mobile, seperti telephone genggang dan computer tablet. Banyak orang yang sudah menggunakan perangkat mobile untuk fungsi pertukaran informasi, keamanan dan kerahasiaan merupakan aspek penting yang dibutuhkan dalam proses pertukarannpesan atau informasi. Ada berbagai macam pengamanan teks di aplikasi note, salah satunya dengan cara mengenkripsi teks catatan tersebut. Enkripsi adalah proses untuk menyamarkan isi dari teks catatan, sehingga orang yang tidak berkepentingan atau bahkan penyadap tidak bisa mengetahui isi dari teks catatan tersebut. Proses enkripsi membuat teks catatan yang tersamarkan isinya namun masih berbentuk tulisan oleh karena itu walau teks catatan itu telah di enkripsi tetap akan menimbulkan kecurigaan sehingga dapat memicu orang yang ingin tau makna teks catatan untuk mencari makna sebenarnya dari teks catatan tersebut. Karena sekarang ini banyak sekali kejahatan yang terjadi dalam aspek keamanan informasi, berbagai macam teknik keamanan telah dikembangkan untuk melindungi dan menjaga kerahasiaan pesan dari orang-orang yang tidak bertanggungjawab, salah satunya yaitu teknik kriptografi. Kriptografi adalah teknik menyembunyikan sehingga orang yang tidak berkepentingan atau bahkan penyadap tidak bisa mengetahui isi dari teks catatan tersebut. Peneliti ini membahas tentang implementasi algoritma aes 128 bit sebagai pengaman teks dan algoritma yang digunakan adalah advance encryption standard. Peneliti ini bertujuan untuk membangun aplikasi yang dapat mengenkripsi teks dan mendeskripsi teks yang diimplementasikan pada perangkat mobile android. Aplikasi ini dibuat dengan menggunakan android studio. Berdasarkan penggunaan aplikasi didapat hasil bahwa teks yang di enkripsi dengan algoritma advanced encryption standard pada perangkat mobile android dapat dideskripsikan kembali.*

***Kata Kunci :** Kriptografi, Algoritma AES 128 bit, Enkripsi, Android.*

***Abstract** : In all spheres of life from all circles utilizing technology to exchange information. One of the media owned by a lot of people are mobile device, such as mobile phones and tablet computers, many people already use mobile devices for information exchange of messages of information. There are various kind of safety text in the note application, one of them by way of encrypting the note text. Encryption is the process of disguising the contents of the note text, so that unauthorized persons or even hacker can not know the contents of the note text. The encryption process create text notes in disguise their contents but still a form of writing therefore, although its text has been encrypted notes will still arouse suspicion so that occur in the aspects of information security, the security of various technique. Cryptography is a technique to hide so that people who are not interested or even eavesdroppers can not know the contents of the note text. This study discusses the implementation of Aes 128 bit algorithm for securing the text and the algorithm used is advanced encryption standard. This study aims to build application that can encrypt text and describe text which implemented on mobile devices android. The application is built using android studio. Based on the use of the application showed that text is encrypted with advanced encryption standard algorithm on mobile devices android can be described back in.*

***Keywords :** Cryptography, AES 128 bit algorithm, encryption, android.*

1.1 Latar Belakang

Perkembangan Teknologi komputer dan telekomunikasi yang cukup pesat masa kini berpengaruh pada penggunaan informasi. Sehingga manusia termotivasi untuk membuat inovasi baru yang memudahkan kita dalam menyelesaikan suatu masalah. Handphone adalah salah satu inovasi manusia untuk membantu dalam penyelesaian masalah tersebut. Seiring dengan perkembangan dan kemudahan dari teknologi-teknologi tersebut, banyak informasi baru bermunculan, baik yang layak disebarluaskan atau dirahasiakan. Namun keamanan dari informasi tersebut belum terjamin. Untuk

p-ISSN : 2527-3930, e-ISSN : 2614-5448
https://journal.uniku.ac.id/index.php/jejaring

mengamankan informasi tersebut, digunakanlah ilmu Kriptografi.(Joko Tri Susilo, 2014:1-2)

Ilmu kriptografi sangat cepat berkembang, Tidak hanya bisa digunakan di komputer, tapi juga digunakan di beberapa perangkat dan sistem operasi, seperti Blackberry, Android, iPhone dan masih banyak lagi. Terutama disini adalah Android, sistem operasi yang dikembangkan oleh Google ini mengalami peningkatan jumlah pengguna dan tentu saja perangkat yang menggunakan sistem operasi ini menjamur dan sangat laris di pasaran.

Ada berbagai macam pengaman teks di aplikasi note, salah satunya dengan cara mengenkripsi teks catatan tersebut. Enkripsi adalah proses untuk menyamarkan isi dari teks catatan, sehingga orang yang tidak berkepentingan atau bahkan penyadap tidak bisa mengetahui isi dari teks catatan tersebut. Proses enkripsi membuat teks catatan yang tersamarkan isinya namun masih berbentuk tulisan oleh karena itu walau teks catatan itu telah di enkripsi tetap akan menimbulkan kecurigaan sehingga dapat memicu orang yang ingin tau makna teks catatn untuk mencari makna sebenarnya dari teks catatan tersebut.

Dunia kriptografi masa kini semakin dipermudah dengan adanya aplikasi kriptografi dimana pengguna tidak lagi membutuhkan waktu yang lama, rumit dan berpotensi menimbulkan kesalahan, dengan menggunakan algoritma yang ada, pengguna dapat dengan mudah mengenkripsi sebuah teks hanya dengan sekali klik. Sayangnya jumlah aplikasi kriptografi yang ada saat ini sangat minim, terutama di sistem operasi android. (Noni Endriani, 2014:1-2)

Oleh karena itu penulis mencoba merancang sebuah aplikasi kriptografi untuk
telepon selular berbasis Android dengan algoritma enkripsi yang kuat.

Algoritma yang digunakan di aplikasi ini menggunakan basis perhitungan matematika sehingga hasil dari teks yang terenkripsi cukup kuat, aplikasi ini sangat berguna untuk mempermudah penyandian suatu informasi tanpa harus membutuhkan waktu yang lama, rumit dan memahami algoritma ataupun cara kerjanya. Oleh karena itu, penulis mengambil judul **" IMPLEMENTASI ALGORITMA AES 128 BIT SEBAGAI PENGAMAN TEKS DI APLIKASI NOTE BERBASIS ANDROID".**

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang masalah diatas, adapun identifikasi masalah yang akan dibahas dalam skripsi ini adalah :

1. Bagaimana merancang dan mengamankan teks di aplikasi note berbasis android?
2. Bagaimana algoritma AES 128 Bit dapat mengamankan isi teks di aplikasi note?

1.3 Batasan Masalah

Adapun batasan masalah dalam penelitian ini adalah :

1. Aplikasi ini ditujukan untuk pengguna dengan sistem operasi Android minimal Versi 2.3 (Gingerbread).
2. Algoritma yang digunakan untuk mengamankan aplikasi note terhadap isi teks adalah algoritma AES 128 Bit yang meliputi tahapan, AddRoundKey, SubByte, ShiftRows, MixColoums, ChiperText.
3. Input Password berupa teks, angka, symbol, atau kombinasi.
4. Minimal Password 6 Digit dan Maximum Password 16 Digit.
5. Software yang digunakan untuk membuat aplikasi adalah Java dengan IDE Eclips.

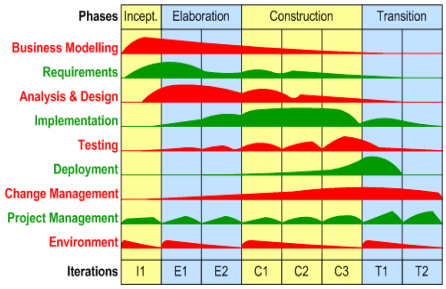
1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah :

1. Dapat menjaga keamanan teks dengan mengimplementasikan android dan algoritma AES.
2. Untuk mengimplementasikan algoritma AES 128 Bit.

1.5 Metode Penelitian

Metodologi penelitian pengembangan perangkat lunak yang digunakan oleh penulis dalam penelitian ini adalah pendekatan *Rational Unified Proses* (RUP).



1.6 Metode Pengumpulan Data

Teknik pengumpulan data Mencari dan mengumpulkan literatur-literatur ilmiah yang diambil selain dari buku-buku yang ada, dan juga mencari dari internet ataupun melalui perkumpulan surat-surat elektronik yang terkait dengan permasalahan yang dihadapi dalam penyusunan penelitian.

2. LANDASAN TEORI

2.1 Pengertian Sistem

Sistem adalah suatu gabungan dari beberapa komponen yang saling berinteraksi untuk mencapai cuatu tujuan tertentu.

p-ISSN : 2527-3930, e-ISSN : 2614-5448
https://journal.uniku.ac.id/index.php/jejaring

2.2 Aplikasi

Aplikasi merupakan penerapan, menyimpan sesuatu hal, data, permasalahan, pekerjaan kedalam suatu sarana atau media yang dapat digunakan untuk menerapkan atau mengimplementasikan hal atau permasalahan yang ada sehingga berubah menjadi bentuk baru tanpa menghilangkan nilai-nilai dasar dari hal data, permasalahan, pekerjaan itu sendiri. (Jogiyanto, 2005)

2.3 Sejarah Android

Android merupakan perangkat lunak (software) sistem operasi yang memakai basis kode komputer yang dapat didistribusikan secara terbuka atau open source sehingga pengguna bisa membuat aplikasi baru didalamnya.

2.4 Pengertian Kriptografi

Kriptografi (*cryptography*) berasal dari Bahasa Yunani, yaitu dari kata *crypto* dan *graphia* yang berate 'penulisan rahasia'. Kriptografi adalah ilmu ataupun seni yang mempelajari bagaimana membuat suatu pesan yang dikirim oleh pengirim dapat disampaikan kepada penerima dengan aman (Schneier, 1996).

2.5 Proses Enkripsi Algoritma AES Rijndael

Proses enkripsi algoritma AES terdiri atas empat jenis transformasi bytes, yaitu subBytes, ShiftRows, MixColoumns, dan AddRoundKey. Pada awal proses enkripsi, input yang telah dikopikan kedalam state akan mengalami transportasi byte AddRoundKey.

2.6 Algoritma Advanced Encryption Standard(AES)

Vincent Rijmen dan Jhon Daemen asal belgia merupakan pemenang kontes algoritma kriptografi pengganti DES, yang diadakan oleh National Institutes of Standards and Technology (NIST) milik pemerintah amerika serikat pada 26 november 2001, yang diberi nama Rijndael (Munir, 2006). Algoritma rijndael inilah yang kemudian dikenal dengan Advanced Encryption Standard(AES). Dalam algoritma AES terdapat 4 proses yang dilakukan saat melakukan enkripsi yaitu **Subbytes, ShiftRows, MixColumns,** dan **AddRoundKey**. Berikut gambaran perhitungan pada algoritma AES:
Plaintext (hexadesimal) = 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF.
Kunci (hexadesimal) = 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F.

3. ANALISIS DAN PERANCANGAN

3.1 Analisis Masalah

Keamanan dan kerahasiaan merupakan aspek penting yang dibutuhkan dalam proses pertukaran pesan atau informasi. Berbagai macam teknik keamanan telah dikembangkan untuk melindungi dan menjaga kerahasiaan catatan agar terhindar dari orang yang tidak berhak, salah satunya yaitu teknik Kriptograpi dengan mengeknkripsi catatan kita.

3.2 Perhitungan Algoritma AES 128 Bit

Enkripsi AES 128 Bit AES merupakan sistem penyandian blok yang bersifat non-Fiestel karena AES menggunakan komponen yang selalu memiliki invers dengan panjang blok 128 bit. Kunci AES dapat memiliki panjang kunci bit 128 bit, 192 bit, dan 256 bit.

Dalam algoritma AES terdapat 4 proses yang dilakukan saat melakukan enkripsi yaitu **Subbytes, ShiftRows, MixColumns,** dan **AddRoundKey**. Berikut gambaran perhitungan pada algoritma AES:
Plaintext (hexadesimal) = 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF.
Kunci (hexadesimal) = 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F.

Yang perlu diperhatkan dalam perhitungan MixColumn ketika $s'_{0,c}$, $s'_{1,c}$, $s'_{2,c}$, $s'_{3,c}$ memiliki hasil lebih dari 0xFF maka dimoduluskan dengan 0x11B.

Perkalian (•)

1. $s'_{0,c}$ = ([02]•63) ⊕ ([03]•53) ⊕ E0 ⊕ 8C
   '02' • '63' = $(x)\cdot(x^6 + x^5 + x + 1)$
   $= x^7 + x^6 + x^2 + x$
   = 11000110
   '03' • '53' = $(x + 1)\cdot(x^6 + x^4 + x + 1)$
   $= (x^7 + x^5 + x^2 + x) + (x^6 + x^4 + x + 1)$
   $= x^7 + x^6 + x^5 + x^4 + x^2 + 1$
   = 11110101
   '01' • 'E0' = E0
   = 11100000
   '01' • '8C' = 8C
   = 10001100
2. $s'_{1,c}$ = 63 ⊕ ([02]•53) ⊕ ([03]•E0) ⊕ 8C
   '01' • '63' = 63
   = 01100011
   '02' • '53' = $(x)\cdot(x^6 + x^4 + x + 1)$
   $= x^7 + x^5 + x^2 + x$
   = 10100110
   '03' • 'E0' = $(x + 1)\cdot(x^7 + x^6 + x^5)$

p-ISSN : 2527-3930, e-ISSN : 2614-5448
https://journal.uniku.ac.id/index.php/jejaring

$= (x^8 + x^7 + x^6)+(x^7 + x^6 + x^5)$
$= (x^8 + x^5) \bmod (x^8 + x^4 + x^3 + x + 1)$
$= x^5 + x^4 + x^3 + x + 1$
$= 00111011$

‘01’ • ‘8C’ = 8C
$= 10001100$

3. $s'_{2,c} = 63 \oplus 53 \oplus ([02]\bullet E0) \oplus ([03]\bullet 8C)$

‘01’ • ‘63’ = 63
$= 01100011$
‘01’ • ‘53’ = 53
$= 01010011$
‘02’ • ‘E0’ = $(x)\cdot(x^7 + x^6 + x^5)$
$= x^8 + x^7 + x^6$
$= (x^8 + x^7 + x^6) \bmod (x^8 + x^4 + x^3 + x + 1)$
$= x^7 + x^6 + x^4 + x^3 + x + 1$
$= 11011011$
‘03’ • ‘8C’ = $(x + 1)\cdot(x^7 + x^3 + x^2)$
$= (x^8 + x^4 + x^3)+(x^7 + x^3 + x^2)$
$= x^8 + x^7 + x^4 + x^2$
$= (x^8 + x^7 + x^4 + x^2) \bmod (x^8 + x^4 + x^3 + x + 1)$
$= x^7 + x^3 + x^2 + x + 1$
$= 10001111$

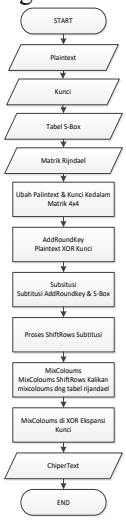
4. $s'_{3,c} = ([03]\bullet 63) \oplus 53 \oplus E0 \oplus ([02]\bullet 8C)$

‘03’ • ‘63’ = $(x + 1)\cdot(x^6 + x^5 + x + 1)$
$= (x^7 + x^6 + x^2 + x)+(x^6 + x^5 + x + 1)$
$= x^7 + x^5 + x^2 + 1$
$= 10100101$
‘01’ • ‘53’ = 53
$= 01010011$
‘01’ • ‘E0’ = E0
$= 11100000$
‘02’ • ‘8C’ = $(x)\cdot(x^7 + x^3 + x^2)$
$= x^8 + x^4 + x^3$
$= (x^8 + x^4 + x^3) \bmod (x^8 + x^4 + x^3 + x + 1)$
$= x + 1$
$= 00000011$

Operasi SubBytes, ShiftRows, MixColumns, dan AddRoundKey dilakukan perulangan sebanyak 10 kali sesuai dengan kunci yang digunakan yaitu 128 bit. Hasil setiap ronde disertakan dalam lampiran, dan hasil akhir yang didapatkan adalah:

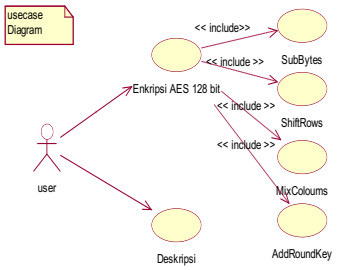
ChiperText = 69 C4 E0 D8 6A 7B 04 30 D8 CD B7 80 70 B4 C5 5A.

1 Flowchart Algoritma AES 128 Bit



3.3 Usecase Diagram

Use Case diagram menggambarkan fungsionalitas yang diharapkan dari sebuah sistem, sebuah use case merepresentasikan sebuah interaksi antara aktor sengan sistem. Use Case Diagram pada penelitian ini adalah sebagai berikut :

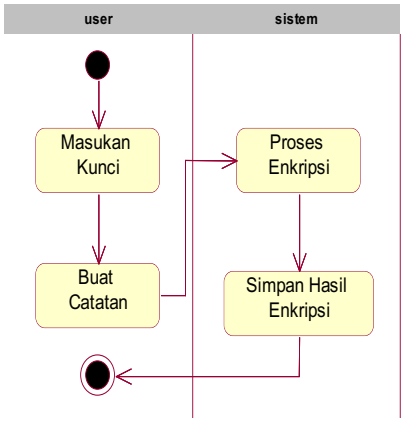


3.4 Activity Diagram

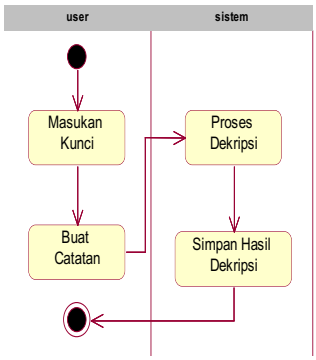
Activity diagram ini menggambarkan berbagai alir aktifitas dalam system yang sedang dirancang. Berikut ini akan digambarkan aktivitas-aktivitas Sistem Enkripsi.

p-ISSN : 2527-3930, e-ISSN : 2614-5448
https://journal.uniku.ac.id/index.php/jejaring

1. Activity Diagram Sistem Enkripsi

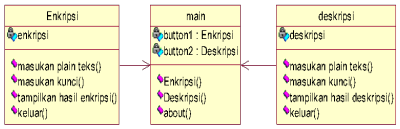


1. Activity diagram Sistem deskripsi sebagai berikut :



3.5 Class Diagram

Class diagram merupakan objek-objek yang mempunyai struktur umum, behavior umum, relasi umum, dan semantic umum. Class diagram ini digunakan untuk menampilkan beberapa kelas serta paket-paket yang ada pada sistem atau perangkat lunak yang sedang kita gunakan. Class diagram untuk aplikasi ini adalah sebagai berikut :



3.6 Sequence Diagram

Sequence diagram mendokumentasikan komunikasi/interaksi antara kelas-kelas. Diagram ini menunjukan sejumlah objek dan message (pesan) yang diletakan antara objek-objek didalam use case.

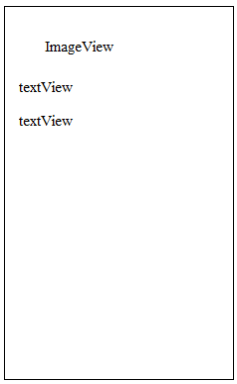
3.7 Perancangan Interface/Antarmuka

Perancangan antarmuka merupakan suatu langkah dalam membuat pebuah program aplikasi. Program dirancang sesuai dengan hasil pengamatan. Perancangan program dibuat meliputi beberapa perancangan diantaranya perancangan input dan perancangan output. Perancangan input output merupakan tahapan untuk membuat tampilan atau desain dari aplikasi yang akan dibuat. Perancangan tersebut sangat penting untuk memenuhi kriteria yang mudah digunakan, menarik dan user friendly bagi pemakai. Oleh karena itu dibutuhkan perancangan input output.

3.8 Perancangan Input

Perancangan input merupakan suatu rancangan masukan data yang akan diproses oleh aplikasi yang kemudian menghasilkan keluaran berupa hasil data yang dienkripsi (Kriptografi) yang langsung tersimpan dalam komputer. Berikut ini merupakan perancangan input aplikasi Kriptografi :

Halaman Utama Aplikasi



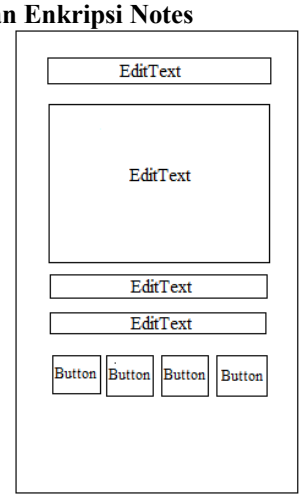
p-ISSN : 2527-3930, e-ISSN : 2614-5448
https://journal.uniku.ac.id/index.php/jejaring

Merupakan halaman awal pada aplikasi notes, pada halaman awal akan ada informasi aplikasi,logo aplikasi dan nama aplikasi. untuk spesifikasi komponen

No	Komponen	Keterangan
1	ImageView	Untuk Logo Aplikasi
2	TextView	Untuk Nama Aplikasi
3	TextView	Untuk Judul Aplikasi yg dibuat

rancangan form halaman utama dapat dilihat pada tabel 3.9*Spesifikasi Halaman Aplikasi*

1. Halaman Enkripsi Notes

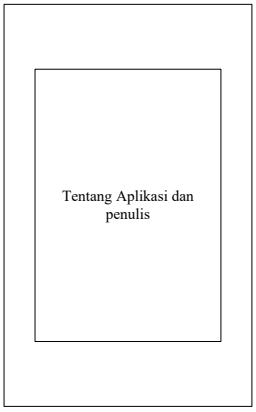


merupakan form untuk memasukan kunci dan membuat catatan, untuk spesifikasi komponen dalam rancangan form *enkripsi* dapat dilihat pada tabel 3.8

Tabel 3.6 Spesifikasi Halaman Enkripsi & Dekripsi

No	Komponen	Keterangan
1	EditText1	Nama Kunci
2	EditText2	Catatan yang akan dibuat oleh pengguna
3	EditText3	Hasil Enkripsi
4	EditText4	Hasil Deskripsi
5	Button1	Save untuk menyimpan hasil enkripsi
6	Button2	Encrypt berfungsi untuk mengenkripsi catatan
7	Button3	Decrypt untuk mendekrip catatan yang telah di enkripsi
8	Button4	Load untuk menampilkan data yang telah disimpan di directori.

2. Halaman Tentang Aplikasi dan Pembuat Aplikasi



Gambar 3.11 Halaman Tentang Aplikasi dan Pembuat
Keterangan :

1. Menampilkan informasi tentang aplikasi dan pembuat aplikasi.

4 IMPLEMENTASI DAN PENGUJIAN

4.1 Implementasi Sistem

Implementasi sistem adalah tahap penerapan hasil perancangan yang prosesnya diuraikan pada bab sebelumnya. Implementasi yang dilakukan antara lain adalah menerapkan perancangan antar muka ke dalam

p-ISSN : 2527-3930, e-ISSN : 2614-5448
https://journal.uniku.ac.id/index.php/jejaring

bentuk tampilan dalam aplikasi Android, pembuatan kode program dan sebagainya.

4.2 Spesifikasi Perangkat Lunak

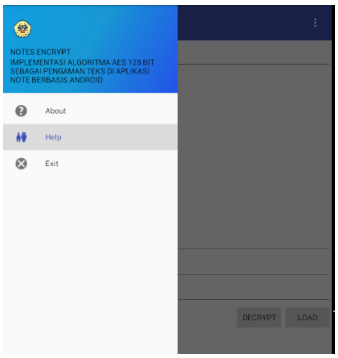
1. Sistem Operasi Windows 8.1 Pro 32bit
2. Minimal Sistem Operasi Android versi 2.3 (Gingerbread)
3. Android Studio versi 2.1.2
4. Tools Oracle JDK dan JRE versi 8u66
5. Perancangan Sistem Rational Rose 2002

4.3 Spesifikasi Perangkat Keras

1. Genymotion Versi 4.0
2. CPU 1.3 GHz
3. Memory 4 GB

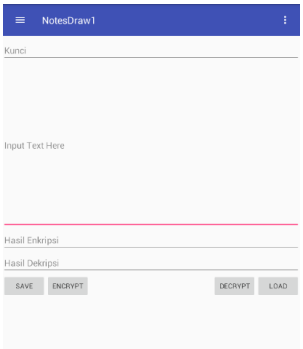
4.4 Tampilan Halaman Utama

Menampilkan halaman utama berfungsi sebagai pembuka aplikasi Enkripsi, tujuannya agar tidak langsung masuk ke menu aplikasi.



1. Tampilan Menu Aplikasi

Gambar 4.2 merupakan tampilan menu dalam aplikasi enkripsi dan terdapat beberapa tombol.

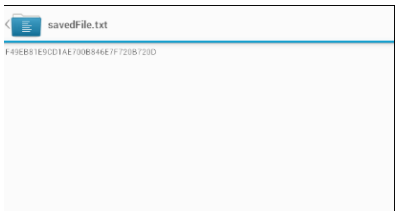


4.5 Tampilan Menu Enkripsi

Pada menu ini menampilkan beberapa fungsi untuk memulai proses enkripsi pesan. input kata kunci sebagai kata kunci saat proses enkripsi, input pesan yang akan dienkripsi, dan tombol encrypt untuk memulai proses enkripsi catatan, tombol descrypt untuk mendekripsi hasil dari proses enkripsi, tombol save untuk menyimpan hasil catatan yang telah di enkripsi, dan tombol load untuk membaca catatan yang telah tersimpan dan terenkripsi.

4.6 Tampilan Menu Enkripsi

Pada tampilan ini terdapat beberapa fungsi yang hampir sama dengan proses enkripsi, button save berfungsi untuk menyimpan hasil dari proses enkripsi berbentuk txt, input kata kunci berfungsi untuk memasukan kunci, dan tombol encrypt untuk mengenkripsi catatan, button descrypt untuk menampilkan catatan yang telah di enkripsi, kemudian terakhir button load untuk menampilkan hasil enkripsi yang telah disimpan.



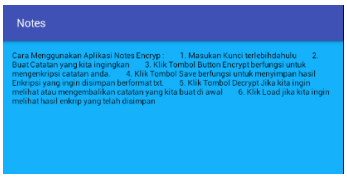
4.7 Tampilan Tentang Aplikasi

Ketika user memilih menu Bantuan pada menu utama makan akan menampilkan informasi tentang bantuan menggunakan aplikasi steganografi ini.

p-ISSN : 2527-3930, e-ISSN : 2614-5448
https://journal.uniku.ac.id/index.php/jejaring

4.8 Tampilan Bantuan Penggunaan Aplikasi

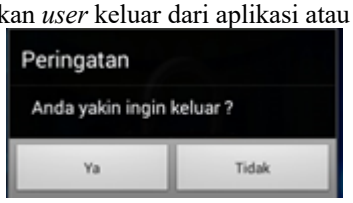
Ketika user memilih menu Bantuan pada menu utama makan akan menampilkan informasi tentang bantuan menggunakan aplikasi steganografi ini.



Gambar 4.6 Tampilan Bantuan Penggunaan Aplikasi

4.9 Tampilan Pesan Keluar dari Aplikasi

Ketika *user* menutup aplikasinya baik disengaja maupun tidak maka akan menampilkan pesan keluar dari aplikasi untuk menyakinkan *user* keluar dari aplikasi atau tidak.



Gambar 4.7 Tampilan Pesan Keluar dari Aplikasi

4.10 Pengujian Perangkat Lunak

Pengujian dilakukan untuk menentukan kesalahan atau kekurangan pada perangkat lunak yang diuji. Pengujian bermaksud untuk mengetahui perangkat lunak yang dibangun sudah sesuai dengan perancangan yang dibuat dan memenuhi kebutuhan pengguna.
Pengujian yang dilakukan yaitu pengujian *black box* dan *white box*. Pengujian *black box* digunakan untuk mengetahui kesalahan proses secara fungsional sedangkan *white box* digunakan untuk menguji performa dari metode yang digunakan. Pengujian *black box* berfokus pada persyaratan fungsional perangkat lunak sedangkan *white box* berfokus pada algoritma yang digunakan.

4.11 Pengujian Blackbox

Pengujian blackbox merupakan pengujian yang berfokus pada spesifikasi fungsional dari perangkat lunak, tester dapat mendefinisikan kumpulan kondisi input dan melakukan pengetesan pada spesifikasi fungsional program.
Pengujian fungsionalitas aplikasi dilakukan pada perangkat emulator Genymotion dengan sistem operasi Android 4.1 (*Kitkat*). Fungsi-fungsi yang diuji dapat dilihat pada tabel dibawah ini.

4.12 Pengujian White Box

Pengujian *white box* meupakan pengujian internal dari perangkat lunak yang meliputi kode-kode program sehingga dapat dianalisis kesalahan-kesalahan yang terjadi pada penulisan kode program.
Berikut ini adalah kasus menguji perangkat lunak yang telah dibangun dengan menggunakan pengujian white box, terdapat dua pengujian white box yaitu proses pengujian Encrypt dan proses pengujian Descrypt.
Berikut adalah pengujian white box untuk proses pengujian Encrypt pada perangkat lunak ini :

4.13 Hasil Pengujian Perangkat Lunak

Berdasarkan hasil dari pengujian di atas serta implementasi algoritma yang digunakan dalam enkripsi teks dapat dikategorikan penulis telah sesuai dengan yang diharapkan yakni menenkripsi sebuah teks dan dapat deskripsi kembali.
Oleh karena itu, program kriptografi yang dibuat dengan tujuan untuk menenkripsi teks telah berhasil sehingga keberadaan teks ini tidak bisa dibaca oleh semua orang.

5 PENUTUP

5.1 Kesimpulan

Berdasarkan penelitian yang sudah dilakukan oleh penulis, dapat ditarik kesimpulan sebagai berikut :

1. Aplikasi Notes Encrypt berbasis Android ini menggunakan algoritma AES 128 Bit yang dapat diimplementasikan kedalam aplikasi
2. Dapat Menjaga keamanan teks dengan mengimplementasikan android dan algoritma AES 128 bit.

3. Aplikasi Kriptografi dengan menggunakan Algoritma AES 128 bit ini ketika akan mengenkripsi suatu teks memerlukan suatu kata kunci, ketika kata kunci yang dimasukan benar maka pesan dapat dilihat sesuai pesan asli yang sebelumnya di enkripsi, namun ketika kata kunci salah maka atau kurang dari 6 digit pesan tidak dapat di enkripsi.
4. Aplikasi Kriptografi dengan menggunakan Algoritma AES 128 bit dapat mengamankan teks dan menyimpan di directori HP berektensi file .txt.

5.2 lSaran

Adapun saran yang direkomendasikan untuk mengembangkan penelitian ini adalah sebagai berikut :

1. Pada aplikasi ini memiliki keterbatasan yaitu media yang digunakan untuk mengenkripsi sebuah teks yang bertipe file txt, dan teks yang dienkripsi hanya berupa teks, penulis berharap pada pengujian selanjutnya dapat di kembangkan kembali dengan tidak membatasi file txt yang digunakan dan teks yang di enkripsi bias berupa dokumen seperti .doc, .pdf, dan sebagainya.
2. Dibuatkan juga untuk platform yang lain, seperti Blackberry OS, iOS, ataupun yang lainnya.

DAFTAR PUSTAKA

Jogiyanto. 2005. *Analisis dan Desain Sistem Informasi*. Yogyakarta: Penerbit Andi.

Joko Widodo. 2010. *Analisis Kebijakan Publik, Konsep dan Aplikasi Analisis Kebijakan Publik.* Malang: Bayu Media.

Kurniawan, Yusuf, (2004), *Kriptografi Keamanan Internet dan Jaringan Komunikasi*, Bandung : Penerbit Informatika Bandung.

Krismiaji, 2010. *Sistem Informasi Akuntansi*, UMP YKPN, Yogyakarta.

Muhammad Galih. *RUP (Rational Unified Process)*. 26 Maret 2013. http://aih25.blogspot.com/2013/03/rup-rational-unified-process.html.

Munir, Rinaldi. (2004). *Steganografi dan Watermarking*. Departemen Teknik Informatika, Institut Teknologi Bandung. http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/Steganografi%20dan%20Wate marking.pdf

Noni Indriani. 2014. *Implementasi Algoritma AES Enkripsi Pada SMS berbasis android.* Program Studi Teknik Informatika, Universitas AMIKOM.

Nugroho, Adi. 2005. *Pemodelan erorientasi objek*. Penerbit informatika bandung.

http://www.onesearch.id/Record/IOS266oai:e-journal.uajy.ac.id:395http://e-journal.uajy.ac.id/395/3/2MTI01472.pdf

Nur, Hidayat Rian. *"Rancang bangun pembuatan aplikasi "Voice Recognition secure" sebagai mediaKeamanan data berbasis android"* Sekolah Tinggi Manajemen Informatika Dan Komputeramikom Yogyakarta, 8 Agustus 2015.

Philippe Kruchten. (2010). *The Rational Unified Process: An Introduction (2nd edition)*.

Pudjo Widoo, Prabowo dan Herlawati, (2011), *Menggunakan UML,* Bandung Penerbit Informatika.

Pressman, R.S., 2010, *Software Engineering*, Seventh Edition, McGraw-Hill
Education (Asia).

Sadikin, Rifki., (2012), *Kriptografi untuk keamanan jaringan*, Yogyakarta : Penerbit Andi Yogyakarta.

Setyaningsih. Emy (2015) S.Si.,M.Kom 2015. *Kriptografi & Implementasinya menggunakan MATLAB.* Yogyakarta Penerbit ANDI Yogyakarta

Soeherman, Bonnie. 2008. *Designign Information System Concepts and cases With visoo.* Jakarta : PT Elex Media Komputindo.

Suhendar, A. Gunadi, Hariman. 2002. Visual Modeling : Menggunakan UML dan Rational Rose. Bandung : Informatika.

Sugrue J. 2009. *Getting Started with UML.*