JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 02 JULI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

APLIKASI ENKRIPSI DENGAN ALGORITMA RIVEST SHAMI ALDEMAN (RSA) DAN PARITY BIT CODING UNTUK FILE MULTIMEDIA

Usanto S.
Prodi Sistem Informasi, Fakultas Teknologi, ITB Swadharma

Correspondence author: Usanto S, usanto.s@swadharma.ac.id, Jakarta, Indonesia

Abstract

Encryption is the most effective way to obtain data security. In order to read the encrypted file, we must have access to a password that will allow us to decrypt the message. Data that is not encrypted is called plain text, while the encrypted one is called cipher text. As for steganography is the process of hiding data in digital files so that people do not think that if there are digital files there is no message. If these two processes are in combination then the message will be more secure. For this reason, it is necessary to make an application to store messages in images with encryption in the first process. Many methods are used to recognize cryptography, one of which is the RSA method. The use of this method aims to find out how cryptography works and the systems contained in the cryptographic process. This cryptography and steganography application uses an application called Eclipse which is commonly used to create android mobile applications.

Keywords: encryption, cryptography, RSA, steganography, android

Abstrak

Enkripsi adalah cara yang paling efektif untuk memperoleh pengamanan data. Untuk membaca file yang dienkripsi, kita harus mempunyai akses terhadap kata sandi yang memungkinkan kita mendeskripsi pesan tersebut. Data yang tidak dienkripsi disebut plain text, sedangkan yang dienkripsi disebut cipher text. Adapun steganografi adalah proses menyembunyikan data dalam file digital sehingga orang tidak berpikir bahwa jika file digital tidak ada pesan. Jika kedua proses ini dalam kombinasi maka pesan akan lebih aman. Untuk itu perlu dibuat sebuah aplikasi untuk menyimpan pesan alam gambar dengan enkripsi proses pertama. Banyak metode yang digunakan untuk mengenal kriptografi, salah satunya dengan metode RSA. Penggunaan metode ini bertujuan untuk mengetahui cara kerja kriptografi dan sistem yang terdapat dalam proses kriptografi tersebut. Aplikasi kriptografi dan steganografi ini menggunakan aplikasi bernama Eclipse yang biasa digunakan untuk membuat aplikasi mobile android.

Kata Kunci: enkripsi, kriptografi, RSA, steganografi, android

A. PENDAHULUAN

Pada era globalisasi, pengguna komputer dilakukan berbagai macam cara untuk menjaga keamanan data-data perusahaan maupun data kelompok dari pihak – pihak yang tidak berkepentingan. Karena rentangnya keamanan maka pengguna harus lebih canggih untuk menjaga data – data sehingga perlu dirancang pengamanan fata tersebuSetiap perubahan yang terjadi diamati dan dicatat, perubahan yang begitu halus atau tanpa cacat dalam kondisi fisik gambar tersebut sehingga tidak ada pihak lain yang menyadarinya bahwa didalam gambar tersebut terdapat sebuah informasi yang bersifat rahasia jika pihak lain tidak benar-benar memperhatikannya menggunakan aplikasi untuk mendeteksi informasi tersembunyi dalam gambar digital (Sandro, 2013).

Secara fisik tidak akan menarik perhatian dari penyerang potensial atau hacker, sebagai contoh sebuah gambar yang terlihat tidak berbahaya atau tidak berpotensi untuk diserang, pilihlah gambar yang umum yang telah diketahui oleh orang lain (Reddy & Raja, 2011). Sedangkan menurut (Nazelliana & Hapsari, 2015) untuk teknik steganografi bermanfaat jika digunakan tepat sasaran pada kasus yang berhubungan dengan perangkat keraskomputer karena terdapat banyak sekali format berkas digital yang dapat dijadikan media atau wadah penampung untuk menyembunyikan pesan yang ingin dititipkant

Ada cara yang lebih baik untuk mengamankan *file text* agar sulit diketahui oleh pihak-pihak yang tidak diinginkan yaitu dengan cara mengenkripsi (*encrypt*) pesan (*file*) tersebut menjadi karakter - karakter acak yang tidak dimengerti sehingga hanya bagi seseorang yang memiliki kunci (*key*) yang dapat mengembalikan pesan kebentuk semula.

Banyak didalam dunia komputer beberapa cara untuk mengamankan data agar tidak dapat seseorang melihat *file – file* pribadi, apalagi *file* tersebut bersifat rahasia dan penting. Salah satunya adalah dengan kriptografi. Kriptografi adalah seni atau ilmu yang mempunyai prinsip dan metode tentang perubahan pesan, dari pesan yang dapat dibaca menjadi pesan yang tidak dapat dibaca, kemudian akan dikembalikan menjadi kondisi semula. Metode yang digunakan adalah metode Rivest, Shami, Adleman (RSA) dan masih banyak lagi metode – metode yang membahas tentang kriptografi.

Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana penyembunyian pesan. Namun pada pengertian modern kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas. Jadi pengertian kriptografi modern adalah tidak saja berurusan hanya dengan penyembunyian pesan namun pada lebih pada sekumpulan teknik yang menyediakan keamanan informasi. (Rifki Sadikin, 2012).

Dalam kamus *hacker* (Dony Ariyus, 2005) dalam (andi Mardianto, 2014) kriptografi diartikan sebagai ilmu yang mempelajari penulisan secara rahasia. Secara umum kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan berita.

Pada tahun 1977, Rivest, Shamir, dan Adleman merumuskan algoritma praktis yang mengimplementasikan sistem kriptografi kunci public disebut dengan sistem kriptografi RSA. (Rives et al., 1983). Meskipun pada tahun 1997 badan sandi Inggris memublikasikan bahwa Clifford Cock telah merumuskan sistem kriptografi RSA 3 tahun lebih dahulu daripada Rivest, Shamir, dan Adleman. (Rifki Sadikin, 2012).

Steganografi adalah ilmu yang mempelajari bagaimana menyembunyikan teks pada media lain yang telah ada sedemikian sehingga teks yang tersembunyi menyatu dengan media itu. Media tempat penyembunyian pesan tersembunyi dapat

berupa media teks, gambar, audio atau video. Steganografi yang kuat memiliki sifat media yang telah tertanam teks tersembunyi sulit dibedakan dengan media asli namun teks tersembunyi tetap dapat diekstrasi. (Rifki Sadikin, 2012). Metode steganografi yang ideal hendaknya mendapatkan predikat high di setiap spesifikasi. Sayangnya, dari metode-metode yang dievaluasi, tidak ada metode yang dapat memenuhi setiap spesifikasi yang ada. Akan ada spesifikasi yang perlu dikorbankan untuk dapat memenuhi spesifikasi yang lain. Spesifikasi yang diutamakan dapat dipilih sesuai keperluan.

Teknik - teknik dalam steganografi telah berkembang untuk menyesuaikan terhadap banyaknya variasi data yang disisipkan dan media yang digunakan. Steganografi *file* multimedia mengenal sebuah teknik yang dinamakan teknik *parity coding*. Pada teknik *parity coding* sinyal dari berkas *file* dipecah menjadi beberapa region berbeda dan mengenkripsi setiap bit dari pesan rahasia yang ingin disisipkan pada sebuah sampel region yang berisi *parity* bit. ada beberapa metode yang tersedia untuk steganografi audio, secara singkat akan dijelaskan sebagai berikut :

1. LSB Encoding, Teknik sampling di ikuti dengan proses kuantisasi untuk mengkonversi sinyal audio analog ke dalam biner digital. Dalam teknik LSB ini, urutan biner dari masing-masing sampel berkas audio digital diganti dengan setiap biner dari pesan rahasia, (Begum & Venkataramani, 2011)
2. Phase Encoding, Sistem Auditory Manusia tidak dapat dengan mudah mengenali perubahan fasa dalam sinyal audio, metode Phase Encoding mengeksploitasi fakta ini. Teknik ini mengkodekan bit pesan rahasia sebagai pergeseran fase dalam spektrum fase dari sinyal digital, (Kaur & Behal, 2014)
3. Spread Spectrum, Ada dua pendekatan yang digunakan dalam teknik ini: Direct Sequence Spread Spectrum (DSSS) dan Frequency Hopping Spread Spectrum (FHSS). DSSS adalah teknik modulasi yang digunakan dibidang telekomunikasi. Seperti dengan teknologi spread spectrum lain, sinyal yang ditransmisikan membutuhkan bandwidth yang lebih dari sinyal informasi yang sedang dimodulasi, (Reddy, et al., 2013)

Sehingga pada penelitian ini dapat dirumuskan merancang sebuah aplikasi kriptografi dengan metode RSA yang disembunyikan dengan steganografi yang digunakan di aplikasi *mobile*, untuk membuat data – data yang di simpan di telepon genggam lebih aman. Android merupakan jenis OS yang banyak digunakan di telepon genggam, dan mencoba membuat aplikasi kriptografi dan steganografi di perangkat lunak telepon genggam berbasis android.

Android adalah sebuah sistem operasi untuk perangkat *mobile* berbasis linux yang mencangkup sistem operasi, *middleware*, dan aplikasi. Android menyediakan *platfrom* terbuka bagi para pengembang untuk menciptakan aplikasi mereka. Awalnya, Google Inc, membeli Android Inc yang merupakan pendatang baru untuk membuat perangkat lunak untuk ponsel / *smartphone*. Kemudian untuk mengembangkan android dibentuklah *Open Handset Alliance*, konsorsium dari 34 perusahaan perangkat keras, perangkat lunak dan telekomunikasi, termasuk Google Inc, HTC, Motorolla, Qualcomm, T-Mobile dan Nvidia. (Nazruddin Safaat H, 2012).

Android adalah sistem operasi untuk telepon seluler yang berbasis Linux. Android menyediakan *platform* terbuka bagi para pengembang buat menciptakan aplikasi mereka sendiri untuk digunakan oleh bermacam peranti bergerak. Awalnya, Google Inc. membeli Android Inc., pendatang baru yang membuat peranti lunak untuk ponsel. (Murphy, 2010).

Keamanan data sangat penting, dan banyak data yang selalu di simpan di telepon genggam, untuk menjaga keamanan data dari pihak – pihak yang tidak berkepentingan, berbagai cara dilakukan untuk menjaga keamanan data. Sedikitnya aplikasi telepon genggam yang menyediakan untuk keamanan file, maka pengguna perlu mempunyai sistem pengamanan agar datanya tidak dicuri dan tidak bisa diubah – ubah isinya oleh orang lain.

Dari kenyataan tersebut, maka akan dibuat aplikasi pengamanan file dengan kriptografi menggunakan android dengan *study* kasus keamanan file di telepon genggam berbasis android. Bagaimana mengubah teks asli menjadi teks sandi dengan mengenkripsi dan mengembalikan teks itu kembali, mengimplementasikan steganografi file gambar dengan teknik *Parity Coding* pada perangkat *mobile phone* dan menjaga kualitas berkas file gambar sebagai media steganografi sesudah implementasi teknik *Parity Coding*.

Tujuan dari penelitian adalah untuk membuat aplikasi sistem keamanan file agar file yang tersimpan di telepon genggam menjadi aman dan tidak bisa di lihat, dicuri dan diubah isinya oleh pihak yang tidak berkepentingan, sebingga bermanfaat bagi pengguna telepon genggam dapat merasa aman dengan data – datanya, dan dapat leluasa menulis dan menyimpan data tanpa takut terbaca dan dicuri oleh pihak – pihak yang tidak berkepentingan.

B. METODE PENELITIAN

Metode penelitian pada dasarnya merupakan cara ilmiah untuk mendapatkan data dengan tujuan dan kegunaan tertentu. Penelitian ini menggunakan metode penelitian kualitatif dengan menggunakan pendekatan penelitian pengamatan (observasi), dan Studi Pustaka untuk pengumpulan data sekunder yang dilakukan untuk memperoleh keterangan dan data dari literatur yang berupa buku, majalah, makalah, *internet* yang relevan dengan landasan teori atas masalah yang diteliti agar diperoleh suatu pemahaman yang mendalam serta menunjang proses pembahasan mengenai masalah-masalah yang telah diidentifikasi.

C. HASIL DAN PEMBAHASAN

Proses pemecahan masalah perlu dilakukan analisa secara teliti, tepat, dan akurat. Semakin rumit masalah yang dihadapi, maka analisa yang harus dikerjakan akan semakin komplek. Karena dukungan data, informasi, teori, atau konsep dasar dan alat bantu yang memadai secara kualitatif sangat penting untuk menghasilkan pemecahan masalah yang baik.

Didalam metode RSA menggunakan dua *key* yaitu *private key* dan *public key*, sedangkan metode lain hanya membutuhkan satu *key* atau bahkan tidak membutuhkan *key* sama sekali. Inlah yang membedakan metode RSA dengan metode – metode yang lain.

Untuk *encrypt* data, masukan data ("*plaintext*") dan sebuah kunci enkripsi untuk porsi enkripsi algoritma. Untuk dekrip "*ciphertext*", sebuah kunci dekripsi yang benar digunakan pada porsi dekripsi algoritma. Kunci – kunci tersebut, yang mengandung sejumlah *string* sederhana disebut kunci publik dan kunci kunci privat, secara langsung.

Kunci acak

1. Acak 2 bilangan prima besar, p dan q
   p = 17
   q = 31
2. n = pq
   n = 17 * 31
   = 527
3. m = (17 -1) (31-1)
   = 16 * 30
   = 480
4. Pilih angka kecil, e *coprime* ke m
   e *comprime* ke m, berarti bahwa angka terbesar dapat dibagi secara tepat dengan

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 02 JULI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

kedua *variable* e dan m (pembagian umum terbesar, atau gcd) adalah 1, algoritma *Euclid* digunakan untuk mencari gcd dari 2 bilangan, misalnya e dipilih 77, nilai 77 memenuhi syarat karena gcd (480,77) = 1. Jadi kunci K_{publik} = (77, 527)

5. Temukan d, de mod m = 1
   Ini adalah *equivalen* untuk mencari d yang memuaskan de = 1 + nm dimana n adalah *integer* atau juga (1 + nm)/2. Sekarang kita bekerja melalui nilai – nilai n sampai sebuah solusi *integer* untuk 2 ditemukan :
   n = 47 ➔ 480 x 47 = 22560 + 1 = 22561, d = 22561/ 77 = 293

Untuk melakukannya dengan bilangan – bilangan besar, algoritma yang lebih canggih disebut *Euclid extended* harus digunakan.

Kunci rahasia, kunci publik
N = 527 n = 527
e = 77 d = 293

Enkripsi

Pesan harus sejumlah kecil dari p dan q yang lebih kecil. Bagaimanapun, pada poin ini kita tidak tahu p dan q, jadi dalam prakteknya batas yang lebih rendah p dan q harus ditampilkan. Hal ini dapat menjadi sesuatu dibawah nilai benarnya dan demikian pula bukan sebuah konsen keamanan mayor. Untuk contoh ini, mari kita gunakan pesan "51".

$C = P^e \bmod n$
$= 51^{77} \bmod 527 = 493$

Dekripsi

Proses ini sangat mirip dengan enkripsi, tapi memasukkan pangkat yang lebih besar, yang dapat dipecahkan ke dalam beberapa langkah.

$P = C^d \bmod n$
$= 493^{293} \bmod 527 = 51$

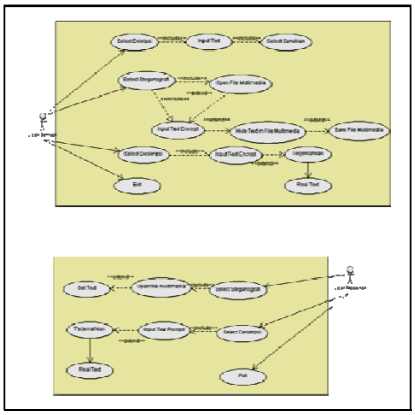
Setelah mendapatkan algoritma dari metode RSA tersebut maka barulah membuat programnya di dalam Android

Perencanaan dilaksanakan setelah selesai melakukan tahap analisis terhadap sistem. Kembali kepada permasalahan setiap seseorang mempunyai suatu hal yang dirahasiakan dan tidak dapat di akses orang lain, terutama dalam pengiriman informasi yang tidak ingin dipublikasikan hanya untuk yang dituju saja sehingga informasi yang tidak dapat disalah gunakan oleh pihak lain yang dapat merugikan.

Pesatnya kemajuan teknologi dalam pengiriman pesan, menimbulkan dampak negatif. Dampak negatif yang terjadi adanya pihak – pihak yang menyalah gunakan teknologi informasi yang sudah ada untuk memperoleh informasi yang penting bagi *user* (penyadapan). Penulis memikirkan bagaimana untuk melindungi informasi dalam bentuk pesan agar tidak dapat disadap oleh orang lain. Penggunaan aplikasi untuk mengubah kata – kata pada pesan kedalam bentuk tulisan acak dengan metode enkripsi dan menyimpannya di dalam file multimedia yang disebut *steganografi*. Proses pembacaan pesan dengan cara mengeluarkan pesan dari gambar dan untuk membaca pesan yang diacak dengan menggunakan metode deskripsi. Android merupakan perkembangan di teknologi telepon genggam yang disebut *smartphone*, sehingga penulis ingin mengaplikasikan di telepon genggam berbasis android. *Use case* diagram menggambarkan fungsionalitas yang diharapkan dari sebuah sistem. *Use-case diagram* adalah sebuah diagram yang mendeskripsikan interaksi antara sistem dengan bagian eksternal dari sistem serta dengan *user, (*Whitten dan Bentley, 2012:246)

Analisa yang dilakukan menggunakan UML (*Unified Modelling Language*) menghasilkan beberapa diagram, diantaranya adalah :

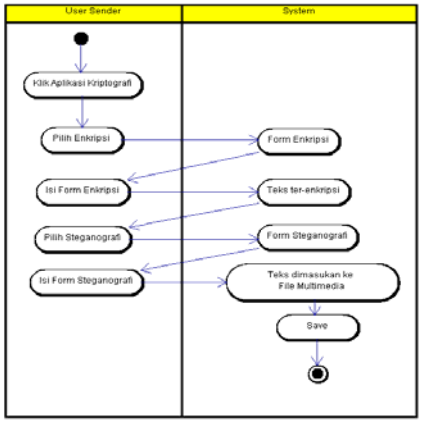
1. ***Use case Diagram***
   Diagram Use case sistem usulan kriptografi dan steganografi dapat dilihat pada gambar 1



Gambar 1. Diagram Use Case Sistem Usulan

2. *Activity Diagram*

Diagram Activity sistem usulan kriptografi dan steganografi dapat dilihat pada gambar 2 dan 3

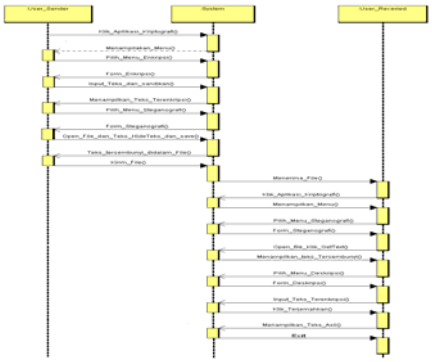


Gambar 2. Diagram *Activity* Sistem Usulan

Gambar 3. Diagram *Activity* Sistem Usulan

3. *Sequence Diagram*

Sequence diagram sistem usulan kriptografi dan steganografi dapat dilihat pada gambar 4



Gambar 4. Diagram *Sequence* Sistem Usulan

Perancangan Sistem Usulan

Perancangan sistem usulan secara garis besar disimpulakn melalui diagram *Hierarchy Input Process Output* (HIPO) untuk mewakili modul sistem sebagai hirarki dan dokumentasi setiap modul. Desain bagian struktur mirip dengan penampilan struktur organisasi, namun telah dimodifikasi untuk menunjukan detail tambahan sehingga mendukung pelaksanaan sistem untuk menunjukan proses berjalannya aplikasi kriptografi dan steganografi.

Rancangan aplikasi kriptografi dan steganografi digunakan pada telepon gengam dengan menggunakan OS android. (Lessard & Kessler , 2012), pengertian dari android adalah sistem operasi untuk telepon genggam yang berbasis Linux. Dalam sistem operasi android, menyediakan platform terbuka bagi para pengembangnya untuk menciptakan aplikasi mereka sendiri sehingga dapat digunakan oleh bermacam perangkat.

Kemudian untuk mengembangkan android dibentuklah *Open Handset Alliance*, konsorsium dari 34 perusahaan perangkat keras, perangkat lunak dan telekomunikasi, termasuk Google Inc, HTC, Motorolla, Qualcomm, T-Mobile dan Nvidia. (Nazruddin Safaat H, 2012).

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 02 JULI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

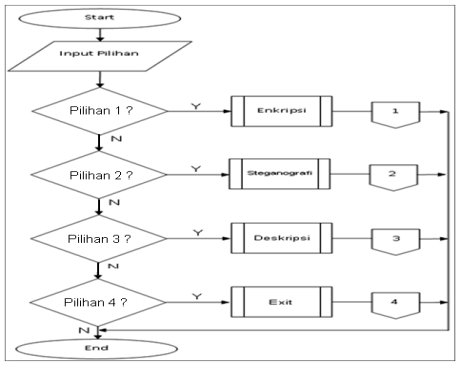
Dibutuhkan beberapa *software* pendukung yang harus terinstal sebelum mengembangkan aplikasi android, antara lain (1). *Java Development Kit* (JDK), (2). IDE Eclipse, (3). Android *Software Development Kid* (SDK), (4). *Android Development Tools* (ADT) *Plugins*, (Dodit Supriyanto & Rini Agustina, 2012). Eclipse selalu dilengkapi dengan JDT (*Java Development Tools*), yaitu sebuah *plug-in* yang membuat eclipse dapat dipakai untuk mengembangkan program Java, serta ada juga PDE (*Plug-in Development Environment*) yang bisa dipakai untuk membuat *plug-in* baru.(Wahana Komputer, 2013).

Kegunaan aplikasi ini memudahkan pengguna dalam mengamankan isi atau informasi agar tidak mudah terbaca dan diketahui pihak luar. diagram *Hierarchy Input Process Output* (HIPO) dapat dilihat pada gambar 4

Gambar 5. Diagram *Hierarchy Input Process Output* (HIPO)

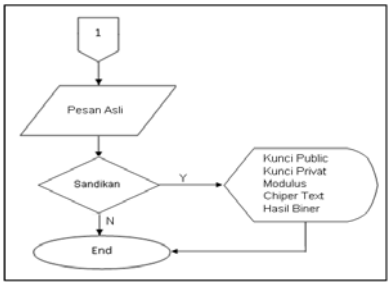
Flowchart Aplikasi

Flowchart Menu Utama Aplikasi Kriptografi dan Steganografi pada menu utama akan muncul beberapa pilihan menu yaitu enkripsi, deskripsi, steganografi dan exit dan dapat dilihat pada gambar 6.



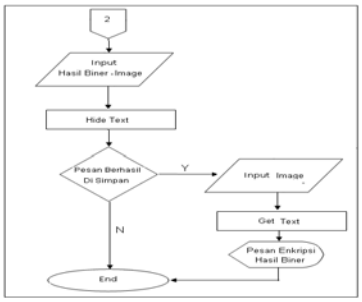
Gambar 6. *Flowchart* Menu Utama

Gambar dibawah ini menjelaskan menu enkripsi, didalamnya *user* dapat melakukan input pesan asli, jika memilih tombol sandikan maka kunci public, kunci privat dan modulus sebagai perhitungan untuk mengubah pesan asli menjadi terenkripsi yang ditampilkan di *chipper text* dan di ubah menjadi bilangan biner yang ditampilkan di hasil biner



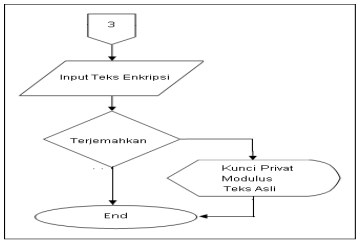
Gambar 7. *Flowchart* Enkripsi

Gambar di dibawah ini menjelaskan menu steganografi, didalamnya *user* dapat melakukan input hasil biner dan *image*, menekan tombol *hide text* akan melakukan proses memasukan hasil biner kedalam *image* dan *image* akan tersimpan. Jika image berhasil disimpan menginput kembali *image* yang sudah tersimpan dan diproses dengan tombol *get text* untuk mengeluarkan hasil biner dan menampilkannya di kolom hasil biner diproses menjadi *integer* ditampilkan di pesan enkripsi.



Gambar 8. *Flowchart* Menu Steganografi

Gambar dibawah ini menjelaskan menu deskripsi, didalamnya user dapat melakukan input teks enkripsi, jika menekan tombol terjemahan maka menampilkan kunci privat dan modulus sebagai perhitungan untuk menghasikkan teks asli di kolom teks asli

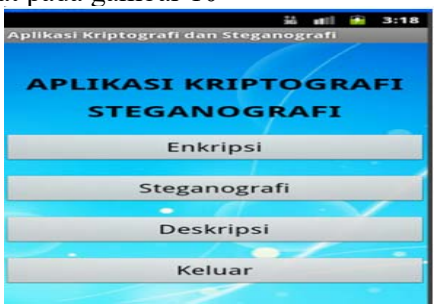


Gambar 9. *Flowchart* Menu Deskripsi

Rancangan Tampilan

1. Menu Utama

Halaman menu utama berfungsi untuk menampilkan menu saat aplikasi pertama kali di telepon genggam berbasis android yang sudah terinstall Aplikasi Kriptografi dan Steganografi. *User* dapat menggunakan menu yang tersedia di menu utama, seperti terlihat pada gambar 10



Gambar10. Tampilan Menu Utama

2. Menu Enkripsi

Setelah memilih menu enkripsi maka akan menampilkan sebuah *form* yang berisikan :

a. Pesan merupakan pesan asli yang belum di enkripsi
b. Kunci publik merupakan suatu kode semacam gembok sebagai proses pengenkripsian teks.
c. Kunci Privat merupakan suatu kode semacam kunci gembok sebagai proses pengenkripsian teks
d. Modulus merupakan kode untuk pengacak teks sebagai proses pengenkripsian teks .
e. *Chipertext* merupakan kode acak dari proses pengenkripsian teks setelah mengklik *button* sandikan.
f. Pesan biner merupakan bilangan biner dari proses pengenkripsian teks ke biner setelah mengklik *button* sandikan.
g. Sandikan berfungsi untuk melakukan proses pengenkripsian teks yang akan memperoleh hasil di *text field chipertext*

Gambar11. Menu Enkripsi

3. Menu Steganografi

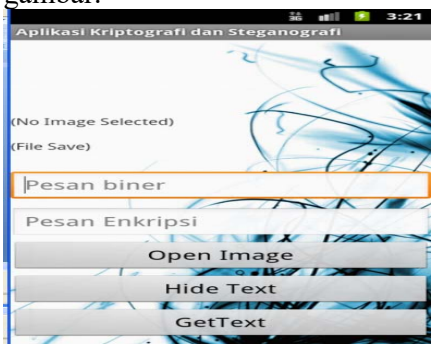
Setelah memilih menu steganografi maka akan menampilkan sebuah *form* yang berisikan :

a. *Image view* merupakan tampilan gambar yang dipilih.
b. Pesan biner merupakan bilangan biner yang dimasukan kedalam gambar dan dikeluarkan dari gambar.
c. Pesan enkripsi merupakan pesan enkripsi yang tampil saat mengeluarkan pesan dari gambar.
d. *Open file* merupakan *button* berfungsi untuk mengambil file gambar dari galeri

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 02 NOMOR 02 JULI 2022
ISSN 2774 – 5775 | eISSN 2774-5767

yang terdapat di telpon genggam berbasis android.

e. *Hide Text* merupakan *button* yang berfungsi untuk menyembunyikan teks ke dalam gambar.
f. *Get Text* merupakan *button* yang berfungsi untuk mengeluarkan teks dari gambar.

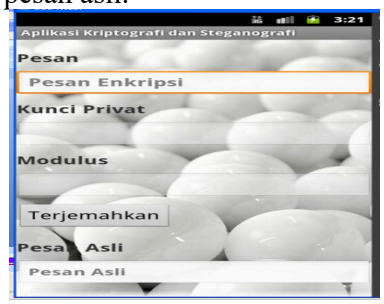


Gambar12. Menu Steganografi

4. Menu Deskripsi

Setelah memilih menu deskripsi maka akan menampilkan sebuah *form* yang berisikan :

a. Isi pesan merupakan pesan yang sudah terenkripsi.
b. Kunci Privat merupakan suatu kode sebagai proses pendeskripsian teks untuk menjadi teks asli.
c. Modulus merupakan kode pengacak teks sebagai proses pendeskripsian teks untuk menjadi teks asli.
d. Pesan asli merupakan pesan yang sudah terdeskripsi menjadi pesan asli.
e. Terjemahkan merupakan *button* yang berfungsi melakukan pendeskripsian teks yang akan memperoleh hasil di *text field* pesan asli.



Gambar13. Menu Deskripsi

Black Box Testing

Pengujian *Black Box* berfokus pada persyaratan fungsional perangkat lunak. Pengujian *Black Box* memungkinkan perekayasa perangkat lunak mendapatkan serangkaian kondisi input yang sepenuhnya menggunakan semua persyaratan fungsional untuk suatu program.

Tabel 1.Rencana Pengujian Aplikasi

Item Uji	Detail Pengujian	Jenis Pengujian
Tampilan Enkripsi	Pilih Menu Enkripsi	*Black Box*
Tampilan Steganografi	Pilih Menu Steganografi	*Black Box*
Tampilan Deskripsi	Pilih Menu Deskripsi	*Black Box*

Tabel 2. Pengujian Menu Enkripsi

Kasus dan Hasil Uji Data	
Aksi	Pilih Enkripsi dan isi form enkripsi kemudian sandikan
Yang Diharapkan	Muncul form enkripsi,teks terenkripsi dan hasil biner
Pengamatan	Pilih enkripsi kemudian dilakukan uji dengan isi form dan teks terenkripsi
Kesimpulan	Pengujian Diterima

Tabel 3. Menu Steganografi

Kasus dan Hasil Uji Data	
Aksi	Pilih Steganografi dan isi form Steganografi kemudian menyembunyikan teks kedalam file multimedia atau mengeluarkan teks dari file multimedia
Yang Diharapkan	Muncul form Steganografi, open file, menyembunyikan bilangan biner kedalam file multimedia atau mengeluarkan teks biner dan teks enkripsi dari file

Kasus dan Hasil Uji Data	
	multimedia
Pengamatan	Pilih enkripsi kemudian dilakukan uji dengan isi form dan menyembunyikan teks ke gambar dan mengeluarkan teks dari gambar
Kesimpulan	Pengujian Diterima

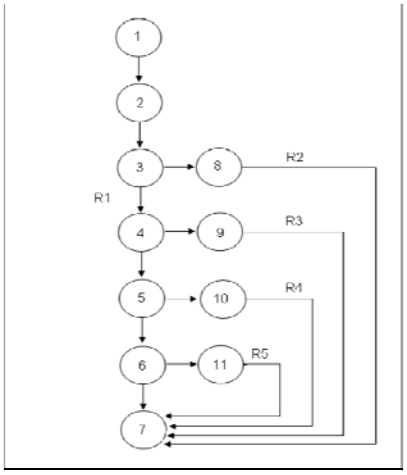
Tabel 4. Menu Deskripsi

Kasus dan Hasil Uji Data	
Aksi	Pilih Deskripsi dan isi form deskripsi kemudian terjemahkan pesan enkripsi
Yang Diharapkan	Muncul form Deskripsi dan teks terenkripsi menjadi teks asli
Pengamatan	Pilih menu deskripsi kemudian dilakukan uji dengan isi form dan teks terdeskripsi atau menjadi pesan asli
Kesimpulan	Pengujian Diterima

Berdasarkan pengujian *Black Box* yang telah dilakukan memperoleh kesimpulan bahwa secara fungsional semua proses pada Aplikasi Kriptografi dan Steganografi dapat berfungsi dengan cukup baik , semua berfungsi sesuai dengan proses yang sudah diperhitungakan dan aplikasi ini memberikan *output* sesuai yang diharapkan.

White Box Testing

Pengujian dilakukan untuk memastikan bahwa semua *statement* pada program telah dieksekusi paling tidak satu kali selama pengujian dan bahwa semua kondisi logis telah diuji.



Gambar 14 Tampilan Grafik Alir Pengirim

Dari Flowchart diatas di dapatkan :
Region (R) = 5
R1 = Keseluruhan
R2 = 3,8,7
R3 = 4,9,7
R4 = 5,10,7
R5 = 6,11,7
Edge (E) =14
Node (N) =11
Predicate Node = R – 1= 5 – 1= 4
P1 = 4
Perhitungan :

1. V(G) = E – N + 2
   V(G) = E – N + 2
   = 14 – 11 + 2 = 5
2. V(G) = P + 1
   V(G) = P + = 4 + 1= 5
3. Cyclomatic complexity (CC) = R1,R2,R3,R4,R5 = 5
   Path 1 : -2-3-8-7
   Path 2 : 1-2-3-4-9-7
   Path 3 : 1-2-3-4-5-10-7
   Path 4 : 1-2-3-4-5-6-1Path
   Path 5Path 4 : 1-2-3-4-5-6-7
   Path 6

Berdasarkan hasil pengujian uji coba *white box testing* diatas dapat disimpulkan bahwa *flowchart* benar. Hasil uji coba diatas menunjukan penerapan metode test case dengan pendekatan *white box testing* dapat menghasilkan aplikasi dan proses pada

flowchart di aplikasi menjadi efektif dan efesien

D. PENUTUP

Berdasarkan hasil penelitian yang dilakukan terhadap pembuatan Aplikasi Kriptografi dan Steganografi, ada beberapa hal yang dapat disimpulkan,yaitu :

1. Untuk mengamankan sebuah pengiriman informasi dalam bentuk teks di perlukan aplikasi kriptografi untuk proses enkripsi dan deskripsi dengan metode RSA,
2. Aplikasi dapat melakukan enkripsi dan dekripsi terhadap pesan dengan masukan kunci yang yang digunakan pada saat proses.
3. Untuk mengimplementasikan proses memasukan dan mengeluarkan teks pada file gambar atau disebut dengan steganografi menggunakan metode *Parity Coding* pada aplikasi.
4. Mengimplementasikan teknik parity coding pada perangkat mobile phone dengan cara pesan diubah menjadi bilangan biner, memilih gambar dan diproses gambar diubah menjadi biner dan setiap 8 bit akhir dimasukan 1 bit biner pesan.
5. Perangkat lunak yang digunakan untuk mengimplementasikan steganografi gambar dengan teknik *Parity Coding* pada berkas *image* berhasil dibangun. Kebutuhan fungsional dari perangkat lunak seperti proses penyembunyian dan ekstraksi pesan serta penggunaan kunci sudah dapat dilakukan dengan benar.
6. Pada proses ekstraksi, pesan atau informasi yang disisispkan pada file gambar uji dalam aplikasi Steganografi ini, dapat diperoleh kembali secara utuh atau dengan kata lain pesan yang disisipkan sebelum proses penyisipan dan setelah proses ekstraksi sama tanpa ada perubahan.

Berdasarkan kesimpulan dan hasil yang dicapai, maka akan disampaikan hal – hal yang perlu ditambahkan sebagai berikut :

1. Pengembangan tampilan dengan menggunakan *background* dan *interface* yang lebih menarik.
2. Penambahan *login* pada saat membuka aplikasi agar lebih aman lagi.
3. Penggunaan database untuk dapat menyimpan nilai kunci public, kunci privat, dan modulus agar lebih banyak.

E. DAFTAR PUSTAKA

Begum, M. B. & Venkataramani, Y., 2011 . LSB Based Audio Steganography based OnText Compression. International Conference On Communication Technology and System Design

Kaur, N. & Behal, S., 2014. Audio Steganography Techniques-a Survey. Journal of Engineering Research and Applications

Lessard, j. & kessler , g. C., 2010. Android forensics: simplifying cell phone examinations. Small scale digital device forensics journal , volume 4, p. 1.

Nazelliana, D & Hapsari, A. T., 2015. Implementasi penyisipan pesan file ke dalam gambar dengan algoritma huffman. Faktor exacta, volume 08

Reddy, H. S. M. & Raja, K. B., 2011. Wavelet based non lsb steganography. Int. J. Advanced networking and applications,

Reddy, V. L., Subramanyam , A. & Reddy , P. C., 2013. A Novel Approach For Hiding Encrypted Data in Image, Audio and Video Using Steganography. International journal of computer applications (0975 – 8887),

Sadikin, Rifki 2012, Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java : CV Andi Offset, Yogyakarta

Safaat H, Nazruddin.2012. Pemograman Aplikasi Mobile Smartphone dan Tablet PC Berbasis Android

Sandro Sembiring. 2013. Perancangan Aplikasi Steganografi Untuk Menyisipkan Pesan Teks Pada Gambar Dengan Metode End Of File.

Supriyanto, Dodit & Agustina, Rini, S.Kom. 2012. Pemograman Aplikasi Android : Step by Step Membuat Aplikasi Android untuk SmartPhone dan Tablet, Yogyakarta.

Wahana Komputer 2013 Android Programming With Eclipse: CV Andi Offset, Yogyakarta.

Whitten dan Bentley. 2012. System Analysis and Design for The Global Enterprise (7th Edition). New York: McGraw-Hill Companie.