

## IMPLEMENTASI KRIPTOGRAFI EMAIL BERBASIS ANDROID DENGAN METODE ELGAMAL PADA PT SUDATA MAKMUR

**Jaqfar Sholeh ,Ferdiansyah**

*Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur*

*Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260*

*Telp. (021) 5853753, Fax. (021) 5866369*

*E-mail : [jaqfarvadaq@gmail.com](mailto:jaqfarvadaq@gmail.com) , [ferdiansyah@budiluhur.ac.id](mailto:ferdiansyah@budiluhur.ac.id)*

### ABSTRAK

PT SUDATA MAKMUR merupakan sebuah PT yang bergerak dibidang distributor agen penjualan yang selalu berkomunikasi dengan sesama anggota dan klien nya lewat *email* untuk memberikan informasi soal distribusi. Untuk menjaga keamanan informasi tersebut dibutuhkan suatu cara untuk menjaga kerahasiaan dari informasi informasi tersebut. Kriptografi adalah teknik pengamanan data atau informasi yang mengubah *plaintext* (data asli) menjadi *ciphertext* (data yang tidak bisa dibaca), itulah yang disebut enkripsi. Serta dapat mengembalikan data dari *ciphertext* menjadi *plaintext* , proses tersebut dinamakan dekripsi. Dewasa ini kekhawatiran akan keamanan data perusahaan semakin besar, melihat semakin maraknya pencurian informasi penting dari sebuah perusahaan. Untuk itulah perlu dibangun sebuah aplikasi kriptografi *email* dengan implementasi algoritma ElGamal. ElGamal adalah algoritma enkripsi untuk mengubah *text* menjadi deretan karakter acak dan merupakan standar enkripsi yang banyak digunakan saat ini serta merupakan salah satu algoritma *hashing* yang sering digunakan untuk enkripsi data. ElGamal terkenal dengan kekuatan, kesederhanaan, dan kecepatannya. dalam mengamankan *password*. Aplikasi ini akan mengenkripsi data yang digunakan PT. Sudata Makmur untuk bertukar informasi dengan rekan perusahaannya dengan aman. Aplikasi *email* kriptografi berbasis android ini dapat diimplementasikan dengan baik, Sehingga mengurangi kekhawatiran perusahaan akan keamanan datanya.

**Kata Kunci :** Kriptografi, *Email*, Enkripsi, Dekripsi Elgamal, *Mobile*  
xi + 74 halaman; 37 gambar; 1 lampiran

### 1. PENDAHULUAN

#### 1.1. Latar Belakang

Seiring dengan kemajuan teknologi yang semakin canggih menjadikan manusia semakin mudah untuk berkomunikasi dan saling bertukar informasi dengan jarak jauh, khususnya melalui media internet. Menurut Iskandar Akisyahbana (1980) manusia telah mengenal teknologi sejak jutaan tahun yang lalu karena dorongan untuk hidup yang lebih nyaman, makmur dan sejahtera. Jadi sejak awal peradaban sebenarnya telah ada teknologi, mestipun istilah “teknologi” belum digunakan. Istilah “teknologi” didapat dari kata “techne” yang artinya cara dan “logos” yang artinya pengetahuan. Jadi secara teoritis teknologi adalah pengetahuan tentang cara yang perlu dilakukan dengan bantuan akal dan alat agar kebutuhan manusia dapat terpenuhi.

Media komunikasi yang dimanfaatkan tentu harus merupakan media yang mudah digunakan oleh banyak kalangan dan mudah dijangkau, contoh media komunikasi yang memungkinkan adalah *email*. *Email* memanfaatkan suatu *text area* untuk mengirimkan informasi. Namun akibat dari banyaknya orang yang menyalahgunakan

penggunaan dari *email*, Informasi menjadi sangat berpotensi untuk diketahui oleh orang yang tidak bertanggung jawab serta tidak sedikit orang yang mencari tahu mengenai informasi tersebut dengan melakukan *hack* ke *email*. Sejalan dengan hal itu, tuntutan akan keamanan terhadap suatu kerahasiaan data atau informasi semakin meningkat dan sangat dibutuhkan.

Karena itu timbul gagasan demi menjaga keamanan serta kerahasiaan data dan informasi PT. Sudata Makmur. Dan metode yang akan diambil adalah kriptografi yang dapat digunakan untuk mengamankan isi pesan *email* pada PT. Sudata makmur. Penerapan kriptografi pada tugas akhir ini akan difokuskan pada implementasi sebuah metode yang dipakai untuk dapat mengamankan isi pesan *email* yang dikirim menjadi aman sampai dengan pesan *email* diterima dan dibuka oleh pihak-pihak yang berhak untuk membukanya.

#### 1.2. Masalah

Masalah yang akan dibahas dalam Tugas Akhir ini yaitu:

- a. Bagaimana membuat aplikasi untuk mengamankan informasi yang akan dikirimkan melalui *email* dengan mengimplementasikan algoritma Elgamal?
- b. Bagaimana mengembalikan informasi asli tanpa perubahan setelah dilakukan enkripsi? .

### 1.3. Tujuan Penulisan

- a. Mengamankan sekaligus mengirimkan data atau informasi melalui *email* dalam aplikasi.
- b. Meminimalisir penyadapan informasi yang dikirimkan lewat email.

### 1.4. Batasan Masalah

- a. Menggunakan bahasa pemrograman *Java*.
- b. Metode kriptografi yang digunakan untuk mengamankan informasi adalah algoritma Elgamal.
- c. Berjalan dengan sistem operasi Android
- d. Pembuatan aplikasi menggunakan editor Android studio.

## 2. LANDASAN TEORI

### 2.1. *E-mail (Electronic Mail)*

#### 2.1.1. Pengertian *E-mail*

Istilah *E-mail* diambil dari *Elektronik Mail* yang bermakna surat-menyurat dengan media elektronik. Alasan *E-mail* kerap kali digunakan karena mudah dikirim dan cepat sampai tujuan dibanding surat konvensional. Cukup dengan mengetik lewat *keyboard* tanpa membutuhkan kertas, amplop dan perangko, dalam sekejap surat akan sampai tujuan meskipun antara pengirim dan penerima berjarak ribuan mil. Saat ini *e-mail* merupakan salah satu fasilitas dari internet yang paling populer digunakan. Tidak dapat dipungkiri, inilah sarana pengiriman surat yang efisien sekaligus ekonomis pada era seperti sekarang.

#### 2.1.2. Fungsi *E-mail*

1. Menghubungkan kita dengan siapapun yang terhubung di internet di seluruh dunia.
2. Data dikirim melalui internet sehingga sampai tujuan dengan cepat
3. Dapat mengirim kepada lebih dari 1 orang dalam waktu bersamaan
4. Digunakan untuk mendaftar aplikasi atau media sosial.
5. Memudahkan komunikasi di era sekarang.

#### 2.1.3. Jenis – Jenis *E-mail*

1. *POP Mail*
2. *Web-based Mail*
3. *E-mail Forwarding*

## 2.2. Kriptografi

### 2.2.1. Pengertian Kriptografi

Kriptografi diambil dari kosakata Yunani, *Crypto* yang artinya *secret* (rahasia) dan *graphia* artinya *writing* (tulisan). Secara umum, kriptografi

dapat diartikan sebagai tulisan rahasia. Secara teori, kriptografi adalah seni atau ilmu untuk mengamankan informasi ketika proses pengiriman sedang berjalan.

Kriptografi bisa disebut juga sebagai salah satu metode yang mengajarkan cara-cara menjaga data atau informasi tetap aman disaat proses pengiriman, antara pengirim dan penerima tanpa mengalami gangguan dari pihak luar. Sehingga algoritma kriptografi merupakan langkah-langkah logis dalam usaha memproteksi pesan dari orang-orang yang tidak bertanggung jawab.

### 2.2.2. Tujuan Kriptografi

Menurut Rifki Sadikin (2012), Ilmu kriptografi merupakan salah satu aspek penting dari keamanan informasi. Terdapat 4 tujuan mendasar, yakni :

#### 1. *Confidentiality*

Kerahasiaan, upaya untuk proteksi supaya orang yang tidak berkepentingan tidak bisa membaca pesan. Untuk itulah diperlukan suatu metode yang mampu mengubah isi pesan agar menjadi tidak mudah untuk dibaca dan dipahami, didalam kriptografi hal ini direalisasikan dengan menyandikan plaintext menjadi ciphertext. Contoh : pesan yang berisi “minggu depan kita rapat” disandikan menjadi “hjjg&08potnaiuhd#!%”.

#### 2. *Data Integrity*

Integritas Data, adalah cara untuk mampu mengetahui apakah ada perubahan (hapus, ubah atau tambah) data dari pihak luar dan untuk menjamin bahwa pesan masih asli/utuh sewaktu mengirim data. Itu artinya, integritas data dapat digambarkan dengan pertanyaan : “apakah pesan yang diterima tidak mengalami manipulasi data?”

#### 3. *Authentication*

Otentifikasi, proses yang berhubungan dengan mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication*). Dua pihak yang saling berkomunikasi harus dapat mengotentifikasi satu sama lain sehingga ia dapat memastikan sumber pesan.

#### 4. *Non-Repudiation*

Nirpenyangkalan, Adalah cara untuk menjaga entitas bagi yang berkomunikasi untuk melakukan penyangkalan, pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

### 2.2.3. Keamanan Sistem Kriptografi

Keamanan sebuah metode kriptografi menjadi poin yang sangat penting untuk menjaga keamanan sistem. Dengan menggunakan sistem yang umum digunakan, maka keamanan suatu sistem akan lebih mudah dianalisa bahkan dibobol. Sistem kriptografi dibuat untuk menjaga plaintext dari kemungkinan dibaca oleh pihak-pihak tidak berwenang, yang secara umum dinamakan sebagai penyadap. Penyadap diasumsikan memiliki akses yang tak

terbatas dijalar yang tak aman bertujuan untuk mengirimkan chipertext. Oleh karena itu, penyadap dianggap memiliki akses langsung terhadap chipertext. Tipe penyadap paling umum terhadap sistem kriptografi adalah serangan dari kriptanalisis. Kriptanalisis merupakan ilmu yang mempelajari tentang upaya-upaya untuk memperoleh plaintext dari chipertext tanpa informasi tentang kunci yang digunakan. (Dony Ariyus, 2005).

#### 2.2.4. Algoritma Elgamal

Ditemukan pada tahun 1985 oleh ilmuwan asal mesir yaitu Taher ElGamal. Algoritma ini merupakan algoritma yang berkonsep kunci publik. Dimana pada dasarnya digunakan untuk digital signature, namun pada era sekarang dimodifikasi ulang agar dapat dimanfaatkan untuk enkripsi dan dekripsi.

Algoritma ini membutuhkan perhitungan logaritma diskrit yang cukup rumit pada modulo prima yang besar, jadi akan cukup sulit untuk memecahkan logaritma ini. Hal itu membuat algoritma ini bisa dibilang cukup terjamin keamanannya.

### 3. ANALISA MASALAH DAN RANCANGAN PROGRAM

#### 3.1. Permasalahan dan Rancangan Aplikasi

##### 3.1.1. Analisa Masalah

Data atau informasi merupakan aset yang berharga dan sangat penting untuk dijaga, terutama bila data tersebut sifatnya rahasia dimana tidak semua orang mempunyai hak yang sama untuk mengetahui isi dari data tersebut. Maka dari itu aspek privasi data menjadi salah satu perhatian utama agar informasi atau data dapat terjamin kerahasiaannya.

PT. Sudata Makmur, sebuah perusahaan yang bergerak dibidang distributor agen penjualan. PT ini selalu berhubungan dengan sesama anggota dan klien nya lewat *email* untuk memberikan informasi persoalan – persoalan pekerjaan. Untuk menjaga kerahasiaan daripada informasi tersebut maka dibutuhkan suatu aplikasi yang dapat menjaga kerahasiaan dari informasi informasi tersebut.

Sejalan dengan hal yang dijelaskan diatas, Perusahaan berupaya untuk menerapkan teknologi terkini dimana pada pengembangan kali ini upaya yang dilakukan adalah memanfaatkan teknologi kriptografi berbasis android agar lebih mudah dan efisien serta untuk menjaga kerahasiaan dan privasi dari sebuah data atau informasi yang menyangkut perusahaan.

##### 3.1.2. Penyelesaian Masalah

Dari permasalahan yang telah diuraikan diatas, diperlukan adanya sebuah aplikasi yang dapat menjaga kerahasiaan dari sebuah pesan email atau informasi. Sehingga isi dari pesan email tersebut tidak dapat dibaca oleh orang lain yang tidak berkepentingan atau tidak berhak mengetahui isi dari pesan email tersebut. Sehingga keberadaannya tidak

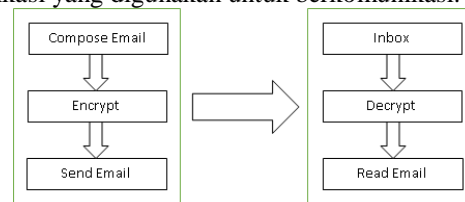
terdeteksi atau diketahui oleh pihak lain yang tidak berhak untuk informasi tersebut. Aplikasi tersebut nantinya dapat mengacak isi dari pesan email (mengacak isi pesan email dengan kata kunci atau password) melalui jalur komunikasi publik hingga dapat diterima oleh pengguna kedua yaitu penerima. Kemudian pengguna kedua atau penerima informasi tersebut dapat mengembalikan informasi rahasia yang ada didalamnya.

Dengan adanya aplikasi ini diharapkan pesan *email* penting yang sifatnya rahasia dapat dikirimkan ke pihak yang berhak menerima tanpa penyalahgunaan oleh pihak pihak yang tidak bertanggung jawab agar kerahasiaan data tetap terjaga.

#### 3.1.3. Perancangan Aplikasi

Tahapan ini dijalankan untuk mendapatkan bentuk terbaik dari sistem yang akan dibangun berdasarkan beberapa masalah dan kebutuhan user yang telah dijelaskan sebelumnya. Upaya yang dilakukan adalah dengan berusaha mencari kombinasi penggunaa teknologi perangkat keras (*hardware*) dan perangkat lunak (*software*) yang tepat sehingga diperoleh hasil yang optimal dan mudah untuk diimplementasikannya.

Aplikasi yang akan dibuat merupakan aplikasi yang diterapkan pada perangkat mobile berbasis Android dan memiliki fungsi untuk enkrip dan dekrip pesan. Aplikasi yang akan dibuat harus dapat melakukan pengiriman pesan email lalu di enkripsi dan penerimaan pesan yang terenkripsi dapat di dekripsi tanpa adanya perubahan dari isi pesan email tersebut, aplikasi yang akan dibuat merupakan aplikasi yang digunakan untuk berkomunikasi.



Gambar 1 : Rancangan Umum Aplikasi

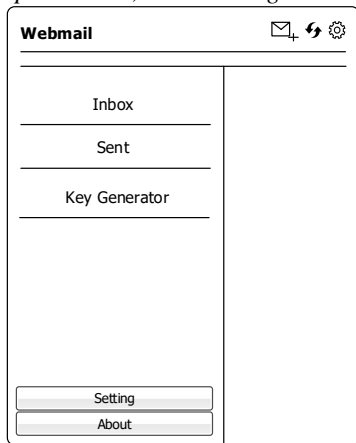
#### 3.2. Rancangan Layar

Dalam membuat suatu aplikasi diperlukan rancangan layar. Rancangan layar ini harus bersifat sederhana dan mudah dimengerti, agar dalam menggunakan aplikasi ini pengguna atau *user* merasa mudah dalam mengoperasikan aplikasi ini. Dan rancangan layar tidak boleh membingungkan si pengguna atau *user* saat mengoperasikannya. Rancangan layar dibawah ini adalah rancangan layar dari menu – menu yang ada pada aplikasi enkripsi *email* pada telepon genggam berbasis Android yang penulis buat.

##### 3.2.1. Layar Form Menu Utama

Pada rancangan layar berikut ini adalah gambar rancangan layar Menu Utama. Menu ini ada

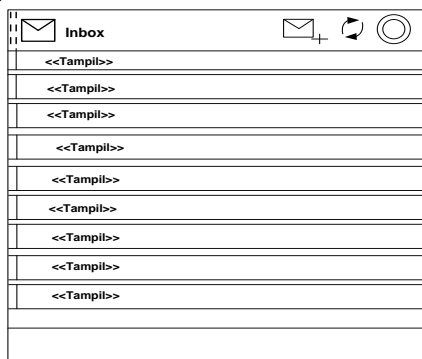
setelah pengguna melakukan *log in* di menu *setting* pada aplikasi ini. Menu utama berisi *menu inbox, sent items, compose email*, menu *setting* dan menu *about*.



Gambar 2 : Form Menu Utama

### 3.2.2. Layar Form Menu Inbox

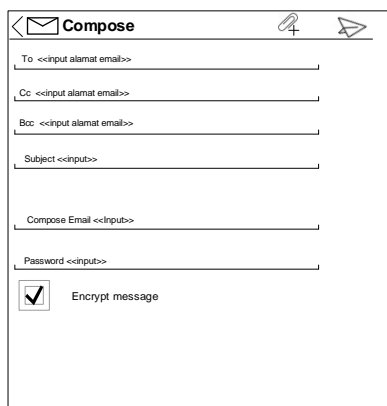
Didalam menu ini terdapat email-email yang sudah masuk. Dan jika kita membuka isi inbox maka akan tampil form atau button untuk melakukan dekrip pesan.



Gambar 3 : Form Menu Inbox

### 3.2.3. Layar Form Compose Email

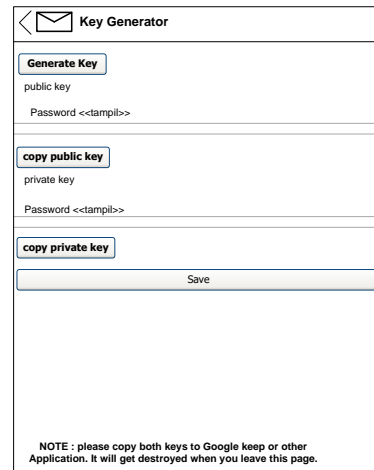
pengguna bisa mengirimkan *email* berupa file maupun hanya teks saja. Dan di menu ini *user* bisa menentukan *email* yang dikirim mau dienkripsi atau tidak.



Gambar 4 : Layar Form Compose Email

### 3.2.4. Layar Form Generate Key

Rancangan layar ini berisi tentang pembuatan *password* untuk enkrip dan dekrip. Didalam form ini terdapat *public key* dan *private key*

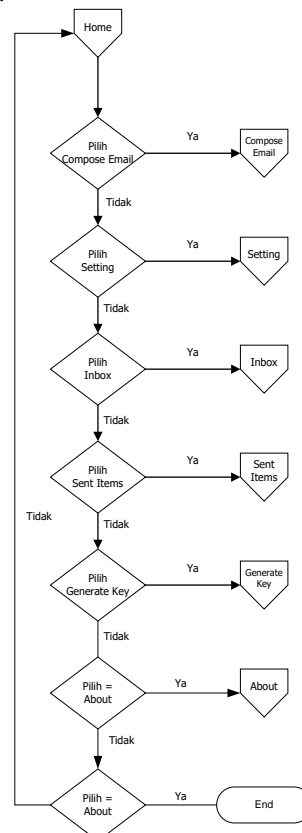


Gambar 5 : Layar Form Generate Key

## 3.3. Flowchart

### 3.3.1. Flowchart Form Menu Utama

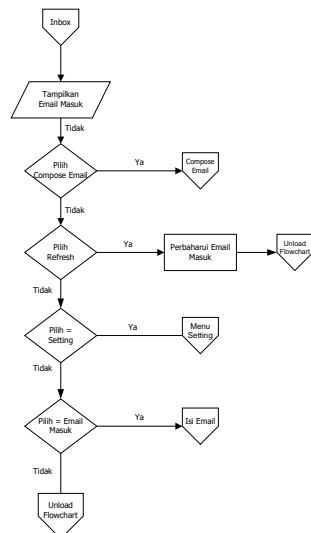
Pada gambar berikut ini adalah gambar *Flowchart form* menu utama. Proses alur didalam menu utama. Di proses ini terdapat menu menu seperti *form menu compose email, form menu inbox, form menu setting, form menu sent items*, dan *form menu about*.



Gambar 6 : Flowchart Form Menu Utama

### 3.3.2. Flowchart Form Menu Inbox

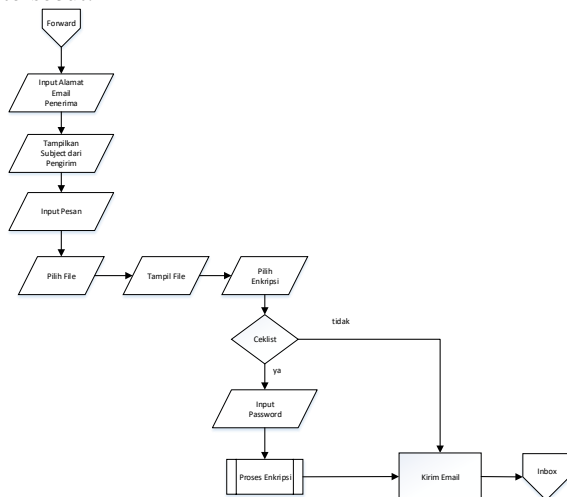
*Flowchart Menu inbox* dibawah ini adalah proses alur proses pada menu *inbox*. Didalam proses ini terdapat proses seperti proses *setting, compose email*.



Gambar 7 : Flowchart Form Menu Inbox

**3.3.3. Flowchart Form Compose Email**

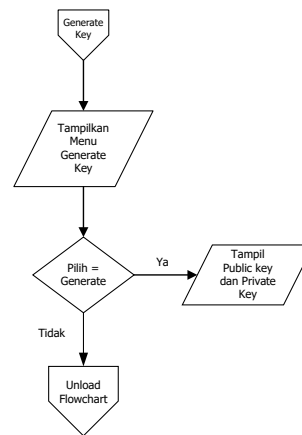
Flowchart ini menjelaskan bagaimana cara pengguna aplikasi mengirim pesan dengan aplikasi ini. user *input* alamat yang dituju untuk dikirimkan serta *input* subject email. Dapat juga memilih file dan terdapat pilihan (berbentuk *Checkbox*) untuk menentukan pesan yang dikirim butuh enkripsi atau tidak. Sebelumnya *input* password untuk enkrip email tersebut.



Gambar 8 : Flowchart Form Compose Email

**3.3.4. Flowchart Form Generate Key**

Flowchart ini menjelaskan alur proses dari pembentukan *public key* dan *private key*. Dimana sebelum proses enkrip dan dekrip *password*nya dibuat di form ini.



Gambar 9 : Flowchart Form Generate Key

**4. IMPLEMENTASI DAN ANALISA HASIL UJI COBA APLIKASI**

**4.1. Pendahuluan Implementasi Aplikasi**

Pada pengimplementasian dan analisa program akan dilakukan pengujian serta analisa program dari aplikasi enkripsi *email* pada perangkat *mobile*. Tujuannya adalah untuk mengukur sejauh mana aplikasi kriptografi ini dapat menyelesaikan masalah yang ada. Untuk mengetahui hal tersebut perlu dilakukan implementasi dan analisa hasil uji coba program. Dengan adanya pengimplementasian dan uji coba ini dapat mempermudah pengguna untuk melihat adanya kekurangan pada aplikasi yang telah dibuat dan apakah aplikasi ini dapat digunakan sesuai tujuannya dibuat yaitu untuk menyelesaikan masalah yang telah dirumuskan diawal. Selain itu uji coba aplikasi juga membantu pengguna untuk mengetahui cara kerja aplikasi, cara penggunaan, proses yang berlangsung dan hasil yang dikeluarkan oleh aplikasi.

Dengan demikian maka pengguna akan benar benar tahu tentang spesifikasi dan karakter aplikasi sehingga bisa memanfaatkan aplikasi dengan lebih maksimal. Serta dengan mengamati kekurangan dari aplikasi yang telah dibangun ini, maka bisa dijadikan sebagai acuan untuk pengembangan yang lebih baik dan lebih luas dikemudian hari. Sehingga aplikasi ini terus berkembang dan dapat menyelesaikan masalah yang lebih kompleks.

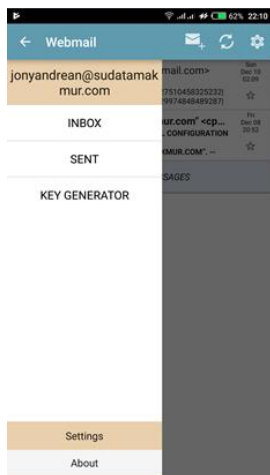
**4.2. Implementasi Program**

hal utama yang perlu diperhatikan adalah tampilan layar dan proses program. Adapun cara penggunaan aplikasi ini dan tampilan yang akan muncul saat aplikasi dijalankan akan dijelaskan sebagai berikut :

**4.2.1. Tampilan Menu Home**

Gambar dibawah adalah tampilan layar menu *home* atau *fragment email*. Untuk memunculkan layar ini adalah jika pengguna sudah melakukan proses *log in* dan masuk ke dalam menu *inbox* maka pengguna bisa geser ke kanan pada kiri layar aplikasi. Di dalam menu home ini terdapat *menu inbox*, *sent item*, *trash* (pesan terhapus), *setting*, *about* dan *compose email*.





Gambar 10 : Tampilan Layar Menu Home

#### 4.2.2. Tampilan Menu Inbox

Gambar dibawah ini adalah tampilan layar dari menu *inbox*. Menu *inbox* ini muncul jika pengguna sudah melakukan *log in*. Di menu *inbox* ini pengguna juga bisa langsung ke menu *compose email* ataupun setting yang ada di kanan atas tampilan layar. Didalam menu *inbox* ini terdapat *email* masuk yang ditujukan ke pengguna.

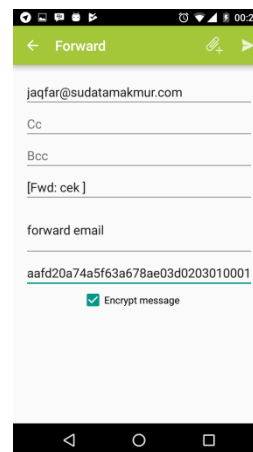


Gambar 11 : Tampilan Layar Menu Inbox

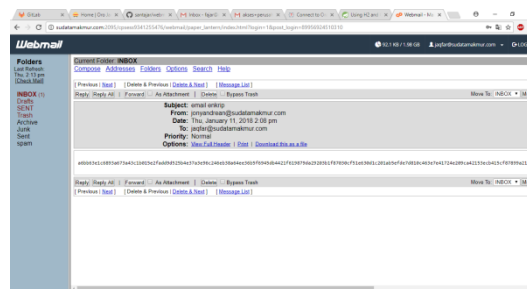
### 4.3. Analisa Hasil Implementasi dan Uji Coba Aplikasi

#### 4.3.1 Hasil Uji Email

Gambar berikut ini adalah gambar hasil uji coba pengiriman *Email* yang di enkripsi, dikirim ke alamat *email* [dwiiyanto.siguit@gmail.com](mailto:dwiiyanto.siguit@gmail.com). Dan gambar kotak masuk *email* [dwiiyanto.siguit@gmail.com](mailto:dwiiyanto.siguit@gmail.com). Ini membuktikan bahwa *email* yang dikirim berupa enkrip dan diterima juga berupa enkrip. Berikut adalah gambarnya.

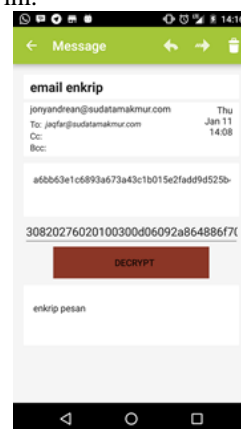


Gambar 12 : Hasil kirim Email



Gambar 13 : Hasil Enkrip Inbox Email

Setelah email diterima oleh *user* maka isi *email* akan di dekrip. Dan hasil dekripsi akan terlihat seperti gambar dibawah ini.



Gambar 14 : Hasil Dekrip Email

#### 4.3.2. Kelebihan

1. Bersifat efisien dan fleksibel Karena terpasang di *mobile phone*
2. *Password* yang di-*input* telah di enkripsi
3. Bisa dijadikan alternatif pengiriman pesan atau data

#### 4.3.3. Kekurangan

1. Harus *copy password* di hasil proses enkrip untuk dikirimkan kepada penerima agar bisa melakukan dekripsi
2. Kurang berjalan dengan baik pada android versi lama, bahkan ada kemungkinan tidak dapat di-*install*

3. Proses enkripsi yang kurang maksimal

#### 4.4. PENUTUP

##### 4.4.1. Kesimpulan

Setelah melewati beberapa proses perancangan, pembuatan, serangkaian uji coba dan analisa program enkripsi *email* pada perangkat *mobile* ini, maka dapat ditarik kesimpulan :

- a. Dengan adanya aplikasi ini, informasi atau data penting dapat lebih terjaga kerahasiaannya saat di kirim.
- b. Aplikasi ini memberikan inovasi yang menarik untuk digunakan oleh user.
- c. Aplikasi ini sangat efisien jika digunakan di zaman sekarang yang membutuhkan segala sesuatu secara cepat dan efisien.
- d. Aplikasi ini dilengkapi enkripsi *key* sebelum pesan tersebut diacak bit bit di dalamnya, agar lebih terjaga kerahasiaan dari suatu data.
- e. Penggunaan algoritma ElGamal dapat diimplementasikan ke dalam aplikasi.

##### 4.4.2. Saran

Berdasarkan hasil pembuatan aplikasi android ini , muncul beberapa saran agar perancangan ini dapat dilanjutkan untuk pengembangan selanjutnya, antara lain :

- a. Untuk *password* dekripsi bisa dibuat lebih sederhana.
- b. Dibuat lebih menarik untuk tampilan menunya.
- c. Untuk kedepannya bisa ditambahkan aplikasi *chat* enkripsi.

## 5. DAFTAR PUSTAKA

- [1] Sadikin,R., 2012, *Kriptografi Untuk Keamanan Jaringan*, Yogyakarta: Andi.
- [2] Munir,R., 2006, *Kriptografi*, Bandung: Informatika.
- [3] Riyanto,M., 2007, *Pengamanan Pesan Rahasia Menggunakan Algoritma Kriptografi ElGamal*, Yogyakarta: Departemen Pendidikan Nasional, Universitas Gajah Mada.
- [4] Ariyus,D., 2008, *Pengantar Ilmu Kriptografi: Teori, Analisis, dan Implementasi*, Yogyakarta: Andi.
- [5] Mahmuzallani, Hendrawaty dan Azhar, 2016, *Implementasi Kriptografi Pada Aplikasi Email Menggunakan Algoritma ElGamal Berbasis Android*. Jurnal Infomedia 1(1).
- [6] Hartono, J., 2005, *Analisis dan Desain Sistem Informasi: Pendekatan Terstruktur Teori dan Praktek Aplikasi Bisnis*, Yogyakarta: Andi.

[7] Harahap, S., 2012, *Pemrograman Aplikasi Mobile Smartphone dan Tablet PC Berbasis Android*, Bandung: Informatika.

[8] Paryati, 2008, *Keamanan Sistem Informasi*, Yogyakarta: Seminar Nasional Informatika., UPN "Veteran".