Pengamanan Email Menggunakan Algoritma RSA dan *Digital Signature* SHA-1 Berbasis *Mobile*

Nuri Wiyono[1], Mardi Hardjianto[2]

[1]*Program Studi Magister Ilmu Komputer, Universitas Budi Luhur*
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
nuriw23@gmail.com

[2]*Fakultas Teknologi Informasi, Universitas Budi Luhur*
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
Mardi.hardjianto@budiluhur.ac.id

ABSTRAK

Saat ini, pengiriman data banyak menggunakan media internet salah satunya menggunakan email. Dengan menggunakan email memungkinkan pengiriman data jarak jauh yang relative cepat dan murah. Di lain pihak pengiriman data melalui media internet sangat memungkinkan pihak lain dapat menyadap dan mengubah data yang dikirimkan. Pengiriman informasi melalui email menyimpan potensi berbahaya, penyalahgunaannya dapat merugikan pengirim maupun penerima pesan. Masalah keamanan dan kerahasiaan data merupakan salah satu aspek yang sangat penting dari suatu sistem informasi. Untuk mengatasi masalah ini perlu dibuatkan sistem untuk mengamankan dan menjaga keaslian isi email, yaitu dengan menggunakan teknik enkripsi. Pada penelitian ini digunakan metode enkripsi asimetris RSA serta tanda tangan digital SHA-1 dalam pengamanan isi pesan email. Dengan algoritma kriptografi ini dapat memberikan solusi pada masalah keamanan data, yaitu masalah kerahasiaan, integritas, otentikasi serta pesan dapat terjaga keasliannya oleh pihak yang tidak bertangguang jawab.

Kata kunci : kriptografi, email, RSA, SHA-1, keamanan, enkripsi

1. PENDAHULUAN

Perkembangan teknologi informasi sangatlah cepat seiring dengan semakin meningkatnya aktivitas penggunaan internet akhir-akhir ini. Pengiriman data pun sudah banyak menggunakan media internet, salah satunya adalah menggunakan media email. Dengan menggunakan email memungkinkan pengiriman data jarak jauh yang relatif cepat dan murah. Apalagi dengan perkembangan teknologi *mobile communication* saat ini, hampir setiap *mobile device* telah dilengkapi dengan fasilitas internet, sehingga dapat mengirim email kapan saja dan dimana saja. Hal ini dapat membuat pengiriman informasi dengan lebih efektif dan efisien.

Di lain pihak pengiriman data melalui media internet sangat memungkinkan pihak lain dapat menyadap dan mengubah data yang dikirimkan. Penyadapan sering dilakukan jika pengguna email menggunakan akses internet publik seperti warnet, area hotspot, dan lain-lain. Cara mengatasi hal tersebut adalah dengan mengenkripsi email yang akan dikirimkan. Dengan dienkripsi isi informasi tersebut tidak dapat diketahui oleh orang yang tidak berhak mengetahuinya.

Masalah keamanan dan kerahasiaan data merupakan salah satu aspek yang sangat penting dari suatu sistem informasi. Dalam teknologi informasi, telah dikembangkan cara-cara untuk menangkal berbagai bentuk serangan semacam itu. Salah satu cara yang ditempuh mengatasi masalah ini ialah dengan menggunakan kriptografi yang menggunakan transformasi data sehingga data yang dihasilkan tidak dapat dimengerti oleh pihak ketiga. Algoritma kriptografi ini dapat memberikan solusi pada masalah keamanan data, yaitu masalah kerahasiaan (confidentiality), integritas (integrity) dan otentikasi (authentication). Kerahasiaan mengandung arti bahwa data yang dikirimkan hanya dapat dimengerti informasinya oleh penerima yang sah. Sedangkan keotentikasian mencegah pihak ketiga untuk mengirimkan data yang salah atau mengubah data yang dikirimkan.

Pada Penelitian ini dirancang sebuah aplikasi yang melakukan metode enkripsi -dekripsi menggunakan algoritma RSA serta menggunakan tanda tangan digital SHA-1 pada isi pesan bertipe *plaintext*. Dengan menggabungkan kelebihan dari masing-masing algoritma tersebut akan memiliki tingkat keamanan cukup tinggi. Dengan dienkripsi keamanan dalam mengirim dan menerima email akan lebih terjamin, walaupun pesan email bisa diambil oleh orang lain tetapi mereka tetap tidak akan bisa membacanya karena teks tertampil dalam bentuk *chipertext*. Pesan yang dienkripsi hanya dapat dibaca oleh orang yang memiliki *private key* itu sendiri.

1.1 Identifikasi Masalah

Dari latar belakang tersebut, terdapat beberapa permasalahan yang yang ada saat ini yang menjadi tantangan untuk diselesaikan, yaitu:

1) Kurangnya keamanan dalam melakukan pertukaran informasi melalui email .
2) Tidak adanya jaminan kerahasiaan dalam pertukaran data melalui email.
3) Mudahnya isi email diketahui oleh orang lain yang tidak berhak.

2. LANDASAN TEORI

2.1. Email

Electronic-Mail (E-Mail) adalah sarana kirim mengirim surat melalui jalur jaringan komputer atau internet. Email merupakan salah satu aplikasi TCP/IP yang paling banyak digunakan . Secara teknis email terdiri dari tiga bagian[5] yaitu: header,body,attachment.

1) *Simple Mail Transfer Protocol* (SMTP).

   Simple Mail Transfer Protocol (SMTP) adalah sebuah protokol yang digunakan untuk mengirimkan email. Port standar yang digunakan pada SMTP adalah port 25, port 465, dan port 587.

2) *Instant Messaging Access Protocol (IMAP)*

   Instant Messaging Access Protocol (IMAP) adalah sebuah protokol yang digunakan untuk menerima email.Port standar yang digunakan pada IMAP adalah port 143 dan port 993.

3) *Post Office Protocol version 3 (POP3*)

   Post Office Protocol version 3 adalah suatu protokol yang berfungsi untuk menarik atau mengambil email dariserver email yang digunakan.

2.2. Kriptografi

Kriptografi (*cryptography*) merupakan ilmu dan seni penyimpanan pesan, data,atau informasi secara aman. Kriptografi berasal dari bahasa Yunani yaitu dari kata *Crypto* dan *Graphia* yang berarti tulisan rahasia. Kriptografi adalah ilmu dan seni untuk menjaga kerahasian pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Kriptografi bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah.

Berdasarkan kunci yang digunakan algoritma kriptografi dapat dibagi mejadi dua, yaitu algoritma simetris dan algoritma asimetris.[1]

2.3. Algoritma RSA

Algortima RSA dijabarkan pada tahun 1977 oleh tiga orang : Ron Rivest, Adi Shamir dan Len Adleman dari Massachusetts Institute of Technology. Huruf RSA itu sendiri berasal dari inisial nama mereka (Rivest—Shamir—Adleman). Algoritma tersebut dipatenkan oleh Massachusetts Institute of Technology(MIT) pada tahun 1983 di Amerika Serikat sebagai U.S. Algoritma RSA menjadi salah satu algoritma asimetris yang popular dan bahkan masih banyak digunakan hingga saat ini. Dalam algoritma RSA ada tiga proses yaitu proses pembangkitan kunci, proses enkripsi, dan proses dekripsi. Pada proses pembangkitan kunci akan menghasilkan dua buah kunci yaitu kunci private yang digunakan untuk proses dekripsi dan kunci public yang digunakan untuk proses enkripsi.

2.4. Fungsi Hash Satu arah

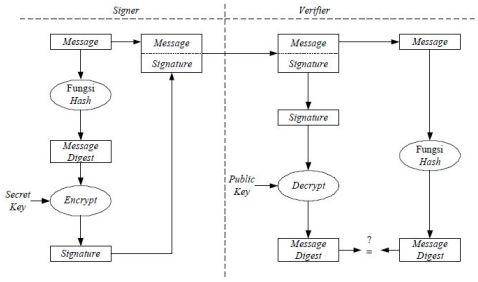
Fungsi hash memiliki algoritma yang iterative dan searah, yang dapat memproses pesan yang diberikan untuk menghasilkan representasi yanglebih pendek yang disebut message digest. Untuk menghasilkan nilai messagedigest dari pesan besar, fungsi hash menerima masukan berupa isi blok pesan saatini serta nilai hash dari blok pesan sebelumnya.Pesan yang sudah diubah menjadi message digest oleh fungsihash tidak dapat dikembalikan lagi menjadi bentuk digunakan algoritma dan kunci yang sama. Sembarang pesan yang berukuran apapun diubah oleh fungsihash menjadi message digest yang berukuran tetap.Beberapa contoh algoritma hash antara lain MD4 ,MD5 ,SHA-0,SHA-1,SHA-256,SHA-512 dan lain-lain. Hash biasa digunakan orang untuk:

a) Menyimpan *Password.*
b) Sebagai *Message Integrity*
c) Sebagai *Message Fingerprint*

2.5. Tanda Tangan Digital

Tanda tangan digital (*Digital Signature*) merupakansuatu nilai kriptografis yang bergantung pada pesan dan pengirim pesan.Tanda tangan digital ini digunakan untuk membuktikan keaslian identitas pengirim pesan dan juga untuk memastikan keaslian pesan yang dikirim.Tanda tangan digital dirancang untuk mengamankan data dari jenis serangan aktif maupun serangan pasif.[7]

Pemberian tanda tangan digital pada suatu pesan dapat dilakukan dengan cara ditambahkan secara langsung kedalam pesan, ataupun dengan cara terpisah dari pesan yang kemudian akan dikirimkan secara bersamaan dengan pesan tersebut.



Gambar 1. Ilustrasi tanda tangan digital

2.6. Java

Java menurut definisi dari Sun adalah nama untuk sekumpulan teknologi untuk membuat dan menjalankan perangkat lunak pada komputer standalone ataupun pada lingkungan jaringan. Java berdiri di atas sebuah mesin interpreter yang diberi nama Java Virtual Machine (JVM). JVM inilah yang akan membaca bytecode dalam file .class dari suatu program sebagai representasi langsung program yang berisi bahasa mesin. Oleh karena itu, bahasa Java disebut sebagai bahasa pemrograman yang portable karena dapat dijalankan pada berbagai sistem operasi, asalkan pada sistem operasi tersebut terdapat JVM. Agar sebuah program Java dapat dijalankan, maka file dengan ekstensi .java harus dikompilasi menjadi file bytecode. Untuk menjalankan bytecode tersebut dibutuhkan JRE (Java Runtime Environtment)

2.7. Android

Android adalah sistem operasi yang berbasis Linux yang dirancang untuk perangkat mobile smartphone dan komputer tablet. Android menyediakan platform terbuka bagi para pengembang untuk menciptakan aplikasi mereka sendiri untuk digunakan oleh berbagai macam perangkat mobile.Android menyediakan developing tools tersendiri untuk para pengembang aplikasi

2.8. Kualitas Perangkat Lunak

The Institute of Electrical and Electronic Engineers (IEEE) mendefinisikan kualitas perangkat lunak adalah tingkat pada system, komponen atau proses yang sesuai kebutuhan atau harapan dari pelanggan. Menurut definisi dalam Steve McConnell's Code Complete membagi perangkat lunak ke dalam dua hal yaitu: internal dan external quality characteristics. Karakteristik kualitas eksternal merupakan bagian-bagian dari suatu produk yang berhubungan dengan para pemakainya, sedangkan karakteristik kualitas internal tidak secara langsung berhubungan dengan pemakai.

2.9. Pengujian Sistem

Dalam pengembangan atau pembuatan suatu sistem ada langkah-langkah yang membentuk suatu lingkaran yang saling terhubung satu dengan lainnya.Komponen-komponen dalam lingkaran tersebut adalah perencanaan, desain, implementasi, pengujian atau testing dan yang terakhir adalah pengembangan. Lingkaran yang terbentuk disebut dengan nama*Software Development Life Cycle*.[8]

Pada tahap pengujian sistem, ada banyak modul yang biasa digunakan untuk menentukan sistem yang telah dibuat tersebut layak atau tidak untuk digunakan. Salah satu modul untuk menentukan hal tersebut adalah ISO 9126.

ISO 9126 adalah suatu standar internasional untuk menilai kualitas *software*.Pada awalnya ISO 9126 dibuat pada tahun 1991, kemudian diperbaharui pada tahun 2004. ISO 9126 berisikan empat komponen penilaian kualitas *software*, diantaranya adalah kualitas model, kualitas internal, kualitas eksternal dan kualitas penggunaan.

Pada kualitas model, klasifikasinya dibagi kedalam enam bagian struktur karakteristik[2], antara lain :

a) *Functionality* (fungsionalitas).
b) *Reliability* (keandalan).
c) *Usability* (kegunaan).
d) *Efficiency* (efisiensi).
e) *Maintainability*
f) *Portability*

2.10. Penelitian Terkait

Berikut adalah ringkasan dari beberapa penelitian sebelumnya yang berkaitan dengan keamanan pengiriman pesan rahasia dengan teknik kriptografi :

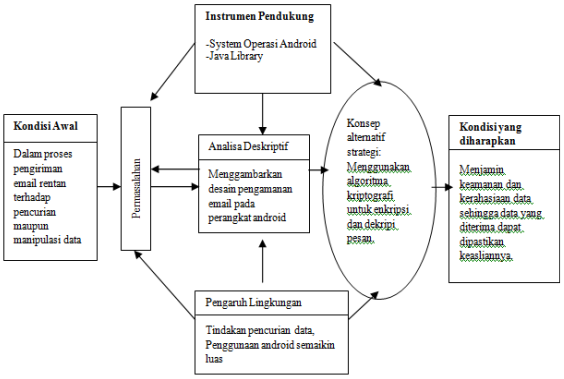
1) Pada penelitian yang dilakukan oleh Indra Lasmana, dengan menggunakan kriptografi algoritma RSA dan fungsi hash MD5 sebagai tanda tangan digital pada web service, disebutkan dalam penelitian tersebut dapat meningatkan keamanan dan kerahasiaan data akademik[4].
2) Pada penelitian yang dilakukan oleh Sasono Wibowo dan Suprayogi, yang berjudul Aplikasi Enkripsi Email dengan Mengguakan Metode Blowfish berbasis J2SE. Dalam penelitiannya dengan menggunakan enkripsi dapat melakukan pengamanan terhadap informasi atau pesan pada email.[10]
3) Pada penelitian yang dilakukan Saoji, Nikita B. Agarwal, Mrunal B. Bokil, Ashwini V. Gosavi yang berjudul *Securing e-mails in XML format using colors and Armstrong numbers,* disebutkan dalam penelitan tersebut dengan menggunakan kunci yang melibatkan sejumlah bilangan Armstrong dan warna dapat meningkatkan keamanan dan fleksibilitas yang lebih tinggi.[6]
4) Pada penelitian yang dilakukan oleh Aeni Jamilia pada layanan e-mail sebagai upaya peningkatan jaminan keamanandalam transaksi informasi secara online dengan implementasi protokol S/MIME seperti confidentiality, integrity, authentication dan non-repudiation pada tanda tangan digital dengan metode kriptografi dapat memberikan aspek keamanan informasi yang lebih baik.[3]

2.11. Tinjauan Objek Penelitian

Pada penelitian tesis ini obyek penelitian yang akan menjadi fokus bagi penulis adalah pengamanan pesan email dengan penggunakan kriptografi RSA yang disertai tanda tangan digital.

Sebelum ditransmisikan pesan akan dienkrpsi terlebih dahulu menggunakan kunci *public*.

2.12. Pola Pikir



Gambar 2. Kerangka pemikiran

2.13. Hipotesis

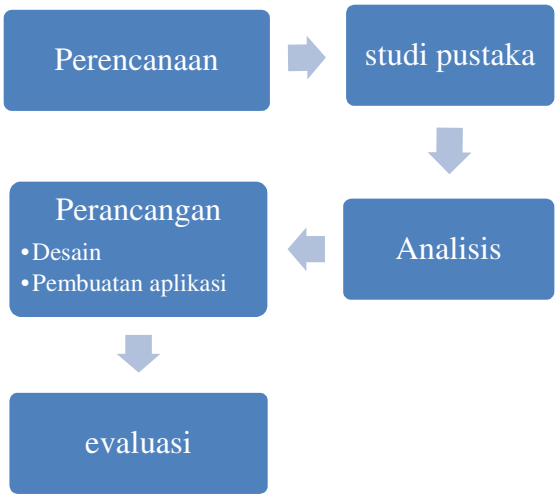
Hipotesis dari penelitian tesis ini yaitu pengamanan email dengan menggunakan kriptografi RSA serta fungsi hash SHA-1 sebagai tanda tangan digital, diduga dapat meningkatkan keamanan dalam pengiriman email agar pesan yang dikirim tidak dapat diketahui oleh orang yang tidak berhak serta dapat diketahui jika pesan tersebut mengalami perubahan pada saat proses pengiriman.

3. METODOLOGI PENELITIAN

3.1. Metode Penelitian

Dalam penelitian ini, metode yang digunakan adalah metode penelitian eksperimen.Penelitian eksperimen adalah penelitian dimana peneliti dapat melakukan manipulasi variabel bebas sesuai keinginan peneliti.[9]. Eksperimen dalam penelitian ini bertujuan untuk membangun sebuah aplikasi pengamanan pesan email pada perangkat mobile berbasis Android menggunakan kriptografi RSA disertai tanda tangan digital menggunakan SHA-1 yang diharapkan dapat memenuhi seluruh aspek keamanan informasi.

Pada penelitian ini, peneliti menggunakan tahapan-tahapan yang dapat dilihat dari gambar berikut ini :



Gambar 3. Tahapan-tahapan penelitian

3.2. Teknik Analisis, Perancangan dan Pengujian

1) Teknik Analisis

Menganalisa spesifikasi kebutuhan sistem, yaitu melakukan perincian mengenai apa saja yang dibutuhkan dalam pengembangan sistem dan membuat perencanaan yang berkaitan dengan proyek sistem. Selain menganalisa spesifikasi kebutuhan system, juga perlu dilakukan analisa kebutuhan fungsional dan kebutuhan non-fungsional sistem. Kebutuhan fungsional adalah kebutuhan yang berisikan proses-proses apa saja yang diberikan oleh perangkat lunak yang akan dibangun. Kebutuhan fungsional ini berhubungan dengan fitur perangkat lunak yang ingin dibangun, sedangkan kebutuhan non fungsional tidak secara langsung terkait pada suatu fitur yang ada didalam perangkat lunak.

Pada penelitian ini kebutuhan fungsional sistem atau perangkat lunak yang dibangun adalah sebagai berikut :

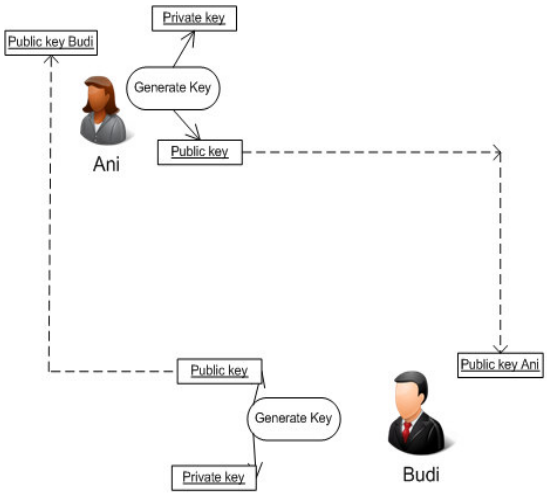
a. Sistem dapat mengirim text ke email tujuan.
b. Sistem dapat menggenerate kunci public dan kunci privete.
c. Sistem dapat menyimpan kunci *private* dan *public* hasil generate.
d. Sistem dapat mendistribusikan kunci *public* ke teman yang akan melakukan pertukaran informasi/ pesan melalui email.
e. Sistem dapat menyimpan kunci *public* dari orang yang akan diajak untuk saling berkirim email.
f. Sistem dapat menenkripsi plaintext.
g. Sistem dapat mendekripsi balik plaintext yang telah dikirim.

Sedangkan untuk kebutuhan non fungsional pada penelitian ini adalah performasi.

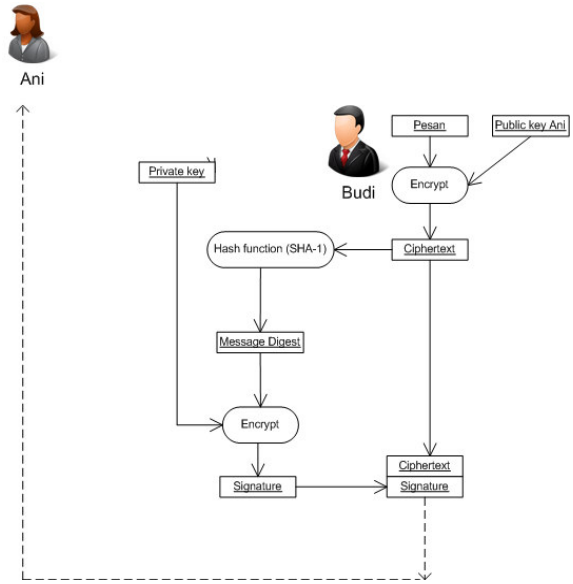
2) Perancangan

Perancangan yaitu membuat desain aliran kerja manajemen dan desain pemrograman yang diperlukan untuk pengembangan sistem. Pada tahap ini dilakukan perancangan interface yang digunakan pada software, serta perancangan alur proses yang akan digunakan pada sistem sehingga semua langkah yang ada dalam aplikasi email client dapat dijalankan sesuai dengan kebutuhan. Membuat desain interface berbasis GUI (Graphical User Interface) dengan mempertimbangkan aspek kemudahan user.

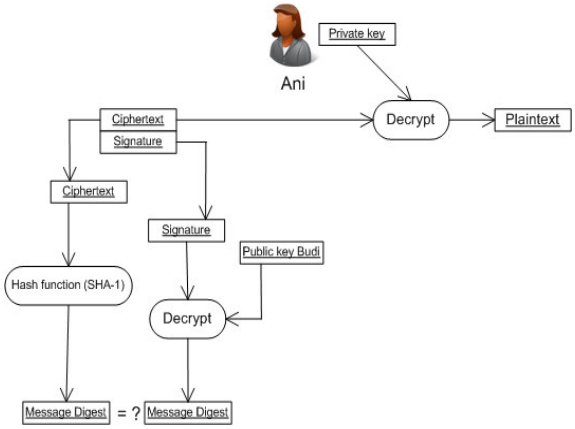
Perancangan dilakukan dengan membuat desain *workflow* terhadap sistem dan pemrograman yang diperlukan dalam penelitian. Proses desain menterjemahkan syarat atau kebutuhan ke dalam sebuah representasi aplikasi yang sudah di analisa sebelumnya.



Gambar 4. Proses distribusi *key*



Gambar 5. Proses enkripsi dan pengiriman pesan



Gambar 6. Proses dekripsi

3) Pengujian Sistem

Pengujian sistem dilakukan dengan tujuan untuk menjamin sistem yang dibuat sesuai dengan hasil analisis dan perancangan serta menghasilkan satu kesimpulan apakah sistem tersebut sesuai dengan yang diharapkan. Untuk itu dibutuhkan sebuah metode pengujian yang menjadi ukuran atau parameter sehingga dapat ditarik kesimpulan bahwa sistem memang telah berjalan sesuai dengan tujuan. Pada penelitian ini metode yang digunakan dalam pengujian diantaranya sebagai berikut:

a) Pengujian dengan ISO 9126

Pengujian sistem berdasarkan empat karakteristik yang terdapat pada ISO 9126, yaitu fungsionalitas, kehandalan, kebergunaan dan efisiensi dilakukan dengan menjalankan sistem.

b) Pengujian dengan Blackbox testing

Pengujian teknik Blackbox ini digunakan untuk menemukan kesalahan dan mendemonstrasikan fungsional aplikasi saat

dioperasikan, apakah input diterima dengan benar dan output yang dihasilkan telah sesuai dengan yang diharapkan sehingga dapat diketahui jika terjadi kesalahan.

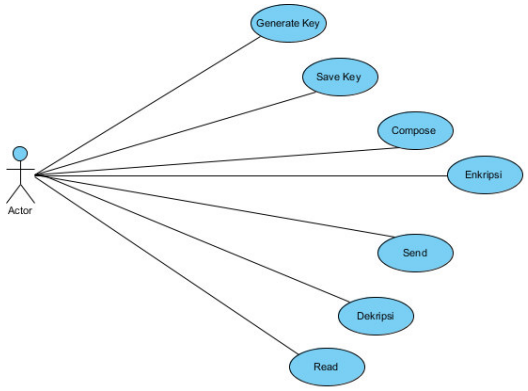
4. PEMBAHASAN HASIL PENELITIAN

4.1. Analisa

Pada penelitian ini untuk mendapatkan kebutuhan dalam perancangan sistem, peneliti menggunkan *Unified Modeling Language* (UML). Dengan menggunakan UML diharapkan dapat menampilkan kebutuhan sistem berupa interaksi sistem dengan lingkungannya, fungsi dan tahapan proses sistem. Hasil akhir adalah spesifikasi kebutuhan perangkat lunak yang akan dibagun.

1) Use Case Diagram

Use Case Diagram menggambarkan interaksi antara sistem dengan pengguna sistem.*Use case diagram* menggambarkan fungsionalitas yang dapat dilakukan dari sebuah sistem.*Use Case Diagram* digunakan dalam tahap perencanaan untuk mendefinisikan kebutuhan suatu sistem dan memahami bagaimana suatu system seharusnya bekerja.*Use case diagram* terdiri atas diagram untuk use case dan actor. *Actor* merupakan orang yang akan mengoperasikan atau orang yang berinteraksi dengan sistem aplikasi, sedangkan *Use case* merepresentasikan operasi-operasi yang dilakukan oleh *actor*. *Use case* digambarkan berbentuk elips dengan nama operasi dituliskan di dalamnya.*Actor* yang melakukan operasi dihubungkan dengan garis lurus ke *use case*.



Gambar 7. *Use case*

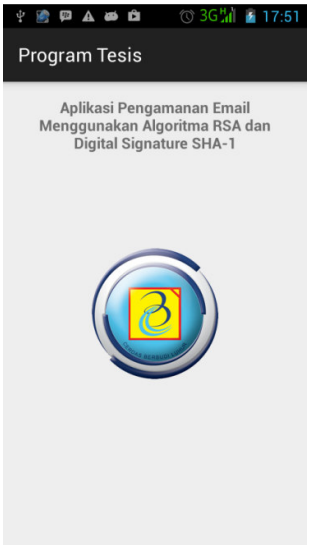
Tabel 1. Deskripsi *Use case*

No	*Use Case*	Deskripsi
1.	*Generate Key*	*Use case* ini mendeskripsikan fungsionalitas yang dimiliki aplikasi dalam membangkitkan kunci baru yang akan digunakan untuk enkripsi pesan.
2.	*Save Key*	*Use case* ini mendeskripsikan fungsionalitas yang dimiliki aplikasi dalam menympan kunci hasil generate maupun kunci dari lawan bertukar informasi/ berkirim pesan rahasia.
3.	*Compose*	*Use case* ini mendeskripsikan fungsionalitas yang dimiliki aplikasi dalam menyusun pesan yang akan dikirim.
4.	Enkripi	*use case* ini mendeskripsikan fungsionalitas yang dimiliki aplikasi dalam mengenkripsi pesan.
5.	*Send*	*use case* ini mendeskripsikan fungsionalitas yang dimiliki aplikasi dalam mengirim pesan.
6	Dekripi	*use case* ini mendeskripsikan fungsionalitas yang dimiliki aplikasi dalam mendekripsi pesan.
7.	*Read*	*use case* ini mendeskripsikan fungsionalitas yang dimiliki aplikasi dalam membaca isi pesan.

4.2. Rancangan Sistem/Prototipe Model

1) Tampilan Utama

Tampilan utama merupakan tampilan awal saat aplikasi dibuka. Terdapat enam menu pada tampila utama yaitu : *inbox, compose mail, settings, my key, friends keys,* dan *exit*.

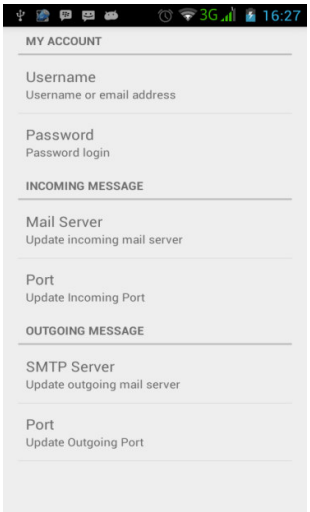


Gambar 8. Tampilan Utama

2) Setting

Setting merupakan tampilan pertama kali yang muncul saat user akan melakukan pengaturan/ konfigurasi *account* email. Pada modul setting ini dapat melakukan pengaturan yaitu *username* atau *email address*, *password, incomming message server atau SMTP, port incomming message, outgoing message server,*dan *port outgoing message*. Sebelum

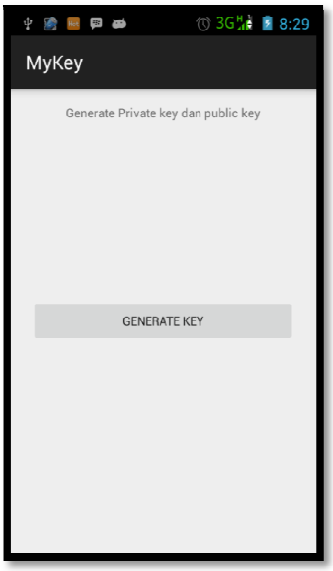
mengirim email pastikan settingan diisi terlebih dulu.



Gambar 9. Tampilan Setting konfigurasi

3) Generate Key

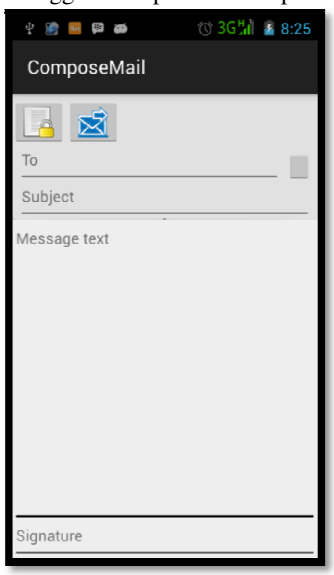
Generate key merupakan tampilan untuk pembentukan kunci *public* dan kunci *private* yang nantinya akan digunakan untuk proses enkripsi dan dekripsi. Kunci public akan di kirim ke pihak yang akan melakukan komunikasi atau pengiriman email, kunci tersebut digunakan untuk mengenkrpsi pesan sebelum pesan dikirim. Sedangkan kunci private digunakan untuk mendekripsi isi pesan(email) yang diterima.



Gambar 10.Tampilan *Generate key*

4) *Compose Mail*

Compose mail adalah tampilan untuk menyusun atau menulis isi pesan yang akan dikirim. Pada modul ini terdapat *button* enkripsi yang berfungsi untuk mengenkripsi isi pesan jika pesan sudah siap untuk dikirim, dan *button* kirim untuk mengirimkan pesan tersebut kepada alamat email yang dituju menggunakan protokol smtp.



Gambar 11. Tampilan *Compose Mail*

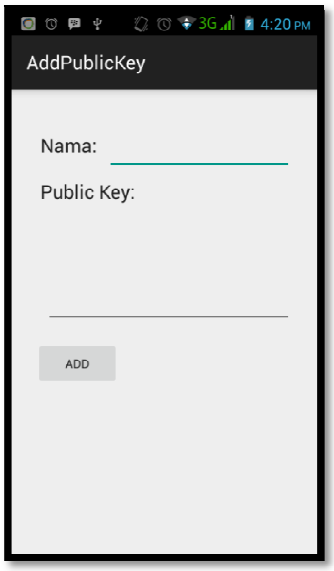
5) *List Friends Key*

List Friends Key adalah tampilan yang menampilkan list alamat email atau nama dari teman atau lawan bertukar infomasi yang sebelumnya telah didaftarkan atau *public key* nya telah ditambahkan ke dalam aplikasi.

Gambar 12. Tampilan *Friends Key*

6) *Add public key*

Add public key adalah tampilan untuk menambah atau menyimpan *public key* baru dari teman atau orang yang akan saling bertukar informasi atau pesan dengan aman menggunakan aplikasi pengamanan email.



Gambar 13. Tampilan *Add Public Key*

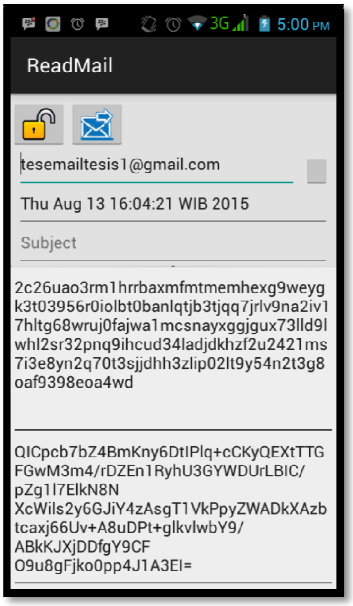
7) *Inbox*

Inbox merupakan tampilan untuk menampilkan list pesan (email) yang diterima. Pesan yang di tampilkan pada halaman ini hanya sebagian atau potongan dari keseluruhan isi email yang diterima. Klik salah satu pesan dari list tersebut untuk melihat keseluruhan isi email, maka akan tampil halaman *read mail* yang akan menampilkan isi pesan tersebut. Jika akan menampilkan pesan yang baru masuk, maka halaman *inbox* ini harus di refresh dahulu.

Gambar 14.Tampilan *Inbox*

8) *Read Mail*

Read Mail adalah tampilan untuk menapilkan isi pesan beserta *signature* yang dikirim. Pada halaman tersebut terdapat *button* untuk mendekripsi pesan *ciphertext* dan memvalidasi isi email tersebut telah mengalami perubahan atau tidak saat email tersebut ditransmisikan.



Gambar 15. Tampilan *Read Mail*

4.3. Pengujian Sistem

Pengujian dilakukan setelah melakukan pembuatan aplikasi pengamanan email menggunakan algoritma RSA dan digital signature

SHA-1.Pengujian dilakukan untuk mengidentifikasi apakah aplikasi sudah sesuai dengan kebutuhan sistem yang telah dianalisa sebelumnya.Pada penelitian ini ada beberapa pengujian yang akan lakukan, yaitu pengujian dengan menggunakan black box testing serta pengujian dengan mengadaptasi ISO 9126.

1) Pengujian dengan *Blackbox Testing*

Pengujian dilakukan untuk mengetahui apakah aplikasi yang dibangun sesuai dengan analisa kebutuhan yang telah ditentukan. Pengujian dilakukan berdasarkan skenario yang telah ditentukan dengan setiap proses dan kemungkinan kesalahan yang dapat terjadi.Setiap modul memiliki skenario test yang akan diamati saat penelitian untuk mengetahui apakah hasil yang diperoleh saat pengujian sesuai dengan yang dikehendaki atau tidak. Berikut ini akan dijelaskan hasil dari setiap pengujian.

Tabel 2. Pengujian Blackbox testing Menu Utama

No	**Skenario pengujian**	***Test Case***	**Hasil yang diharapkan**	**Sesuai / Tidak**
1.	Setelah muncul tampilan utama aplikasi klik option menu.	Klik satu kali	Akan tampil enam sub menu yaitu inbox, compose mail, settings, my key, friends keys, exit	sesuai
2.	Setelah list option menu tampil, kemudian klik menu inbox	Klik sub menu inbox	Tampilan awal akan tertutup dan akan tampil activity inbox	sesuai
3.	Setelah list option menu tampil, kemudian klik menu *compose mail*	Klik sub menu *compose mail*	Tampilan awal akan tertutup dan akan tampil activity *compose mail* (tampilan untuk menulis pesan)	sesuai
4.	Setelah list option menu tampil, kemudian klik menu *settings*	Klik sub menu *settings*	Tampilan awal akan tertutup dan akan tampil activity settings (tampilan untuk mengkonfigurasi *account* email)	sesuai
5.	Setelah list option menu tampil, kemudian klik menu *my key*	Klik sub menu my key	Tampilan awal akan tertutup dan akan tampil activity my key	sesuai
6.	Setelah list option menu tampil, kemudian klik menu *friends keys*	Klik sub menu*friends keys*	Tampilan awal akan tertutup dan akan tampil activity *friends keys*	sesuai
7.	Setelah list option menu tampil, kemudian klik menu exit.	Klik sub menu exit	Akan tampil alert dialog ya/ tidak untuk keluar dari aplikasi, jika pilih ya maka akan keluar dari aplikasi dan jika pilih tidak maka akan kembali ke tampilan awal.	sesuai

Berdasarkan hasil pengujian fungsional yang dilakukan menggunakan *blackbox testing* terlihat bahwa aplikasi pengamanan email dengan algoritma RSA dan tanda tangan digital SHA-1 untuk enkripsi dan dekripsi isi email sudah sesuai dengan uji fungsional yang dilakukan.

2) Pengujian dengan mengadaptasi ISO 9126

Pengujian perangkat lunak dengan mengadaptasi ISO 9126. Hal ini untuk menguji aplikasi dari sisi *functionality, reliability, usability*, dan *efficiency*.Pada penelitian ini pengujian menggunakan adaptasi ISO 9126 dilakukan dengan tingkat masing-masing aspek

berdasarkan empat karakteristik ISO 9126. Responden dipilih dari user yang akan berhubungan langsung dengan aplikas pengiriman email dan pengguna yang akan melakukan pengiriman email dengan aman.

Berdasarkan analisis data yang diperoleh dari kuesioner, rekapitulasi pengujian kualitas berdasarkan empat aspek kualitas berdasarkan adaptasi ISO 9126 dapat ilihat pada Tabel 3.

Tabel 3. Pengujian Tingkat kualitas perangkat lunak keseluruhan

Aspek	**Skor aktual**	**Skor ideal**	**Skor aktual**	**Kriteria**
Functionality	290	350	82,8 %	Baik
Reliability	203	250	81,2 %	Baik
Usability	160	200	80%	Baik
Efficiency	79	100	79%	Baik
Total	732	900	81,3 %	Baik

$$\% \text{ skor aktual} = \frac{732}{900} \times 100\% = 81{,}3\%$$

Dari hasil akhir pengujian didapat hasil skor sebesar 81,3% dan memiliki kriteia baik, ini berarti aplikasi yang dibuat sebagian besar sudah memenuhi kebutuhan.

4.4. Implikasi Penelitian

1) Aspek Sistem

Dalam pengoptimalan penggunaan aplikasi yang dirancang berbasis android mobile, maka pengguna sebaiknya memahami penggunaan device android secara umum sehingga akan lebih mudah dalam penggunaan aplikasi.

Pada penelitian ini dengan menggnakan device android yang memiliki spesifikasi prosesor dual-core 1.2 GHz Cortex-A5,memori 512 MB RAM, hard disk 4 GB dan sistem operasi android OS 4.1.2 Jelly Bean, proses enkripsi dan dekripsi plaintext yang dilakukan relatif cepat.

2) Aspek Penelitian Lanjutan

a) Pengembangan Metode

Penelitian selanjutnya perlu melakukan kajian pada beberapa metode kriptografi yang dapat digunakan untuk meningkatkan keamanan pada pengiriman email.Selain itu juga harus meningkatkan performa aplikasi sehingga aplikasi akan dapat digunakan dengan lebih efektif dan efisien. Selain metode kriptografi diperlukan juga metode pendistribusian kunci *public* yang efisien.

b) Pengembangan Ruang Lingkup

Penelitian ini masih memiliki banyak kekurangan.Pada penelitian selanjutnya, ruang lingkup dapat lebih diperluas agar aplikasi dapat melakukan pengamanan email dengan mengenkripsi berbagai macam bentuk file *attachment* dan aplikasi dapat dijalankan diberbagai *platform* seperti iOS dan blackberry.Hal tersebut guna untuk menambah pengembangan sistem dan dapat memberikan kemudahan dari sisi user dalam melakukan pengiriman email terenkripsi diberbagai perangkat *mobile smartphone*. Selain digunakan sebagai pengamanan email algoritma kriptografi RSA dan SHA-1 juga dapat dikembangkan untuk diterapkan pada metode pembelajaran jarak jauh(e-Learning), ujian online, tes CPNS online, transaksi perbankan, metode pengiriman arsip rahasia yang digunakan pada lembaga-lembaga negara dimana memang dibutuhkan *confidentiality, integrity, authentication* dan *non repudiation* dalam proses pengiriman datanya.

5. PENUTUP

5.1. Kesimpulan

Berdasarkan dari hasil pembahasan penelitian yang telah dilakukan sebelumnya, maka dalam penelitian Pengamanan email menggunakan algoritma RSA dan digital signature SHA-1 berbasis mobile dapat diambil kesimpulan sebagai berikut:

1) Aplikasi dapat melakukan pengamanan email dengan mengenkripsi isi pesan sebelum email ditransmisikan dengan menggunakan alogoritma RSA dan digital signature SHA-1. Aplikasi juga dapat menjaga keaslian isi dari email yang ditransmisikan.
2) Implementasi dapat berjalan dengan baik pada device android smartphone pengguna. Pada penelitian pengujian fungsional dengan menggunakan Blackbox testing.
3) Hasil pengujian menggunakan blackbox testing memperlihatkan bahwa fungsionalitas sudah berjalan sesuai yang diharapkan.
4) Berdasarkan hasil pengujian mengadaptasi ISO 9126 didapat hasil skor sebesar 81,3% dan memiliki kriteria baik, ini berarti aplikasi yang dibuat sebagian besar sudah memenuhi kebutuhan.

5.2. Saran

Selanjutnya peneliti memberikan saran yang relevan dengan hasil penelitian, implikasi dan rencana implementasi yaitu sebagai berikut :

1. Perlu dilakukan sosialisasi dalam manfaat dan cara penggunaan aplikasi terhadap pengguna, sehingga tidak terjadi kesalahan dalam penggunaan aplikasi pengamanan email tersebut.
2. Pada penelitian selanjutnya aplikasi dapat dikembangkan untuk kebutuhan lain yang memerlukan keamanan dalam proses pengiriman datanya. Seperti :ujian online, tes CPNS online, pengiriman dokumen Negara dan lain-lain.

6. DAFTAR PUSTAKA

[1] Ebrahim , Mansoor , Shujaat Khan,Umer Bin Khalid .*Symmetric Algorithm Survey: A Comparative Analysis*. International Journal of Computer Applications (0975 – 8887) Volume 61– No.20, January 2013.

[2] Haboush, Ahmad, et al. *Investigating Software Maintainability Development: A case for ISO 9126.* International Journal of Computer Science Issues, Vol. 11, Issue 2, No 2, March 2014.

[3]Jamilia, Aeni ,Moedjiono ,Hadi Syahrial. *Rancangan Implementasi Protokol S/MIME pada Layanan E-Mail Sebagai Upaya Peningkatan Keamanan dalam Transaksi Informasi Secara Online: Studi Kasus PT. XYZ.* Journal Technology of Information and Communication (TICOM). Vol 1, No 2, 2013.

[4] Lasmana, Indra, *Model Implementasi Keamanan Web Service dengan kriptografi dan Tanda Tangan Digital pada Sistem Informasi Akademik.* Universitas Budi Luhur, Jakarta, 2013.

[5]Pszota, David. *Email Communication Transformation into Knowledge Base*. Journal of Slovak University of Technology Bratislava 2012.

[6] Saoji, Nikita B. Agarwal, Mrunal B. Bokil, Ashwini V. Gosavi. *Securing e-mails in XML format using colors and Armstrong numbers.* International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July 2013.

[7] Solanki ,Chitra, Madhu Sharma, *An Efficient RSA-based and chaos-based Authentication Scheme.* International Journal of Information Systems and Computer Sciences. Volume 4, No.1, January – February 2015.

[8] Sommerville, Ian, *Software Engineering,* Erlangga Edisi 6, 2003.

[9] Wibisono, Dermawan. *Riset bisnis panduan bagi praktisi & akademisi.* Gramedia Pustaka Utama, 2003.

[10] Wibowo ,Sasono, Suprayogi , *Aplikasi Enkripsi Email dengan Mengguakan Metode Blowfish berbasis J2SE.* Techno.COM, Vol. 13, No. 2, Mei 2014.