PENGGUNAAN TEKNIK KRIPTOGRAFI *HYBRID* UNTUK PENGAMANAN SMS PADA PERANGKAT ANDROID

Nazori Agani[1], Muhammad Akbar[2]

Magister Ilmu Komputer, Program Pascasarjana, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Uttara, Kebayoran Lama, Jakarta Selatan 12260
Telp. (021) 5853753
[1]nazori@budiluhur.ac.id, [2]muh_akbar@yahoo.com

ABSTRAK

Secara umum keterbatasan layanan SMS saat ini adalah tidak terjaminnya kerahasiaan dan keutuhan pesan yang dikirim. Oleh karenanya dibutuhkan suatu sistem keamanan yang kuat untuk penyampaian pesan SMS tersebut. Untuk melindungi informasi yang sensitif yang dikirimkan melalui SMS maka perlu diterapkan hal-hal yang terkait dengan keamanan informasi yang meliputi aspek keamanan kerahasiaan (confidentiality), keutuhan (data integrity), keaslian (authentication) dan tidak terdapat penyangkalan (non-repudiation). Pada penelitian tesis ini penulis mengajukan metode pengamanan komunikasi SMS pada perangkat Android dengan menggunakan teknik kriptografi hybrid yang merupakan kombinasi dari algoritma kriptografi simetrik AES-256, algoritma asimetrik EC-Cryptography, fungsi message digest SHA-256, fungsi digital signing dan sistem pembangkit kunci acak, yang diharapkan dapat memenuhi seluruh aspek keamanan informasi. Adapun dari hasil penelitian yang telah dilakukan maka kesimpulan yang diperoleh adalah bahwa dengan metode kriptografi hybrid yang diterapkan sebagai sistem pengamanan komunikasi SMS pada perangkat Android dapat memenuhi keseluruhan aspek keamanan informasi yang terdiri dari confidentiality, data integrity, authentication, dan non-repudiation

Kata Kunci : *SMS, enkripsi, fungsi hash, kriptografi hybrid, android*

1. PENDAHULUAN

Beberapa tahun terakhir terjadi perkembangan yang pesat pada bidang teknologi, dan salah satunya adalah teknologi komunikasi. Salah satu alat komunikasi yang berkembang dan saat ini banyak digunakan adalah telepon seluler (ponsel), mulai dari ponsel yang hanya bisa digunakan untuk berbicara dan sms hingga ponsel cerdas atau *smartphone.*

SMS merupakan suatu layanan untuk mengirimkan pesan singkat kepada pengguna telepon seluler lainnya dengan cepat dan biaya yang murah. Adapun Perkembangan telepon seluler khususnya *smartphone* yang sedang populer saat ini adalah *smartphone* yang berbasis *Android*. Perkembangan *smartphone* berbasis Android ini sangat menakjubkan, dikarenakan *Android* merupakan *Operating Systen Mobile* yang *open platform*, sehingga menyajikan kemudahan dan keleluasaan bagi para pengembang aplikasi untuk membangun aplikasi pada perangkat *smartphone.*

Top Six Smartphone Mobile Operating Systems, Shipments, and Market Share, Q3 2012 (Preliminary)
(Units in Millions)

Operating System	3Q12 Shipment Volumes	3Q12 Market Share	3Q11 Shipment Volumes	3Q11 Market Share	Year-Over-Year Change
Android	136.0	75.0%	71.0	57.5%	91.5%
IOS	26.9	14.9%	17.1	13.8%	57.3%
BlackBerry	7.7	4.3%	11.8	9.5%	-34.7%
Symbian	4.1	2.3%	18.1	14.6%	-77.3%
Windows Phone 7/ Windows Mobile	3.6	2.0%	1.5	1.2%	140.0%
Linux	2.8	1.5%	4.1	3.3%	-31.7%
Others	0.0	0.0%	0.1	0.1%	-100.0%
Totals	181.1	100.0%	123.7	100.0%	46.4%

Gambar 1. Pengiriman dan *market share* sistem operasi *smartphone*[1]

Dengan *market share* yang cukup besar maka perangkat mobile berbasis android ini menjadi cukup populer digunakan oleh berbagai kalangan didunia untuk kepentingan komunikasi dan mempermudah aktivitas bagi pemakaianya. Namun seiring dengan perkembangan teknologi yang semakin canggih menimbulkan pertanyaan mengenai keamanan informasi yang dikirimkan melalui SMS. Keamanan merupakan aspek yang sangat penting dalam berkomunikasi dengan menggunakan komputer dan perangkat komunikasi lainnya. Kerahasiaan data atau informasi harus terjaga dari pihak yang tidak berwenang hingga data atau informasi tersebut terkirim kepada penerima yang semestinya. Selama beberapa tahun terakhir, ada beberapa keterbatasan pada layanan yang ditawarkan melalui SMS. Secara umum SMS tidak menjamin kerahasiaan dan keutuhan pesan yang dikirimkan oleh penggunaOleh karena pesan-pesan teks yang dikirim pengguna terkadang merupakan pesan yang rahasia dan pribadi, sehingga kerahasiaan pesan menjadi sangat penting untuk dijaga dari orang-orang yang tidak berhak mendapatkannya. Sehingga dibutuhkan suatu sistem keamanan dalam menyampaikan pesan tersebut.Untuk melindungi informasi yang sensitif yang dikirimkan melalui SMS, maka perlu diterapkan hal-hal yang terkait dengan keamanan informasi yang meliputi aspek-aspek keamanan kerahasiaan (*confidentiality*), keutuhan (*dataintegrity*), keaslian (*authentication*) dan tidak terdapat penyangkalan (*non-repudiation)*[2]. Terdapat beberapa penelitian ataupun tulisan yang telah dilakukan terkait pengamanan komunikasi SMS[3][4][5][6][7], namun penelitian tersebut belum benar-benar dapat memenuhi aspek-aspek keamanan informasi di

atas. Setelah melalui berbagai pertimbangan akhirnya penulis mengajukan solusi untuk pengamanan komunikasi SMS dengan menggunakan metode kriptografi *Hybrid* yang merupakan gabungan dari algoritma kriptografi klasik simetrik dan algoritma kriptografi modern asimetrik untuk meng-enkripsi data yang berjalan pada sistem operasi Android sehingga diharapkan dapat memenuhi aspek keamanan informasi khususnya bagi para pengguna *smartphone* berbasis Android sehingga dapat mengirim pesan dengan lebih aman.

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

a. Pada saat kita mengirim pesan SMS dari handphone, maka pesan SMS tersebut tidak langsung di kirim ke handphone tujuan, akan tetapi terlebih dahulu dikirim ke SMS Center (SMSC) dengan prinsip *Store and Forward*, setelah itu baru dikirimkan ke handphone yang dituju sehingga tidak dapat dijamin keamanannya.
b. Sistem SMS yang umum digunakan tidak memiliki proteksi terhadap keutuhan SMS tersebut sehingga isi dari SMS memungkinkan untuk di ubah atau di modifikasi baik pada saat transmisi maupun pada saat tersimpan di SMSC tanpa terdeteksi.
c. Secara umum SMS tidak memiliki sistem otentikasi pengirim sehingga tidak bisa menjamin bahwa SMS terkirim oleh pengirim yang sesuai dengan pemilik Nomer SMS pengirim.
d. SMS tidak memiliki sistem yang dapat mencegah adanya penyangkalan oleh pemilik SMS bahwa dia yang telah mengirim SMS tersebut.

Adapun dari penelitian ini diharapkan dapat memberikan pengetahuan tentang apakah dengan menggunakan teknik kriptografi *hybrid* suatu komunikasi SMS pada perangkat Android dapat memenuhi aspek-aspek keamanan informasi sehingga dapat menjamin keamanan bagi para pengguna SMS.

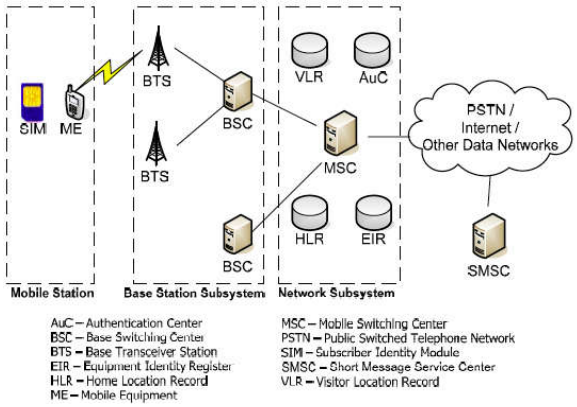
2. LANDASAN PEMIKIRAN

2.1 Tinjauan Pustaka

a. SMS

Pesan SMS yang didefinisikan oleh GSM 03,40 standar[8] sebagai pesan yang berisi dua bagian utama: *Header* dan *Payload*. SMS *header* berisi informasi yang diperlukan bagi operator untuk memberikan SMS ke penerima yang dituju. Selain itu, SMS *header* mungkin berisi beberapa informasi tambahan seperti nomor *port*. Jika *header* berisi nomor *port*, maka *payload* yang cocok dengan pesan protokol SMS akan lebih kecil. *Payload* adalah isi dari pesan, sebuah *Payload* dapat dikodekan dalam tiga pengkodean yang berbeda, 7-bit alfabet, 8-bit data biner atau 16-bit UCS-2 alfabet[9]. Pesan SMS tidak memerlukan ponsel untuk aktif dan dalam jangkauan, karena mereka akan tersimpan selama beberapa saat sampai telepon aktif dan dalam jangkauan. SMS yang dikirimkan dalam jaringan yang sama atau kepada siapa pun dengan kemampuan *roaming*. SMS adalah sebuah layanan *store and forward*, dan tidak dikirim secara langsung, tetapi dikirim melalui SMS Center (SMSC).

Sebuah sistem GSM secara khusus terdiri dari tiga subsistem: *Mobile Station*, subsistem *Base Station* dan subsistem jaringan. Gambar berikut memberikan gambaran tentnag jaringan GSM dan SMS Ceneter (SMSC)



Gambar 2. Overview jaringan *GSM* [10]

b. Kriptografi *Hybrid*

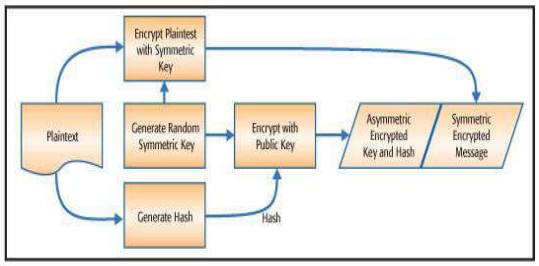
Menurut Munir [11], definisi kriptografi ada 2, yaitu :

1. "Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan".
2. "Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi sepertikerahasiaan, integritas data, serta otentikasi".

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

Protokol kriptografi yang berkembang saat ini kebanyakan menggabungkan penggunaan antara algoritma kriptografi simetrik dan asimetrik. Penggabungan kedua algoritma tersebut menghasilkan sistem yang disebut dengan *hybridcryptosystem* [12]. Pengembangan protokol dengan menggunakan kriptografi *hybrid* dimaksudkan untuk memecahkan permasalahan key *establishment* (mekanisme penggunaan kunci yang disepakati) selain masalah kerahasiaan pesan. Secara umum mekanisme kriptografi *Hybrid* yang mengkombinasikan sistem algoritma kriptografi

simetrik, asimetrik, fungsi hash dan sistem pembangkit kunci acak dapat dilihat pada Gambar 3. di bawah ini.



Gambar 3. Mekanisme Kriptografi *Hybrid* [13]

c. Sistem Operasi Android

Android adalah sistem operasi yang berbasis Linux untuk *smartphone* dan komputer tablet. Android menyediakan platform terbuka bagi para pengembang untuk menciptakan aplikasi mereka sendiri untuk digunakan oleh berbagai macam perangkat mobile[14]. Aplikasi pada Android dapat dikembangkan secara luas dengan bahasa pemrograman berbasis Java. Para pengembang memiliki akses yang penuh ke dalam framework API yang sama digunakan dengan aplikasi native Android.

d. *Konsep Object-Oriented Analysis and Design*

Object-Oriented Analysis and Design (OOAD) adalah metode untuk menganalisa dan merancang sistem dengan pendekatan berorientasi object [15]. OOAD menjelaskan hubungan sebuah masalah utama dan solusi logis dari pandangan sebuah object menurut [16].

Object diartikan sebagai suatu entitas yang memiliki identitas, state, dan behavior [15]. Pada analisa, identitas sebuah object menjelaskan bagaimana seorang user membedakannya dari object lain, dan behavior object digambarkan melalui event yang dilakukannya. Sedangkan pada perancangan, identitas sebuah object digambarkan dengan cara bagaimana object lain mengenalinya sehingga dapat diakses, dan behavior object digambarkan dengan operation yang dapat dilakukan object tersebut yang dapat mempengaruhi object lain dalam sistem.

Unified Modeling Language (UML) merupakan notasi dalam bentuk diagram untuk merancang sistem menggunakan konsep object-oriented menurut [16].

2.2 Tinjauan Studi

Tinjauan studi yang dijadikan acuan dalam melakukan penelitian tesis ini mengacu pada beberapa penelitian terkait yang telah dilakukan sebelumnya yaitu sebagai berikut.

1. Penelitian mengenai pengembangan sistem pengamanan *Short Message Service* (SMS) telah dilakukan oleh Tarek M. Mahmoud, et.al [3]. Sistem yang dikembangkan bertujuan untuk mengatasi permasalahan keamanan pada komunikasi menggunakan SMS. Metode yang digunakan pada sistem tersebut yaitu menggunakan sistem *Hybrid Compression Encryption* (HCE). Metode tersebut dilakukan untuk mengkompresi atau mengurangi panjang SMS untuk kemudian dienkripsi sebelum dikirim ke penerima. Algoritma kompresi yang digunakan yaitu lossless dan algoritma kriptografi asimetrik RSA untuk enkripsi pesan SMS-nya. Hasil penelitian tersebut menyebutkan bahwa proses enkripsi dan dekripsi berhasil dilakukan serta proses kompresi yaitu mencapai 47% pengurangan panjang SMS. Namun berkaitan dengan pemenuhan aspek keamanan informasi, dalam penelitian tersebut hanya memenuhi aspek *confidentiality* dan *authentication.*
2. Penelitian mengenai pengembangan sistem pengamanan Short Message Service (SMS) telah dilakukan oleh Ashish Ranjan, et.al [4]. Sistem yang dikembangkan berupa pengamanan SMS untuk kebutuhan M-Commerce menggunakan program J2ME. Sistem pengamanan SMS tersebut melibatkan server yaitu bank sebagai pihak yang memvalidasi pembayaran oleh pembeli menggunakan ponselnya pada mekanisme M-Commerce. Proses validasi yang dilakukan server bank adalah proses enkripsi, dekripsi dan verifikasi pesan SMS yang dikirim oleh pembeli. Algoritma kriptografi yang digunakan dalam sistem tersebut yaitu algoritma kriptografi simetrik TEA dan fungsi hash MD5. Hasil penelitian tersebut menyebutkan bahwa proses enkripsi, dekripsi dan verifikasi e-mail berhasil diterapkan. Namun berkaitan dengan pemenuhan aspek keamanan informasi, dalam penelitian tersebut hanya memenuhi aspek *confidentiality* dan *data integrity.*
3. Penelitian mengenai pengembangan sistem pengamanan Short Message Service (SMS) telah dilakukan oleh Setiawan, Foni A., et.al [5]. Sistem Algoritma kriptografi yang digunakan dalam sistem tersebut yaitu algoritma kriptografi simetrik RC4 dan fungsi hash MD5. Pada sistem tersebut diasumsikan masing-masing pihak telah memiliki kunci enkripsi yang sama sehingga tidak terdapat key establishment pada kedua pihak yangberkomunikasi. Fungsi hash digunakan untuk memastikan bahwa kunci enkripsi yang dimiliki oleh pihak penerima SMS adalah sama dengan kunci enkripsi yang digunakan oleh pengirim SMS untuk mengenkripsi SMS sebelum dikirimkan. Hasil penelitian tersebut menyebutkan bahwa proses enkripsi dan dekripsi berhasil diterapkan. Namun berkaitan dengan pemenuhan aspek keamanan informasi, dalam penelitian tersebut hanya memenuhi aspek *confidentiality*.
4. Penelitian lainnya berupa rancang bangun aplikasi enkripsi dan dekripsi berbasis android menggunakan algoritma *Hybrid* DES dan Elgamal oleh Aris Kusuma, Martinus, Abdul Rahman [6], dalam penelitian ini dilakukan enkripsi terhadap SMS dengan menggunakan algoritma simetrik DES dan Elgamal dimana algoritma keduanya cukup klasik dan masih belum memenuhi semua unsur terkait dengan keamanan data dmana key yang dibagi antara penerima dan pengirim memungkina untuk diketahui orang lain baik dalam proses pengiriman

key maupun dalam penyimpanan key tersebut sehingga diperlukan tambahan menggunakan enkripsi asimetrik sehingga lebih aman.

5. Penelitian mengenai pengembangan peningkatan keamanan SMS secara end-to-end menggunakan teknik *Hybrid* juga dilakukan oleh Samer Hasan Saif Qaid [7], yang mana dalam penelitiaanya Samer menggunakan asimetrik berupa algoritma NTRU dan simetrik berupa algoritma AES-Rijndael yang dikembangkan pada platform mobile berbasis J2ME, namun dalam pengembangannya terdapat hal yang perlu diperhatikan dimana hasil chiper teks dari algoritma NTRU yang digunakan ukurannya cukup besar sehingga mempengaruhi performa dan besaran teks yang dapat diisi.

Penelitian-penelitian terkait diatas memiliki tujuan yang sama dengan penelitian tesis ini yaitu melakukan pengaman pesan SMS. Namun perbedaaan yang mendasar adalah bahwa penelitian tesis ini lebih terfokus pada pengamanan komunikasi SMS pada perangkat berbasis Android yang dapat memenuhi seluruh kriteria aspek keamanan informasi mulai dari *confidentiality*, *data integrity*, *authentication* dan *non-repudiation*. Untuk memenuhi hal tersebut, maka dalam hal ini penulis mengusulkan menggunakan metode kriptografi *hybrid* yang merupakan kombinasi dari penggunaan algoritma simetrik AES-256, algoritma asimetrik *Elliptic Curve* (EC-Cryptography) fungsi *messagedigest* SHA-256, fungsi digital *signing* dan sistem pembangkit kunci acak.

2.3 Tinjauan Obyek Penelitian

Pada penelitian ini obyek peneltian yang menjadi fokus dalam pengembangan aplikasi meliputi :

Perangkat Keras:

Komputer

1) Prosesor: Intel Core i5 @ 1,8 Ghz
2) Memori: 4 GB
3) *Hard disk*: 256 GB

Sistem operasi: Mac OSX 10.9.1

Perangkat Mobile berbasis Android

1) Prosesor: Dual-core 1.2 GHz Cortex-A5
2) Memori: 1 GB RAM
3) *Hard disk*: 8 GB
4) Sistem operasi: Android OS 4.1.2 *Jelly Bean*

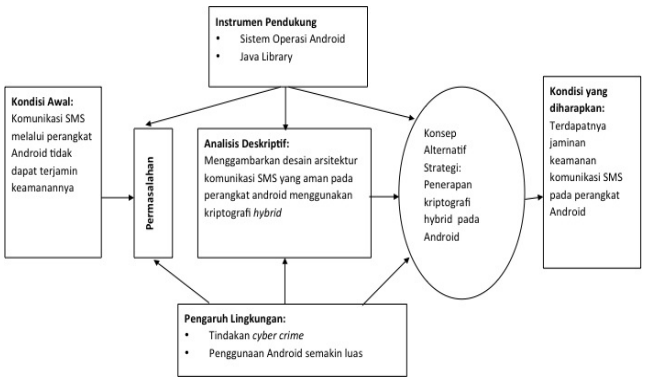
Perangkat mobile Android ini dilengkapi dengan *simcardprovider* GSM lokal di Indonesia dengan akses untuk mengirim dan menerima SMS.

Perangkat Lunak:

Java Development Kit
Android SDK
Eclipse .

2.4 Pola Pikir

Pola pikir yang digunakan dalam menyelesaikan rumusan masalah penelitian dapat dilihat pada gambar berikut:



Gambar 4. Pola Pikir

2.5 Hipotesis

Hipotesis dari penelitian tesis ini yaitu dengan menggunakan metode kriptografi *hybrid* maka sistem pengamanan komunikasi SMS pada perangkat mobile berbasis Android dapat memenuhi seluruh aspek keamanan informasi yang meliputi aspek *confidentiality*, *dataintegrity*, *authentication* dan *non-repudiation*.

3. DESAIN PENELITIAN

3.1. Meode Peneltitian

Tujuan dari penelitian ini yaitu untuk membangun sebuah sistem pengamanan komunikasi SMS pada perangkat *mobile* berbasis Android menggunakan kriptografi *hybrid* yang diharapkan dapat memenuhi seluruh aspek keamanan informasi. Berdasarkan tujuan tersebut, metode penelitian digunakan dalam penelitian ini adalah metode penelitian eksperimen. Penelitian eksperimen adalah penelitian dimana peneliti dapat melakukan manipulasi kondisi yang ada sesuai dengan keinginan peneliti.

3.2. Metode Pengumpulan Data

Metode pengumpulan data yang digunakan dalam penelitian ini adalah pengamatan atau observasi. Observasi adalah kegiatan pengamatan yang direncanakan, sistematis dan hasilnya dicatat serta diinterpretasikan dalam rangka memperoleh pemahaman tentang objek yang diamati.Pada penelitian ini observasi dilaksanakan dengan cara mencatat dan mengamati langsung secara *real time* proses enkripsi dan dekripsi sms untuk mendapatkan paket data sms untuk dilakukan analisis lebih lanjut.

3.3. Teknik Analisis Data

Teknik analisis data dalam penelitian tesis ini menggunakan pendekatan kualitatif dimana data yang telah dikumpulkan sebelumnya dianalisis tidak dengan menggunakan analisis data statistik. Analisis data secara kualitatif dilakukan dengan menganalisis hasil benchmark

yang disusun untuk mengetahui performa komputasi pada proses enkripsi dan ukuran pesan masing-masing perangkat *smartphone*. disamping pencatatan tingkat kerumitan dalam proses enkripsi dan dekripsi serta proses pertukaran dan *establishment key* dengan membandingkan langkah-langkah dari setiap instrumen yang ada, disamping dilakukan pula analisis fungsional dan detail prosedur internaldari aplikasi.

3.4. Langkah-langkah Penelitian

Tahapan-tahapan yang dilakukan dalam rangka melakukan penelitian pengembangan aplikasi ini adalah sebagai berikut:

Gambar 5. Langkah-langkah penelitian

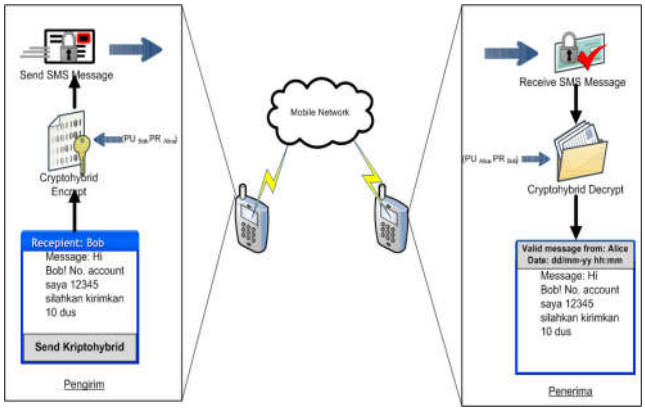
4. ANALISIS, INTERPRESTASI DAN IMPLIKASI PENELITIAN

4.1 Analisis Sistem

Pada tahap analisis sistem aplikasi pengamanan komunikasi SMS dengan teknik kriptografi *Hybrid* pada perangkat *mobile* berbasis Android ini menggunakan pendekatan desain dan analisis berorientasi objek atau *Object Oriented Analysis and Design*(OOAD) dengan menggunakan notasi *Unified Modeling Language* (UML). Pada tahap ini dilakukan analisis pengumpulan kebutuhan elemen-elemen ditingkat aplikasi. Dengan analisis ini, akan ditentukan domain-domain data atau informasi,fungsi, proses atau prosedur yang diperlukan beserta unjuk kerjanya dan antarmuka. Hasil akhir dari tahapan ini adalah spesifikasi kebutuhan aplikasi pengamanan komunikasi SMS pada perangkat *mobile* berbasis Android.

4.2 Perancangan Sistem

Perancangan sistem ini bertujuan untuk memberikan gambaran dan rancang bangun mengenai sistem yang akan dikembangkan. Perancangan sistem yang dilakukan dibagi menjadi dua bagian yaitu perancangan teknik kriptografi *hybrid* dan layar aplikasi.Pada penelitian ini teknik kriptografi *hybrid* merupakan inti dari alternatif solusi guna menyelesaikan permasalahan penelitian yang dituangkan dalam rumusan masalah. Perancangan teknik kriptografi *hybrid* nantinya akan diimplementasikan pada perangkat bergerak berbasis Android menggunakan bahasa pemrograman Java. Gambar 6 di bawah ini memberikan gambaran yang jelas mengenai teknik kriptografi *hybrid* yang akan diimplementasikan.



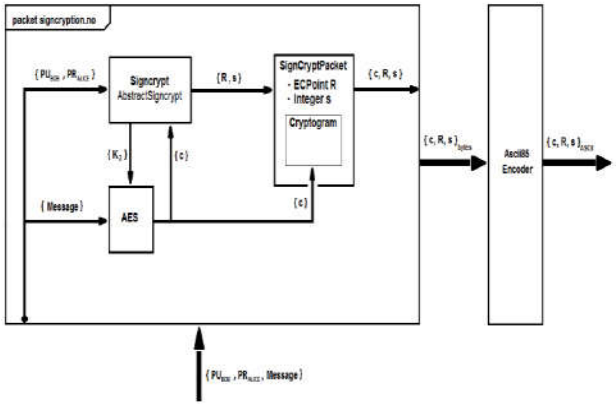
Gambar 6. Proses sistem pengamanan SMS dengan teknik kriptografi *hybrid* yang dikembangkan.

.

Secara singkat perancangan pengamanan SMS dengan teknik kriptografi *hybrid* ini digambarkan pada gambar di atas dan dapat dijelaskan sebagai berikut. Pengirim dan Penerima adalah pengguna yang akan saling berkomunikasi pesan rahasia dimana pengirim akan mengirimkan pesan rahasia melalui komunikasi SMS kepada penerima. Untuk dapat saling berkomunikasi maka masing-masing pengguna harus memasang aplikasi ini pada perangkat bergerak miliknya. Pertama, pengirim membutuhkan pasangan kunci atau *key pair* yakni *public key* dan *private key* yang dapat di *generate* oleh sistem aplikasi secara *background*. Pengirim hanya perlu menjalankan aplikasi atau halaman utama aplikasi kemudian dapat mengelola *key pair* yang ada termasuk bertukar atau mengirimkan *public key* kepada penerima yang diinginkan dari kontak yang ada. Kemudian setelah dilakukan pertukaran *public key* khususnya dari pengirim kepada penerima maka seperti halnya mengirimkan SMS secara biasa maka dapat dilakukan pengriiman pesan SMS ter-enkripsi kepada penerima yang memang telah dilakukan verifikasi untuk dijadikan sebagai kontak yang dipercaya untuk saling melakukan pertukaran atau pengriman SMS rahasia. Pesan rahasia akan dienkripsi menggunakan kriptografi *hybrid* yakni perpaduan antara algoritma kriptografi simetrik (AES-256 bit), algoritma kriptografi asimetrik Ellitptic Curve (EC-Cryptography), fungsi message digest SHA-256, fungsi digital signing dan sistem pembangkit kunci acak.

4.2.1 Enkripsi Pesan SMS

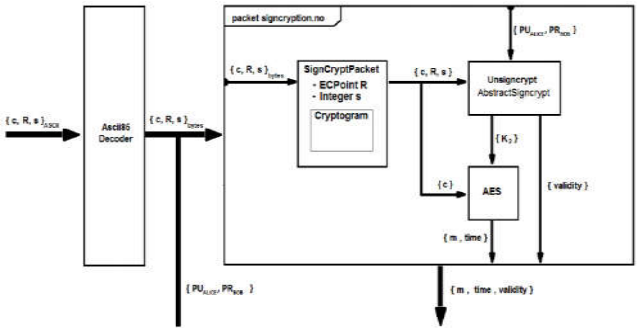
Pada gambar berikut ini akan diperlihatkan rancangan proses enkripsi pesan dengan teknik kriptografi *hybrid*. Untuk melakukan enkripsi pesan, input pada paket *signcryption* adalah *publickey* dari penerima, *privatekey* pengirim dan pesan yang dibuat. *Key* pertama kali digunakan pada signcrypt class untuk men-generate *key* enkripsi simetrik K2. AES *class* akan meng-enkrip pesan dengan K2 dan mengirimkan kembali kepada *signcrypt* class untuk men-generate EC point R dan integer s. Sebagaimana halnya data yng dikirimkan dalam banyak kasus di tangani dengan *bytes* tersendiri, signcryptPacket menyatukan c,R,s kedalam paket bytes. Kemudian paket data akan di encode menjadi karakater ASCII dengan Ascii85 encoder. Setelah itu maka pesan SMS telah ter-enkripsi dan di-sign yang kemudian dapat dikirimkan sebagaimana biasa melalui layanan SMS yang ada pada smartphone.



Gambar 7. Struktur dari *singcryption* teknik kriptografi *hybrid* untuk *signing* dan enkripsi pesan

4.2.2 Dekripsi Pesan SMS

Setelah proses enkripsi maka akan ditampilkan pula proses dekripsi pesan SMS yang dapat dilihat pada gambar berikut. Pertama paket ASCII encoded dari C, R, s akan di decode kembali ke bytes dengan menggunakan Ascii85 encoder. Kemudian signcryptpacket class akan mengeluarkan komponen c, R, s. Dengan kunci publik pengirim, kunci privat penerima, AES chiper text c, EC point R dan integer s, Unsigncrypt class akan mengkalkulasi kunci simetrik AES K2 apakah pesan tersebut memiliki signature yang valid. Sebagai catatan bahwa validasi dapat di verifikasi tanpa men-dekrip ciphertext c. AES class men-dekrip chipertext c dengan menggunakan key K2, dan selanjutnya kita mendapatkan dua komponen yakni cleartext m dan time stamp dari pengirim.



Gambar 8. Struktur dari Unsigncryption/dekripsi SMS

4.3 Implementasi Sistem

Setelah dilakukan proses analisis dan perancangan sistem selanjutnya akan dilakukan implementasi sistem tersebut. Beberapa bagian penting yang dibutuhkan dalam implementasi sistem yaitu meliputi spesifikasi perangkat keras, perangkat lunak, dan implementasi program pada perangkat bergerak berbasis Android.

Tabel 1. Spesifikasi Perangkat Keras

Perangkat Keras	Spesifikasi
Komputer	• *Processor*: Intel Core i5 1.8 GHz • *Memory*: 4 GB • *Harddisk*: 256 GB • Sistem Operasi: Mac OSX 10.9.1
Perangkat bergerak	• *Processor*: Dual-core 1.2 GHz Cortex-A5 • *Memory*: 1 GB RAM • *Harddisk*: 8 GB • Sistem Operasi: Android 4.1.2 Jelly Bean

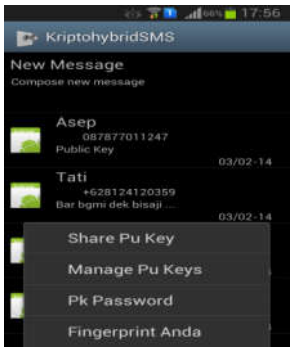
Tabel 2. Spesifikasi Perangkat Lunak

Perangkat Lunak	Spesifikasi
Java Development Kit	JDK 1.7.2.1
Android SDK	Revision 20
ADT Plugin	ADT 20.0.0
Eclipse	Kepler Service Release 1

4.3.1 Implementasi Program

a. Halaman Utama

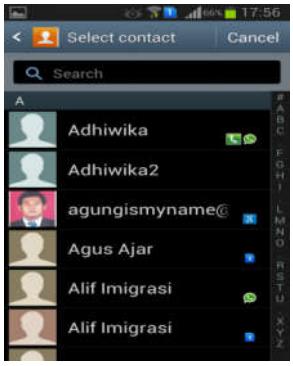
Ketika aplikasi kriptohybrid SMS ini dijalankan, maka yang akan muncul pertama kali adalah halaman utama. Pada halaman utama ini akan berisi daftar SMS sebagaimana *Inbox* pada umumnya dan dilengkapi dengan menu untuk membuat SMS baru, *share PU Key*, *manage PU keys*, *PK password* dan *Fingerprint* anda. Tampilan dari halaman utama ditunjukkan pada gambar di bawah ini.



Gambar 9. Tampilan layar utama aplikasi pengamanan SMS dengan teknik kriptografi hybrid

b. Share PU Keys

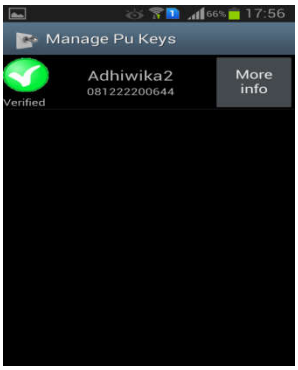
Berikut ini adalah method Share PU key yang digunakan dalam implementasi program untuk use case share PU key. Pada proses ini setelah dilakukan proses generate Public key secara background dan kemudian akan didistribusikan kepada penerima yang dinginkan melalui contact yang ada. Proses pengiriman public key ini sendiri akan menggunakan media SMS untuk mengirimkan kepada kontak yang telah dipilih sebelumnya dan akan mengkonfirmasikan jika SMS yang berisi public key tersebut telah terkirim. Kemudian nantinya public key tersebut akan diterima oleh penerima dan dapat dilakukan verifikasi dan konfirmasi untuk menerima public key tersebut sehingga dimungkina untuk melakukan pertukaran SMS rahasia yang terenkripsi dari pengirim kepada penerima yang dimaksud.



Gambar 10. Tampilan menu share PU key

c. Manage PU keys

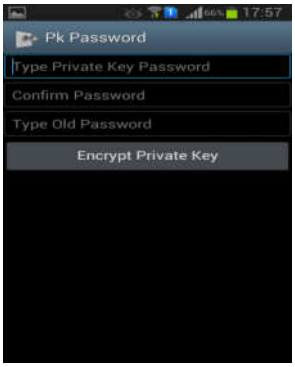
Setelah dilakukan share PU key maka selanjutnya untuk melihat dan mengelola public key yang ada atau untuk memverifikasi public key dari orang lain/pengirim maka dapat dilihat pada method berikut yang merupakan implementasi program untuk use case manage PU keys, dimana pada proses ini akan meminta kita untuk memilih contact yang akan dilakukan share public key , seperti tampilan gambar 11 di bawah.



Gambar 11 Tampilan proses *Manage PU Keys*

d. PK Password

Berikut ini adalah method PK Password yang digunakan sebagai dalam implementasi program untuk use case Genertae key pair. Pada proses ini akan dilakukan pengisian password untuk memproteksi public key yang ada sehingga terjamin kerahasiaannya baik saat disimpan maupun dalam hal pengiriman public key tersebut kepada penerima.



Gambar 12. Tampilan public key password

4.4 Pengujian Sistem

Adapun prototipe sistem yang dikembangkan akan dilakukan pengujian oleh tiga orang, meliputi :

- Developer, yakni peneliti itu sendiri.
- Penguji independen, yakni orang lain yang dipandang memiliki kemampuan dan kapabilitas untuk menguji

sistem.

- Dan calon pengguna sistem yang akan menguji sebagai user acceptance test.

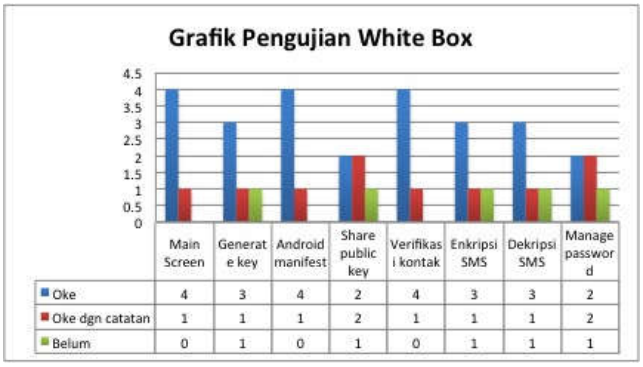
Beberapa pendekatan yang digunakan dalam pengujian yang akan dilakukan yakni :

4.4.1. Pendekatan Whitebox

Pada pendekatan ini yang akan dilakukan adalah :

- Pengamatan detail prosedur.
- Mengamati sampai level percabangan kondisi dan perulangan.

Dari pendekatan dimaksud, berikut ini adalah grafik pengujian kode program berdasarkan modul-modul yang dikelompokkan menjadi lima kali pengujian:

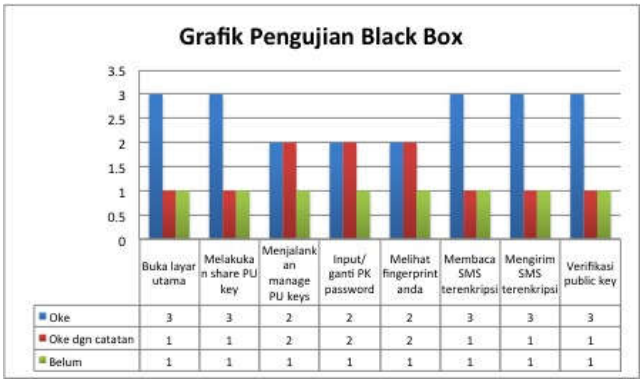


Gambar 13. Grafik Pengujian White Box

4.4.2 Pendekatan Blackbox

Pada pengujian black box terfokus pada apakah implementasi program memenuhi kebutuhan dari analisis sistem yang telah ditentukan. Pengujian dilakukan dengan menjalankan atau mengeksekusi unit atau modul, kemudian diamati apakah hasil dari unit tersebut sesuai dengan proses yang dikehendaki atau tidak. Pada pendekatan ini, yang dilakukan adalah :

- Memastikan fungsional dari perangkat lunak berjalan.
- Kesesuaian input dengan output
- Tidak memperhatikan proses logic internal



Gambar 14 . Grafik Pengujian Black Box

Berdasarkan hasil pengujian black box dapat disimpulkan bahwa sistem yang dikembangkan secara fungsional sudah sesuai dengan yang diharapkan saat desain aplikasi disamping dapat mengetahui fungsi-fungsi yang salah atau hilang, kesalahan dalam data, kesalahan kinerja, inisialisasi dan secara fungsional mengeluarkan hasil yang sesuai dengan yang diharapkan.

4.4.3 Pendekatan Keamanan

a. Pengujian Confidentiality

Pengujian confidentilaity dilakukan untuk membuktikan bahwa sistem yang dikembangkan ini mampu untuk menjamin kerahasiaan pesan SMS yang dikirimkan oleh pengirim kepada penerima. Pada pengujian ini penulis secara sederhana akan menunjukkan bahwa pengiriman SMS secara biasa sangat mudah dibaca oleh orang lain baik dengan menyadap dengan proses sniffing ataupun dengan bantuan aplikasi spy yang mampu melakukan monitoring terhadap SMS yang dikirim maupun diterima. Pada gambar dibawah merupakan tampilan SMS yang dikirim pada perangkat Android tanpa dilakukan enkripsi dan tanpa menggunakan aplikasi kriptohybridSMS.

Pada pengujian confidentiality akan dilakukan skenario yang sama dengan proses pengiriman dan pembacaan SMS yang biasa, hanya saja pada skenario ini dilakukan dengan menggunakan aplikasi pengamanan SMS dengan teknik kriptografi *hybrid* untuk perangkat Android pengirim dan penerima.

Hasil pengujian menunjukkan bahwa SMS yang dikirimkan apabila dilakukan pembacaan biasa maka akan tidak dapat terbaca atau tidak memiliki arti apapun karena hanya berisi kode-kode yang merupakan hasil dari proses kriptografi hybrid yang digunakan. Oleh karena itu aplikasi pengamanan komunikasi SMS yang dikembangkan dapat memenuhi aspek confidentiality karena mampu menjamin kerahasiaan pesan SMS yang dikirimkan oleh pengirim kepada penerima.

b. Data Integrity

Pengujian *data integrity* bertujuan untuk melakukan verifikasi atau mendeteksi jika terjadi perubahan atau modifikasi paket data SMS pada saat transmisi. Pada pengujian ini penguji memodifikasi *source code* untuk mengirim SMS terenkripsi dimana penulis menambahkan karakter "1" pada SMS terenkripsi sebelum SMS dikirim. Hasil pengujian menunjukkan bahwa SMS yang mengalami modifikasi maka akan dinilai oleh sistem SMS tersebut tidak terverifikasi dan dianggap sebagai SMS biasa.

Oleh karena itu berdasarkan pengujian yang dilakukan ,maka aplikasi pengamanan komunikasi SMS yang dikembangkan memenuhi aspek *data integrity* karena mampu melakukan verifikasi atau mendeteksi adanya perubahan atau modifikasi paket data SMS pada saat transmisi.

c. Pengujian Autehntication

Pengujian authentication bertujuan untuk memberikan jaminan bahwa SMS yang dikirim oleh pengirim yang sesuai dengan pemilik nomer kontak pengirim. Aspek ini penting untuk mengindari tindakan SMS spoofing dimana pengirim SMS merupakan orang yang tidak bertanggung jawab yang menggunakan nomer palsu untuk mengirim SMS ke orang lain untuk tujuan yang tidak baik.

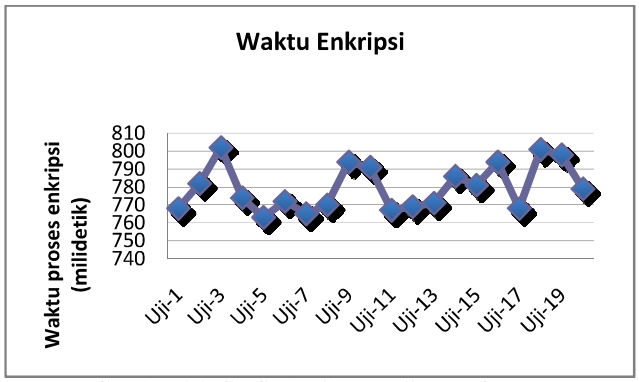
Hasil pengujian menunjukkan bahwa SMS yang dikirim menggunakan nomer palsu tidak dapat diverifikasi oleh aplikasi pengamanan komunikasi SMS ini dan dianggap bahwa pengirim yang mengirimkan SMS tidak ada dalam kontak dan belum diverifikasi untuk saling berkirim SMS rahasia. Hal tersebut terjadi karena kontak yang digunakan tidak terdaftar di public key sistem aplikasi dan tidak memiliki public key. Oleh karena itu berdasarkan pengujian yang dilakukan, maka aplikasi pengamanan komunikasi SMS yang dikembangkan memenuhi aspek authentication karena mampu menjamin SMS yang dikirim oleh pengirim yang sesuai dengan yang ada di kontak serta telah diverifikasi dengan public key.

d. Pengujian Non-Repudiation

Pengujian *non-repudiation* dilakukan untuk mencegah adanya penyangkalan yang dilakukan oleh pemilik kontak SMS bahwa ia yang telah mengirim SMS. Hasil pengujian menunjukkan bahwa *user* penerima akan daapt memverifikasi SMS yang diterimanya. Proses verifikasi tersebut membutuhkan pasangan *public keyuser* pengirim untuk mendekripsi *messagedigest* yang dienkripsi menggunakan *EC-Cryptography* dengan *private key* penerima. Jika proses verifikasi berhasil, maka berarti pasangan *public key* dan *private key* adalah pasangan kunci yang benar dan dianggap valid tidak terdapat penyangkalan bahwa ia telah mengirim SMS terenkripsi. Oleh karena itu berdasarkan pengujian yang dilakukan, maka aplikasi pengamanan komunikasi SMS yang dikembangkan memenuhi aspek *non-repudiation* karena mampu mencegah adanya penyangkalan yang dilakukan oleh pemilik alamat SMS bahwa ia yang telah mengirim SMS.

4.4.4. Pendekatan Performa

Pendekatan performa yang digunakan dalam penelitian ini adalah dengan mengukur kemampuan dan kecepatan waktu proses enkripsi pada saat akan mengirimkan SMS terenkripsi. Pengujian dilakukan dengan menyisipkan fungsi System.currentTimeMillis() pada source code proses enkripsi. Fungsi ini akan menghasilkan angka berisi waktu dalam satuan milidetik (10-3 detik). Pada pengujian performa jumlah sampel data yang diambil berdasarkan random sampling yaitu sebanyak 20 sampel SMS yang dikirim dengan kapasitas jumlah karakter yang sama yaitu 100 karakter untuk mengetahui waktu rata-rata proses enkripsi SMS. Berikut ini adalah hasil pengujian performa tersebut.



Gambar 15. Grafik hasil pengujian performa.

Dari hasil pengujian dapat terlihat bahwa waktu proses enkripsi dengan teknik kriptografi *hybrid* pada sistem yang dikembangkan memiliki wakturata-rataselama 780milidetik untuk kapasitas SMS sebesar100 karakter. Walaupun dengan adanya proses enkripsi menyebabkan sedikit *delay* terhadap performa sistem, namun hal ini tidak akan terlalu mengganggu karena nilai tersebut tidak terlalu signifikan dalam komunikasi melaluiSMS.

4.5 Implikasi Penelitian

Dari penelitian tesis yang telah dijelaskan di atas memberikan beberapa implikasi penelitian terkait dengan beberapa aspek yaitu sebagai berikut.

a. Aspek Sistem

Dengan spesifikasi prosesor Cortex-A5 1.2 GHz, memori 1 GB RAM, hard disk internal 8 GB dan sistem operasi Android OS v4.1.2 Jelly Bean, proses kriptografi hybrid yang dilakukan relatif cepat dimana berdasarkan hasil pengujian untuk kapasitas SMS sebesar 100 karakter hanya membutuhkan waktu rata-rata proses kriptografi hybrid selama 780 milidetik sebelum SMS dikirimkan.

b. Aspek Manajerial

Salah satu penerapan yang dapat diusulkan sebagai metode pengamanan komunikasi SMS adalah menggunakan aplikasi pengamanan komunikasi SMS dengan teknik kriptografi hybrid berbasis Android.

c. Aspek Penelitian Lanjutan

- Pengamanan SMS dengan teknik kriptografi hybrid pada media MMS
- Implementasi sistem dengan standar sertifikat digital X.509 pada public key infrastructure yang memiliki interoperabilitas dengan sistem lainnya
- Implementasi sistem pada sistem operasi mobile lainnya seperti IOS, Windows mobile phone.

4.6 Rencana Implementasi

- Rencana implementasi diawali dengan melakukan perbaikan dan efisiensi implementasi pemrograman berdasarkan masukan dan penilaian pada saat sidang tesis yaitu pada bulan Februari, dimana dengan masukan yang ada maka akan dilakukan perbaikan dan optimalisasi implementasi terhadap aplikasi.

- Selanjutnya aplikasi akan diunggah ke public repository yaitu Google Play agar dapat digunakan pengguna umum secara luas, dan akan dilakukan monitoring terhadap penggunaan aplikasi yang telah diunggah untuk sedapat mungkin menampung masukan dari pengguna yang telah menggunakan aplikasi ini.
- Diharapkan pengguna umum yang mengunduh dan menggunakan aplikasi tersebut akan melaporkan apabila ditemukan kesalahan pada aplikasi seperti bug atau error, begitu juga jika ada masukkan dari pengguna umum agar aplikasi lebih mudah dan nyaman digunakan.
- Laporan-laporan yang diterima akan ditindaklanjuti dengan memperbaiki aplikasi sekaligus mengubah menjadi lebih mudah dan nyaman digunakan sesuai dengan keinginan pengguna.
- Langkah selanjutnya adalah setelah aplikasi diperbaiki, aplikasi diunggah kembali ke dalam Google Play sebagai versi selanjutnya. Aplikasi dapat digunakan kembali oleh pengguna umum.
- Selanjutnya adalah tetap memonitor operasionalisasi penggunaan aplikasi sehingga jika terdapat masalah dapat diatasi segera.

5. KESIMPULAN

Salah satu fitur yang tersedia dan cukup populer digunakan pada perangkat telepon seluler khsusnya yang berbasis Android adalah SMS. Dengan layanan SMS maka dimungkinkan untuk mengirimkan pesan singkat kepada pengguna ponsel yang lainnya dengan cepat dan dengan biaya yang murah. Disadari atau tidak pemanfaatan SMS untuk bertukar informasi dan berkolaborasi tidak hanya terbatas pada informasi yang bersifat biasa saja, tetapi juga informasi yang cukup sensitif dan rahasia yang apabila dipergunakan secara tidak bertanggung jawab oleh pihak lain yang tidak berhak maka akan dapat merugikan pihak lainnya. Secara umum terdapat keterbatasan pada layanan SMS yakni tidak terjaminnya kerahasiaan dan keutuhan pesan yang dikirimkan.

Dalam penelitian yang dilakukan maka dapat diambil kesimpulan bahwa dengan penggunaan metode kriptografi hybrid yang diterapkan sebagai sistem pengamanan komunikasi SMS pada perangkat Android dapat memenuhi keseluruhan aspek keamanan informasi yang meliputi kerahasiaan (confidentiality), keutuhan data (data integrity), keaslian (authentication) dan tidak terdapat penyangkalan (non-repudiation).

DAFTAR PUSTAKA

[1] Ingrid Lunden, Gartner: "Android Accounted For 72% Of Smartphone Sales In Q3, Overall Sales Of Mobile Handsets Down 3%, 2012", http://techcrunch.com/2012/11/14/gartner-samsung widens-its-lead-over-apple-in-smartphones-in-q33-but-overall-sales-of-mobile-handsets-down-3/, (Diakses 17 Oktober 2013).

[2]Menezes,AlfredJ.,et.al.,"*HandbookofAppliedCryptography* ", Florida: CRC PressInc.,1996.

[3] Mahmoud,TarekM., et.al.,"HybridCompressionEncryption Techniquefor Securing SMS",*InternationalJournalofComputerScience and Security(IJCSS)*, volume3, (2009): 437-481.

[4] Ashish Ranjan, Rajashekara Murthy S, Ramakanth Kumar P, "A Review of Secure SMS Based M-Commerce", International Journal of Engineering Sciences & Emerging Technologies, Feb-2012, Volume 1, Issue 2, pp: 1-7

[5] Setiawan, Foni A., et.al., "*Design and Implementation of Short Messaging Service Application Using RC4 Encryption Algorithm for Java- Based Devices*", International Seminar on Scientific Issues and Trends, 2011.

[6] Aris Kusuma Wijaya, Martinus, Abdul Rahman, *Jurnal Jurusan Teknik Informatika* STMIK MDP, 2013.

[7] *"An end-to-end short message service (SMS) security using a hybrid technique of NTRU and AES-Rijndael"*. Dissertation for the master degree of Computer Science & Information Technology, University of Malay, Kuala Lumpur, February 2011.

[8] 3GPP.ORG. 1997. archive [Online]. Available: http://www.3gpp.org/ftp/Specs/archive/03_series/03.40/ [Accessed 25-11-2009].

[9] SUNMICROSYSTEMS 2004. Wireless Messaging API 2.0 Specification.

[10] G. Le Bodic, "Mobile Messaging Technologies and Services SMS, EMS and MMS ", 2nd ed., John Wiley & Sons Ltd, (2005).

[11] Munir, Rinaldi 2006, "Kriptografi", Informatika, Bandung.

[12]Rasmi, PS. And Paul, Varghese., "A Hybrid Crypto System based on a new Circle Symmetric key Algorithm and RSA with CRTA symmetric key Algorithm for Ecommerce Applications ", *International Conference on VLS I, Communication & Instrumentation (ICVCI)* ,(2011):14-18

[13] Arthur Hefti website. "Encryption in PowerBuilder". 2012.http://arthurhefti.syscon.com/node/107040/mobile. (Diakses 26 November 2013).

[14] Android Developers website. "What is Android?". 2012. http://developer.android.com/guide/basics/what-is-android.html. (Diakses 25 November 2013).

[15] Mathiassen, Lars. "Object Oriented Analysis and Design". 1st Edition. Denmark : Marco Publishing Aps.

[16] Larman. "Applying UML And Patterns : An Introduction to Object Oriented Analysis and Design". Prentice Hall Inc.,USA.