KRIPTOGRAFI UNTUK PENGAMANAN DATA SMS

Solichul Huda
Program Studi Teknik Informatika, Fakultas Ilmu Komputer,
Universitas Dian Nuswantoro Semarang
Jl. Nakula I No. 5-11 Semarang
Telp : (024) 3517261, Fax : (024)3520165
E-mail : huda@dosen.dinus.ac.id

Abstract

SMS data in the form of digital data that can be managed with the application program. Cryptography is the technique of writing that is used to encrypt the original data into the data does not actually. Encryption is aimed at hiding data from users who are not genuine entitlement. In this research studies the application of cryptography in securing the SMS data. Application of public key and private key used to complicate the reading of SMS data. Implementation will be used programming language that runs on mobile phones. The digital signature is applied in this study to allow a user to secure the SMS data. After the study is expected to show a new technique for securing SMS data that can be used in different kinds Mobile. It also wanted to prove that the concept of private key and public key can be implemented in security in mobile phone technology.

Keywords : *Data, SMS, Cryptography, Digital Signature, Private key, Public key.*

1. PENDAHULUAN

Perkembangan teknologi komunikasi saat ini memicu munculnya bermacam jenis teknologi baru, salah satunya adalah . SMS (*Short Message Service*). SMS merupakan salah satu produk dari teknologi komunikasi yang perangkat telepon selulernya banyak dipakai oleh masyarakat. SMS adalah sarana komunikasi dimana seseorang dapat mengirimkan sebuah pesan dari sebuah handphone (telepon selular) ke handphone lainnya.

Penggunaan SMS semakin hari semakin meningkat selain karena perangkat harga Handphone terjangkau juga karena siswa sekolah iku memakai teknologi SMS ini . Pada saat pertama kali SMS masuk Indonesia, SMS banyak digunakan oleh orang-orang untuk melakukan penghematan dalam melakukan komunikasi lewat handphone (mengingat biaya telepon via ponsel jauh lebih mahal dibandingkan SMS).

Namun kini penggunaan SMS mulai bergeser ke hal-hal yang bisa dikategorikan cukup penting. Seperti biasanya, penggunaan sebuah teknologi baru diikuti dengan munculnya sebuah masalah baru yang harus kita pecahkan. Masalah yang timbul dalam penggunaan teknologi SMS untuk pengiriman pesan-pesan yang penting adalah kerahasiaan. Jika kita mengirimkan sebuah SMS, maka SMS disandikan sebelum dikirim ke nomor tujuan.

Kriptografi merupakan seni menulis yang dapat dipergunakan untuk menyandikan pesan dari suatu data menjadi data yang tidak sebenarnya. Pesan SMS dienkripsi sebelum dikirim dan penerima SMS dapat mendapatkan pesan aslinya dengan mendekripsi data. Dalam penelitian ini akan dikembangkan dengan penerapan public key dan private key pada kriptografi ini. Dalam penelitian ini akan dicoba implementasikan kriptografi dalam bentuk program aplikasi untuk pengamanan pesan SMS .

2. PEMBAHASAN

2.1 Kriptografi

Pesan (*messages*) adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain untuk pesan adalah plaintext. Pesan dapat berupa data atau informasi yang dikirim melalui kurir atau media telekomunikasi lain atau yang di dalam media penyimpan (*storage*). Agar pesan tidak dapat dimengerti maknanya oleh pihak lain, maka pesan harus disandikan ke bentuk lain yang tidak dapat dipahami. Bentuk pesan yang tersandikan disebut *ciphertext. Ciphertext* harus dapat dikembalikan ke bentuk awal atau dikembalikan menjadi plaintext semula agar pesan dapat dibaca oleh orang yang seharusnya menerima pesan. Seperti juga

perkembangan ilmu kriptografi, tujuan-tujuan dari kriptografi teruslah berkembang. Bila pertama kali dibuat hanya untuk keamanan data saja, tetapi sekarang semakin banyak tujuan-tujuan yang ingin dicapai , yaitu:

1. Privasi, Musuh tidak dapat membongkar tulisan yang kita kirim.
2. Autentikasi, Penerima pesan dapat meyakinkan dirinya bahwa pesan yang diterima tidak terjadi perubahan dan berasal dari orang yang diinginkan.
3. Tanda tangan, penerima pesan dapat meyakinkan pihak ketiga bahwa pesan yang yang diterima berasal dari orang yang diinginkan.
4. Minimal, Tidak ada yang dapat berkomunikasi dengan pihak lain kecuali berkomunikasi dengan pihak yang diinginkan.
5. Pertukaran bersama, suatu nilai (misalnya tanda tangan sebuah kontrak) tidak akan dikeluarkan sebelum nilai lainnya (misalnya tanda tangan pihak lain) diterima.
6. Koordinasi, di dalam komunikasi dengan banyak pihak, setiap pihak dapat berkoordinasi untuk tujuan yang sama walaupun terdapat kehadiran musuh.

Konsep matematis yang mendasari algortima kriptografi adalah relasi antara dua buah himpunan, yaitu himpunan yang berisi elemen–elemen plaintext dan himpunan yang berisi ciphertext. Enkripsi dan dekripsi merupakan fungsi yang memetakan elemen – elemen antara kedua himpunan tersebut. Misalnya P menyatakan plaintext dan C menyatakan ciphertext,
maka fungsi enkripsi E memetakan P ke C :

$$E(P) = C$$

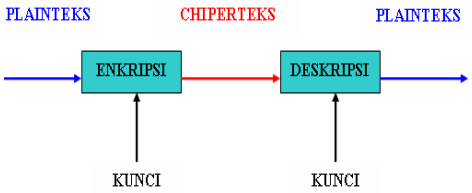
Dan fungsi dekripsi D memetakan C ke P :

$$D(C) = P$$

Karena proses enkripsi kemudian dekripsi mengembalikan pesan ke pesan awal, maka kesamaan berikut harus benar :

$$D(E(P)) = P$$

Keamanan algoritma kriptografi sering diukur dari banyaknya kerja (*work)* yang dibutuhkan untuk memecahkan ciphertext menjadi plaintext-nya tanpa mengetahui kunci yang digunakan. Kerja ini dapat diekivalenkan dengan waktu, memori, uang, dan lain-lain. Semakin banyak kerja yang dibutuhkan, juga semakin lama waktu yang dibutuhkan, maka semakin baik algoritma tersebut, berarti semakin aman digunakan untuk menyandikan pesan.



Gambar 1. Skema enkripsi

2.2 Tanda Tangan Digital

Tanda Tangan Digital berawal dari penggunaan teknik kriptografi yang digunakan untuk mengamankan informasi yang hendak ditransmisikan/disampaikan kepada orang yang lain yang sudah digunakan sejak ratusan tahun yang lalu. Dalam suatu kriptografi suatu pesan dienkripsi (*encrypt*) dengan menggunakan suatu kunci (*key*). Hasil dari enkripsi ini yaitu berupa chipertext tersebut lalu ditransmisikan/diserahkan ke tujuan yang dikehendaki. Chipertext tersebut di sisi penerima akan dibuka/didekripsi (*decrypt*) dengan suatu kunci untuk mendapatkan informasi yang telah enkripsi tersebut. Terdapat dua macam cara dalam melakukan enkripsi yaitu dengan menggunakan kriptografi simetris (*symetric crypthography/secret key crypthography*) dan kriptografi asimetris (*asymetric crypthography*) yang kemudian lebih dikenal sebagai public key crypthography. Secret key crypthografi atau yang dikenal sebagai kriptografi simetris, menggunakan kunci yang sama dalam melakukan enkripsi dan dekripsi terhadap suatu pesan (message), disini pengirim dan penerima menggunakan kunci yang sama sehingga mereka harus menjaga kerahasian (secret) terhadap kunci tersebut.

Salah satu algoritma yang terkenal dalam kriptografi simetris ini adalah *Data Encryption standard (DES). Public key crypthography,* atau dikenal juga sebagai kriptografi simetris, menggunakan dua kunci (*key*) : satu kunci digunakan untuk melakukan enkripsi terhadap suatu pesan (*messages*) dan kunci yang lain digunakan untuk melakukan dekripsi terhadap pesan tersebut. Kedua kunci tersebut mempunyai hubungan secara matematis sehingga suatu pesan yang dienkripsi dengan suatu kunci hanya dapat didekripsi dengan kunci pasangannya. Seorang pengguna mempunyai dua buah kunci, yaitu sebuah kunci privat (*privat key*) dan juga sebuah kunci publik (*public key*). Pengguna (*user*) tersebut kemudian mendistribusikan /menyebarluaskan kunci publik miliknya. Karena terdapat hubungan antara kedua kunci tersebut, pengguna dan seseorang yang menerima kunci publik akan

merasa yakin bahwa suatu data yang diterimanya dan telah berhasil didekripsi hanya dapat berasal dari pengguna yang mempunyai kunci privat. Kepastian /keyakinan ini hanya ada selama kunci privat ini tidak diketahui oleh orang lain. Kedua kunci ini berasal atau diciptakan sendiri oleh penggunanya. Salah satu algoritma yang terbaik yang dikenal selama ini adalah RSA (dinamakan sesuai dengan nama penciptanya Rivest, Shamir, Adleman).

Pada saat dua orang hendak saling berkomunikasi atau saling bertukar data/pesan secara aman, mereka kemudian saling mengirimkan salah satu kunci yang dipunyainya, yaitu kunci publiknya. Sedangkan mereka menyimpan kunci private sebagai pasangan dari kunci publik yang didistribusikannya. Karena data /pesan ini hanya dapat dienkripsi dan dekripsi dengan menggunakan kunci pasangannya maka data ini dapat dapat ditransmisikan dengan aman melalui jaringan yang relatif tidak aman (melalui internet). Contoh dari penggunaan kriptografi ini adalah jika Bob hendak mentransmisikan suatu data / pesan rahasia kepada Susan maka ia akan melakukan enkripsi data tersebut dengan menggunakan kunci publik Susan. Selama Susan yakin bahwa tidak ada seorang pun yang mengetahui kunci privatnya, maka mereka dapat merasa yakin bahwa yang dapat membaca pesan tersebut hanyalah Susan.

Dalam tanda tangan digital suatu data / pesan akan dienkripsi dengan menggunakan kunci simetris yang diciptakan secara acak (*randomly generated symmetric key*). Kunci ini kemudian akan dienkripsi dengan menggunakan kunci publik dari calon penerima pesan. Hasil dari enkripsi ini kemudian dikenal/disebut sebagai "digital envelope" yang kemudian akan dikirimkan bersama pesan/data yang telah dienkripsi. Setelah menerima digital envelope penerima kemudian akan membuka/mendekripsi dengan menggunakan kunci kunci privatnya. Hasil yang ia dapatkan dari dekripsi tersebut adalah sebuah kunci simetris yang dapat digunakannya untuk membuka data/pesan tersebut. Kombinasi antara tanda tangan digital dengan message digest menyebabkan seorang pengguna dapat "menandatangani secara digital" (*digitally sign*) suatu data/pesan.

Maksud dari menandatangani secara digital adalah memberikan suatu *katakunci* terhadap suatu pesan. Pada saat message dienkripsi dengan menggunakan kunci *private* dari pengirim dan "*ditambahkan*" kepada data/pesan yang asli maka hasil yang didapat adalah tanda tangan digital dari pesan tersebut. Penerima dari tanda tangan digital akan dapat mempercayai bahwa data/pesan benar berasal pengirim. Dan karena apabila terdapat perubahan suatu data/pesan akan menyebabkan akan merubah message dengan suatu cara yang tidak dapat diprediksi (*in unpredictible way*) maka penerima akan merasa yakin bahwa data/pesan tersebut tidak pernah diubah setelah message dikirim.

Sebelum kedua belah pihak (pengirim/penerima) hendak melakukan komunikasi diantaranya dengan menggunakan kriptografi kunci publik, masing-masing pihak harus merasa yakin akan keberadan mereka. Mereka kemudian akan melakukan otentifikasi terhadap keberadaan masing-masing pihak. maka mereka menunjuk pihak ketiga yang akan memberikan otentifikasi terhadap kunci publik mereka. Pihak ketiga ini kita kenal sebagai *Certification Authorithy*.

Certification authorithy ini kemudian akan memberikan suatu sertifikat (certificate) yang berisi identitas dari pengguna (misalnya Susan), sertifikat ini ditandatangani secara digital oleh Certification authority tersebut. Isi dari sertifikat tersebut selain identitas ia juga berisi kunci publik dari pemiliknya. Berikut ini merupakan gambaran dari digital signature. Bob telah diberi 2 kunci, salah satunya disebut public key dan yang satu disebut private key..

Kunci publik Bob tersedia untuk siapa saja yang membutuhkannya, tetapi kunci private nya disimpan untuk dirinya sendiri. Dimana kunci tersebut digunakan untuk mengenkripsi data. Susan dapat mengenkripsi pesan menggunakan kunci publik Bob dan Bob mengguna kan kunci privatenya untuk mendekripsi pesan tersebut. Siapapun dari Teman sekerja bob mungkin mempunyai akses terhadap pesan susan yang dienkripsi, tetapi tanpa Kunci private Bob, data tersebut tidak berharga.

2.3 Enkripsi SMS

Format data yang umum untuk SMS adalah plainteks. Enkripsi dilakukan pada saat transisi adalah hanya antara *Base Tranceiver Station* (BTS) dan *Mobile Station*. Namun, seperti yang kita tahu sebelumnya, algoritma yang digunakan untuk mengenkripsi data yang ditransmisikan antara BTS dan *Mobile Station* sehingga data terjaga keasliannya dari orang yang tidak berhak. Enkripsi SMS selain digunakan untuk komputer juga bisa terapkan di handphone salah satunya menggunakan Java ME (J2ME).

Pengguna perangkat lunak adalah pemilik sebuah tandatangan digital yang ingin menjaga isi data digital yang akan dikirimkan kepada seorang penerima dengan tujuan agar isi dari dokumen digital tersebut tidak diubah. Penerima data akan membuktikan keautentikan isi dan pemilik data digital tersebut. Berikut ini adalah matriks peran dan tanggung jawab dari pengguna perangkat lunak Tandatangan Digital (*Digital Signature*).

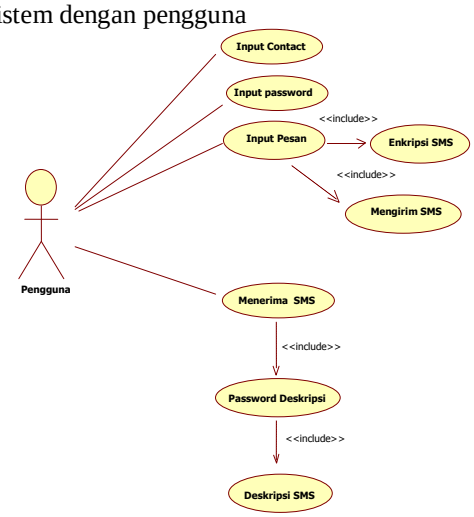
Tabel 1. Matriks Pengguna Aplikasi

Pengguna	**Peran**	**Tanggung Jawab**
Pemilik data	Pengguna	Menggunakan perangkat lunak *tanda tangan digital* untuk membangkitkan kunci *private* dan kunci publik sehingga dapat memberikan tanda tangan digital untuk data digital
Penerima data	Pengguna	Menggunakan perangkat lunak tanda tangan digital untuk membuktikan keautentikan isi dan pemilik data digital

Pada tahap aliran kerja analisa yang harus dilakukan adalah mengekstraksi kelas entity. Dalam melakukan hal ini dibagi menjadi 4 langkah, yaitu fungsional modeling, entity class modeling, dan interaction modeling.

2.4 Fungsional Modeling

Fungsional modeling yang penulis gambarkan dilakukan adalah mendeskripsikan use case. Use case digunakan untuk melihat interaksi antara sistem dengan pengguna

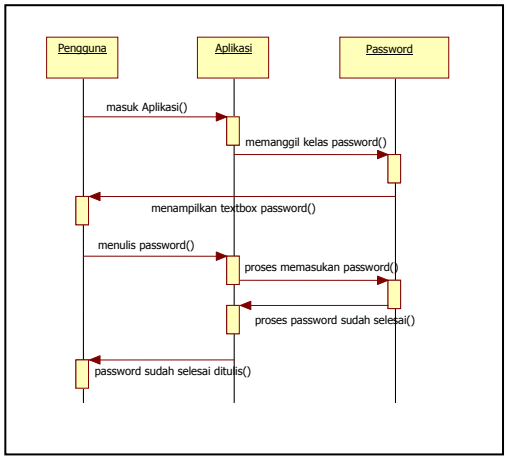


Gambar 2 . Interaksi Sistem Dengan User

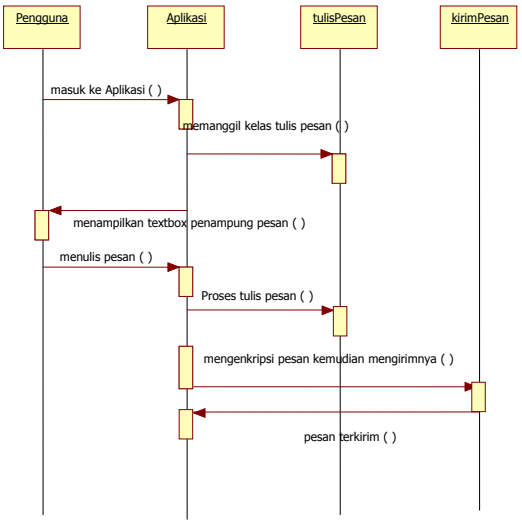
2.5 Interaction Modeling

Pada tahap ini menentukan interaksi antara beberapa objek menggunakan sequence diagram. Sequence diagram merepresentasikan interaksi antar objek di dalam dan di sekitar sistem, termasuk pengguna dan antarmuka pengguna. Sequence diagram terdiri atas dimensi vertikal yang merepresentasikan waktu, dan dimensi horizontal yang merepresentasikan objek-objek terkait. Aspek penting dari sequence diagram adalah keterurutan waktu, yang mengindikasikan bahwa interaksi direpresentasikan tahap demi tahap.

Pada use case tandatangan digital(*Digital Signature*) untuk inputan password akan penulis gambarkan pada Gambar berikut ini

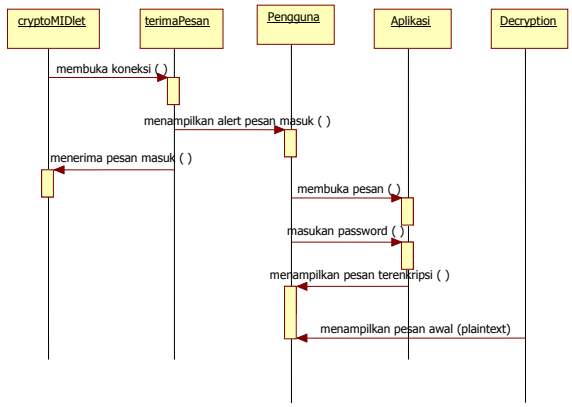


Gambar 3. Diagram pemakaian password



Gambar 4. Diagram Pengiriman SMS

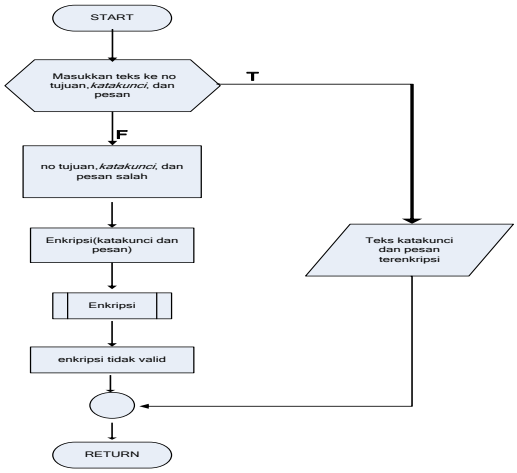
Gambar diatas adalah gambar diagram pengiriman SMS (Sequence Diagram Mengirim SMS)



Gambar 5. Sequence Diagram Menerima SMS

2.6 Proses Enkripsi

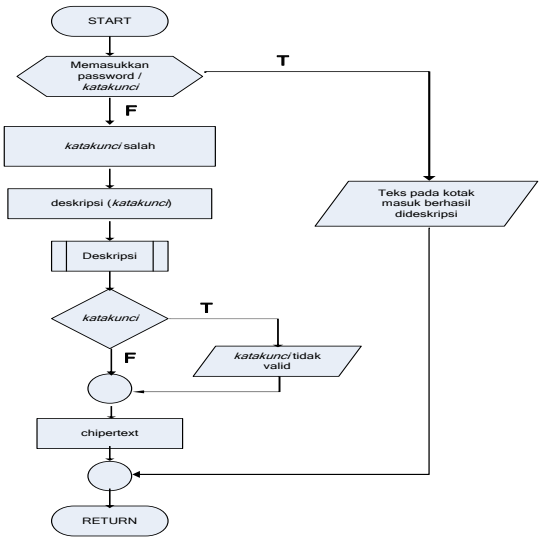
Untuk proses enkripsi, pertama kali program dijalankan dengan no tujuan,password, dan tulis pesan. Setelah menulis pesan maka pesan tersebut di enkripsi secara otomatis pada saat pesan dikirim, seperti terlihat pada gambar 6 dibawah ini.



Gambar 6. Gambar proses enkripsi

2.7 Proses Deskripsi

Proses dekripsi sama dengan proses enkripsi, hanya pada proses dekripsi input yang digunakan berupa ciphertext dan proses kerjanya kebalikan dari proses enkripsi. Pada proses dekripsi urutan kunci yang digunakan merupakan kebalikan dari urutan kunci yang digunakan pada proses enkripsinya. Setelah menerima pesan penerima harus memasukan password, apabila penerima tidak memasukan password maka pesan tersebut masih terenkripsi.fungsi password tersebut adalah untuk membuka pesan dan dideskripsi secara otomatis pada saat menampilkan pesan. Gambar 7. memperlihatkan proses dekripsi yang terjadi.



Gambar 7. Gambar proses Dekripsi

2.8 Proses Tanda Tangan Digital

Proses *tanda tangan digital* ini menggunakan algoritma RSA dan input yang digunakan berupa nilai yang diambil dari nilai validasi. Program akan melakukan proses *Generate* untuk menghasilkan kunci publik dan kunci privat. Kunci privat akan digunakan untuk menandatangani *plaintext* dan kemudian dihasilkan nilai *tanda tangan digital* tersebut. Dalam proses verifikasi, kunci publik yang telah dihasilkan akan digunakan beserta *tanda tangan digital* untuk memperoleh keaslian dari *plaintext*. Algoritma dari proses pembangkit kunci *tanda tangan digital* adalah sebagai berikut:

- Pilih dua buah bilangan prima yang berbeda (p dan q) (1)
- Hitung:
  $n = p * q$ (2)
- Hitung
  $\theta = (p - 1) * (q - 1)$ (3)
- Pilih sebuah integer e dengan batas $1 < e < \theta$ dan memenuhi syarat:
  $\gcd(e,\theta) = 1$ (4)
- Dengan menggunakan algoritma *extended Euclidean* dapat diperoleh nilai d, dengan batas $1 < d < \theta$ dan memenuhi syarat:
  $ed \equiv 1 \pmod{\theta}$ (5)
- Diperoleh kunci publik (e, n) dan kunci privat (d, n)
- Untuk memperoleh nilai *signature* digunakan persamaan:
  $s = Hd \bmod n$, (6)
  nilai H diambil dari nilai validasi
- Dan untuk verifikasi digunakan persamaan:

$$v = se \bmod n \ (7) \quad (1)$$

Untuk proses verifikasi nilai tanda tangan digital penerima harus mengetahui kunci publik dan nilai tanda tangan digitalnya. Pada penerima kemudian akan dilakukan perhitungan verifikasi. Hasil dari perhitungan ini harus sesuai dengan nilai validasi yang digunakan oleh pengirim untuk menghasilkan nilai tanda tangan digitalnya.

3. HASIL PENELITIAN

Hasil uji coba penelitian ini menerapkan konsep *public key* dan *private key*. Program aplikasi yang dibuat mengandung proses enkripsi data dan proses dekripsi data. Pada waktu akan mengirim data, pengirim membuat private key untuk pesan dalam SMS yang akan dibuat. Kemudian program akan mengenkripsi pesan yang akan dikirim. Selanjutnya pesan dikirim ke penerima. Dalam prakteknya data SMS akan disimpan oleh operator seluler selama minimal 2 hari. Sehingga seandanya ada sebuah kasus dan pihak kepolisian meminta backup data yang dimiliki oleh operator seluler, data yang diperoleh kepolisian adalah data enkripsi.

Setelah data diterima oleh penerima, pengirim pesan SMS memberitahu *private key* yang dapat dipergunakan untuk membuka pesan SMS tersebut, sehingga penerima SMS dapat membaca data yang sebenarnya dengan terlebih dahulu memasukkan *private key* yang diberi oleh pembuat pesan.

Dari analisa uji coba program diperoleh hasil sebagai berikut :

1. User yang tidak berhak termasuk pihak operator seluler tidak dapat membaca isi pesan SMS yang sebenarnya.
2. User mudah dalam mengoperasionalkan program aplikasi
3. Program aplikasi tidak membebani operasional pesawat telepon seluler

4. SIMPULAN

Dari penelitian yang penulis lakukan dapat disimpulakn sebagai berikut :

1. Konsep private key dan public key didukung oleh teknologi Telepon Seluler
2. Data dan private key dapat mempergunakan jenis komunikasi yang berbeda.
3. Private key dan pubic key dapat diimplemtasikan untuk kepentingan keamanan perangkat teknologi informasi.

5. DAFTAR PUSTAKA

Budi Raharja, 2007, Java untuk Handphone, Penerbit Informatika, Bandung.

Khan, Johanzeb and Khwaja, Anis. 2003. Building Secure Wireless Network With 802.11. Wileyt Publishing, Inc., Indianapolis

Mc. Athur Conklin, 2004. Principle of Computer Security, Mc Graw Hill, New York.

Renaldi Munir, 2006. Kriptografi, Penerbit Informatika, Bandung

Syafrizal, Melwin, 2005. Pengantar Jaringan Komputer, Penerbit Andi, Yogyakarta

Stalling, William, 2000, Data Communication and Computer Network, Prantice Hall International