RANCANG BANGUN APLIKASI SMS DENGAN MENERAPKAN METODE ENKRIPSI KUNCI PUBLIK KURVA ELLIPTIK BERBASIS MOBILE ANDROID

I.Gst. Agung Bagus Mega Putra[1], Gusti Made Arya Sasmita[2], A.A.K. Agung Cahyawan .W[3]
[1,2,3]*Jurusan Teknik Elektro dan Komputer Fakultas Teknik Universitas Udayana*
Email: ajusgunkmega@yahoo.co.id[1], aryasasmita@it.unud.ac.id[2], agung.cahyawan@gmail.com[3]

ABSTRAK

Pada jaman sekarang dengan adanya teknologi short message service seseorang dapat dengan mudah melakukan pertukaran pesan, namun pertukaran pesan yang bersifat rahasia sangat berbahaya jika dilakukan dengan short message service karena short message service tersebut dapat diketahui oleh orang yang berhasil melakukan penyadapan. Salah satu teknik yang dapat dipakai untuk menangani hal tersebut adalah kriptografi kurva elliptik. Disini dilakukan studi mengenai perancangan aplikasi short message service dengan menerapkan metode enkripsi kunci publik kurva elliptik berbasis mobile android yang diimplementasikan kedalam bahasa pemrograman java menggunakan Android Studio. Hasil analisa yang diperoleh bahwa aplikasi sistem keamanan short message service dengan metode kurva elliptik ini dapat diterapkan untuk menjamin kerahasiaan data dan otentikasi pengirim. Dalam pengujian untuk sebuah short message service aplikasi ini masih memiliki keterbatasan hanya mampu mengolah maksimal 57 karakter.
***Kata kunci:**, short message service, kriptografi, kurva elliptik*

ABSTRACT

At the present, short message service enables people to communicate easily, however secret messages as prone to be hacked. One technique that can be used to deal with such matters is the elliptic curve cryptography. Here we carried out a study to design applications short message service by applying the method of public key encryption elliptic curve based mobile android implemented into the java programming language using Android Studio. The results of the analysis showed that the security system applications short message service with the elliptic curve method can be applied to ensure data confidentiality and sender authentication. In testing for a short message service application still has limitations only able to process a maximum of 57 characters.
***Keyword** : short message service , cryptography, elliptic curve*

1. PENDAHULUAN

Pengamanan akan suatu pesan yang rahasia memang sangat diperlukan, pada jaman sekarang dengan adanya teknologi sms seseorang dapat dengan mudah melakukan pertukaran pesan, namun pertukaran pesan yang bersifat rahasia sangat berbahaya jika dilakukan dengan sms karena sms tersebut dapat diketahui oleh orang yang berhasil melakukan penyadapan. Kerahasiaan sebuah pesan sangatlah penting, penelitian yang dilakukan oleh I Wayan Dharma Satriawan (2013) dengan judul "Aplikasi Enkripsi SMS Dengan Metode RSA Pada Smartphone Berbasis Android" telah menghasilkan aplikasi enkripsi SMS. Pada proses pengiriman SMS terdapat beberapa langkah yang dilakukan seperti meng*input*kan *public key* dan meng*input*kan pesan yang akan dikirim. [1]

Penelitian yang dilakukan oleh Wijaya (2013) dengan judul "Rancang Bangun Aplikasi Enkripsi dan Dekripsi Berbasis *Android* dengan Menggunakan Algoritma *Hybrid DES* dan *Elgamal"* telah menghasilkan aplikasi enkripsi dan dekripsi pesan pada ponsel berbasis Android yang dapat menjaga kerahasiaan pesan, mudah digunakan, bekerja sesuai fungsinya, sudah memenuhi standar kebutuhan, *user friendly* dengan tampilan antarmuka aplikasi yang cukup menarik. [2]

Penelitian yang dilakukan oleh Muhamad (2012) dengan judul "Rancang Bangun Aplikasi Enkripsi SMS Menggunakan Metode RC 4 Berbasis Platform Android" telah menghasilkan aplikasi RQSSms. Pada proses pengiriman SMS terdapat beberapa langkah yang dilakukan seperti meng*input*kan *password* dan meng*input*kan pesan yang akan dikirim. [3]

Penelitian ini dilakukan untuk menciptakan aplikasi yang dapat menjaga kerahasiaan SMS dan akan dibuat pada *platform* android.

2. KAJIAN PUSTAKA

Berisikan tentang teori-teori penunjang yang dijadikan sebagai acuan yang meliputi Algoritma Rivest Code 5 dan Base 64.

2.1 Algoritma Rivest Code 5

Algoritma *cipher* simetri Rivest Code 5 dirancang oleh Ron Rivest dari Laboratorium RSA MIT. Rivest Code 5 dipublikasikan pada Desember 1994. Rivest Code 5 adalah algoritma *cipher* blok simetri yang terparameterisasi dengan 3 parameter utama, yaitu: w, r, dan b. Oleh karena itu algoritma Rivest Code 5 dapat juga ditulis secara lebih spesifik dengan penulisan : **RC5 - w /r /b**. [4]

2.2 Base 64

Base 64 adalah sebuah skema *encoding* yang merepresentasikan data biner ke dalam format ASCII. Umumnya digunakan pada berbagai aplikasi, seperti email via MIME, data XML, atau keperluan *encoding* URL. Penggunaan lain *encoding* Base64 adalah untuk melakukan obfuscation atau pengacakan data. ASCII (American Standard Code for Information Interchange) merupakan suatu standar internasional dalam kode huruf dan simbol seperti Hex dan Unicode tetapi ASCII lebih bersifat universal. Ia selalu digunakan oleh komputer dan alat komunikasi lain untuk menunjukkan teks. Kode ASCII memiliki komposisi bilangan biner sebanyak 8 bit. Dimulai dari 0000 0000 hingga 1111 1111. Total kombinasi yang dihasilkan sebanyak 256, dimulai dari kode 0 hingga 255 dalam sistem bilangan Desimal. [5]

3. METODOLOGI PENELITIAN

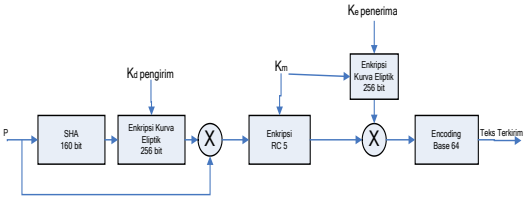
Langkah-langkah dari Rancang Bangun Aplikasi SMS Dengan Menerapkan Metode Enkripsi Kunci Publik Kurva Elliptik Berbasis *Mobile* Android yang dilakukan dalam penelitian ini adalah sebagai berikut :

1. Pendefinisian permasalahan yang akan ditangani sistem yaitu keberhasilan proses enkripsi dan dekripsi pesan.
2. Mendesain sistem dan pembuatan perangkat lunak berbasis android.
3. Penggunaan metode Algoritma Kriptografi Kurva Elliptik untuk mengetahui keberhasilan dalam proses enkripsi dan dekripsi.

3.1 Data Dan Sumber Data

Data yang nantinya digunakan dalam pembuatan aplikasi sms dengan menerapkan metode enkripsi kunci publik kurva elliptik berbasis *mobile* android ini diperoleh dari internet, studi literatur buku-buku, serta beberapa dokumen (dalam bentuk *file* PDF) dari internet.

3.2 Gambaran Umum Sistem



Gambar 3.1 Proses Enkripsi Pesan

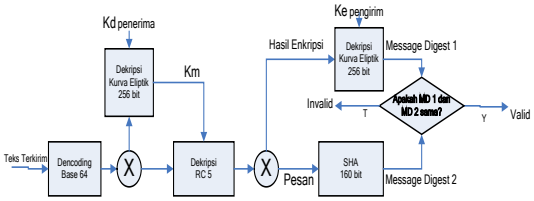
Keterangan :

P : Pesan
K_d : *Private Key*
K_e : *Public Key*
K_m : *Password* pada RC5

Gambar diatas merupakan gambaran umum proses enkripsi pesan. Pengirim akan melakukan tindakan berikut untuk membuat dan mengirim pesan :

1. Pengirim menghasilkan pesan.
2. Hitung pesan *digest* dengan menggunakan fungsi hash SHA 160 bit.
3. Pesan *digest* akan dienkripsi dengan *private key* pengirim dengan menggunakan algoritma kunci publik kurva elliptik 256 bit.
4. Menandatangani pesan *digest* ke pesan.
5. Kemudian terjadi proses enkripsi pesan *digest* tersebut menggunakan algoritma simetri Rivest Code 5.
6. Kunci publik kurva elliptik akan diterapkan ke pesan terenkripsi.
7. Untuk transmisi Km, akan dienkripsi dengan menerapkan kurva eliptik 256 bit menggunakan *public key* penerima.

8. *Encoding* pesan tersebut ke Base 64, lalu kirimkan pesan tersebut ke penerima.



Gambar 3.2 Proses Dekripsi Pesan
Keterangan :

K_d : *Private Key*
K_e : *Public Key*
K_m : *Password* pada RC5
MD : *Message Digest*

Gambar diatas merupakan gambaran umum proses dekripsi pesan. Penerima melakukan tindakan berikut untuk mendapatkan pesan asli, mengotentikasi pengirim dan memeriksa integritas pesan :

1. Pertama *dencoding* dulu pesan tersebut ke Base 64.
2. Dapatkan enkripsi Km dengan mendekripsi itu. Untuk ini, mengusulkan penerima menggunakan *private key* penerima dengan algoritma kunci publik kurva elliptik 256 bit.
3. Hasilnya akan didekripsi menggunakan Rivest Code 5. Setelah dekripsi, penerima akan mendapatkan pesan asli dan ditandatangani pesan *digest*.
4. Agar bisa otentikasi dan memeriksa integritas, penerima mendekripsi pesan *digest* yang ditandatangani pengirim dengan menggunakan *public key* pengirim dan mendapatkan *message digest* 1.
5. Selain itu, penerima menghitung pesan asli menggunakan fungsi hash SHA 160 bit dan mendapatkan *message digest* 2.
6. Terakhir, penerima membandingkan pesan *digest* 1 dan pesan *digest* 2. Jika hasil perbandingan pesan *digest* adalah sama, maka pesan dianggap valid.

4. HASIL DAN PEMBAHASAN

Membahas hasil mengenai Rancang Bangun Aplikasi SMS Dengan Menerapkan Metode Enkripsi Kunci Publik Kurva Elliptik Berbasis *Mobile* Android.

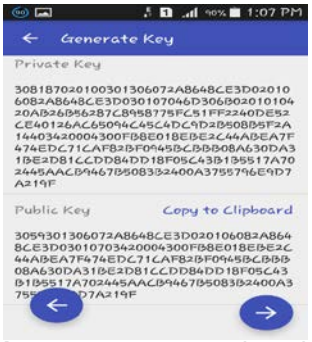
4.1 Proses Implementasi Aplikasi ECDSA Messenger

Pada tahap implementasi ini masih menggunakan HP Samsung Galaxy V dan Samsung Galaxy S Advance.
Contoh :
Pengirim ingin mengirimkan pesan rahasia ke penerima. Berikut tahap implementasi dari aplikasi ECDSA Messenger :

1. Pengirim membuka aplikasi ECDSA Messenger dan pilih *Create Message*. Ketik no. tujuan penerima (087761192615) dan isi pesan (“Halo”), kemudian klik tombol next untuk melakukan proses pembangkitan kunci privat dan kunci public

Gambar 4.1 Menulis Pesan

2. Lalu akan terlihat kunci privat dan kunci publik seperti pada gambar 4.2, kemudian klik tombol next untuk melakukan proses digital signature



Gambar 4.2 Proses Pembangkitan Kunci

3. Disini akan terlihat hasil proses digital signature seperti pada gambar 4.3, lalu klik tombol next untuk mengirim pesan yang telah dienkripsi ke penerima

Gambar 4.3 Proses Digital Signature

4. Masuk ke menu inbox, kemudian buka pesan tersebut untuk melakukan proses dekripsi. Disini penerima melihat pesan terenkripsinya. Klik tombol *next* untuk masuk ke proses *verify signature,* dimana nanti disana akan dilakukan proses dekripsi pesan

Gambar 4.4 Membuka Pesan Masuk

5. Kemudian penerima melakukan proses dekripsi pesan agar pesan masuk dapat dibaca. Penerima memasukkan *public key* dan hasil dari proses *digital signature* yang telah dikirim oleh pengirim dengan cara men-klik *"Paste From Clipboard"* untuk men-*paste public key* dan hasil dari proses *digital signature*

Gambar 4.5 Proses *Verify Signature*

6. Terakhir klik tombol *verify* untuk mendekripsi pesan agar pesan dapat dibaca. Teks pesan "Halo" dapat dibaca oleh penerima

Gambar 4.6 Proses *Encode Message*

5. SIMPULAN

Simpulan yang dapat diambil dari permasalahan dan analisis dari hasil pengujian sistem dapat dilihat sebagai berikut:

1. Aplikasi keamanan pesan SMS dibangun dengan menerapkan metode *kurva elliptik* dan *digital signature* ini dapat diterapkan untuk menjamin kerahasiaan data dan otentikasi pengirim.
2. Aplikasi ini memperoleh kunci publik dengan cara membangkitkan kunci privat dan kunci publik digunakan untuk proses dekripsi pesan, selain itu *digital signature* digunakan untuk menjamin kerahasiaan data dan otentikasi pengirim. Kunci publik akan dikirimkan ke penerima menggunakan SMS.
3. Pengujian untuk sebuah SMS, aplikasi ini masih memiliki keterbatasan hanya mampu mengolah maksimal 57 karakter.

6. DAFTAR PUSTAKA

[1] Satriawan, I.W.D. 2013. Aplikasi Enkripsi SMS Dengan Metode RSA Pada Smartphone Berbasis Android. *Journal Merpati Jurusan Teknologi Informasi Universitas Udayana. Volume 2, No. 2: 1-8*.

[2] Wijaya, Aris, K. 2013. Rancang Bangun Aplikasi Enkripsi dan Dekripsi Berbasis *Android* dengan Menggunakan Algoritma *Hybrid DES* dan *Elgamal*. *Journal STMIK GI MDP. Hal 1-11.*

[3] Eko, Muhamad. 2012. Rancang Bangun Aplikasi Enkripsi SMS Menggunakan Metode RC 4 Berbasis Platform Android. *Journal Sarjana Teknik Informatika Universitas Trunojoyo Madura. Volume 1, No. 1: 1-8.*

[4] Roland. 2006. Perbandingan Algoritma Block Chiper RC5 dan RC6. Institut Teknologi Bandung.

[5] Adriansyah, Yusuf. 2009. Enkripsi Sederhana dengan Base64 dan Substitusi Monoalfabetik ke Huruf Non – Latin. Institut Teknologi Bandung.