Penerapan Algoritma *Elliptic Curve Cryptography* Untuk Enkripsi dan Penandatanganan Data Pada Sistem Informasi Geografis (SIG)

Eric Cahya Lesmana (13508097)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
eric_310@students.itb.ac.id

Sistem Informasi Geografis (SIG) merupakan sistem informasi khusus yang mengelola mengenai data spasial, yaitu data yang bereferensi keruangan. Sistem ini mampu untuk membangun, menyimpan, mengelola, dan menampilkan data atau informasi bereferensi geografis, misalnya pemetaan jalan, pemetaan tempat wisata, dan persebaran penduduk. Dalam pengembangan terintegrasi, sistem ini dituntut untuk memiliki data yang terpercaya karena harapannya dapat memberikan informasi yang akurat sehingga dapat digunakan secara umum. Untuk mencapai hal tersebut, sistem ini dihadapkan dengan masalah keamanan. Pengiriman data dapat dilakukan melalui jaringan internet sehingga mungkin adanya serangan. Komunikasi juga dapat dilakukan melalui aplikasi *mobile*. Ketika seseorang mengetahui alamat *mapservice* dan memiliki akses ke server dapat memberikan data yang tidak tidak terpercaya atau mencuri data.

Dari penjelasan sebelumnya, diberikan salah satu solusi untuk mengatasi masalah tersebut dengan kriptografi. Solusinya adalah menggunakan algoritma *Elliptic Curve Cryptography* untuk melakukan enkripsi data dan penandatanganan data. Enkripsi data digunakan untuk menjaga data supaya tidak dapat dibaca oleh pihak yang tidak berwenang. Penandatanganan digunakan untuk verifikasi data ketika terdapat pengolahan data di *server* oleh *client*.

Kata kunci: SIG, ECC, enkripsi, tandatangan

I. PENDAHULUAN

Pada saat ini telah berkembang Sistem Informasi Geografis (SIG). SIG merupakan sistem informasi khusus yang mengelola mengenai data spasial, yaitu data yang bereferensi keruangan. Sistem ini mampu untuk membangun, menyimpan, mengelola, dan menampilkan data atau informasi bereferensi geografis, misalnya pemetaan jalan, pemetaan tempat wisata, dan persebaran penduduk. Saat ini mulai berkembang Sistem Informasi Geografis ini. Salah satu keuntungannya adalah dalam hal visualisasi yang menyertakan lokasi dan dapat ditampilkan dalam bentuk grafik. Pemanfaatannya juga semakin banyak, seperti pemetaan jalur transportasi, pemetaan tempat wisata, pemetaan pertambangan, dan sebagainya. Bahkan sistem ini juga mulai dikembangkan terintegrasi untuk beberapa data, misalnya data jalan dengan tempat wisata dan penginapan atau hotel. Salah proyek terintegrasi dalam bidang SIG adalah Jaringan Spasial Data Nasional (JSDN) yang merupakan program pemerintah.

Dalam pengembangan terintegrasi, sistem ini dituntut untuk memiliki data yang terpercaya karena harapannya dapat memberikan informasi yang akurat sehingga dapat digunakan secara umum. Untuk mencapai hal tersebut, sistem ini dihadapkan dengan masalah keamanan. Pengiriman data dapat dilakukan melalui jaringan internet sehingga mungkin adanya serangan. Selain itu, data spasial tersebut ada yang bersifat rahasia. Komunikasi juga dapat dilakukan melalui aplikasi *mobile*. Ketika seseorang mengetahui alamat *mapservice* dan memiliki akses ke server dapat memberikan data yang tidak tidak terpercaya atau mencuri data.

Dari penjelasan sebelumnya, diberikan salah satu solusi untuk mengatasi masalah tersebut dengan kriptografi. Solusinya adalah menggunakan algoritma *Elliptic Curve Cryptography* untuk melakukan enkripsi data dan penandatanganan data. Enkripsi data digunakan untuk menjaga data supaya tidak dapat dibaca oleh pihak yang tidak berwenang. Penandatanganan digunakan untuk verifikasi data ketika terdapat pengolahan data di *server* oleh *client*. Batasan dalam makalah ini adalah analisis dan perancangan arsitektur dalam SIG, yang dalam hal ini menggunakan referensi dari produk ESRI.

II. DASAR TEORI

1. Sistem Informasi Geografis

SIG merupakan integrasi dari perangkat keras, perangkat lunak, dan data untuk merekam, mengatur, menganalisis, dan menampilkan ke dalam bentuk spasial. Dengan SIG kita dapat melihat, memahami, dan mengintepretasikan data ke dalam berbagai bentuk, hubungan, dan pola. Model visualisasi tersebut dapat berupa peta, grafik, maupun laporan. Dengan SIG masalah dapat lebih mudah diatasi dengan visualisasi yang lebih mudah dan cepat dimengerti.

ESRI

ESRI merupakan sebuah penyedia layanan tentang SIG terintegrasi. Dalam ESRI terdapat beberapa teknologi yang mendukung pengembangan SIG. Teknologi tersebut adalah:

a. Pembuatan web service

b. Pembuatan web service

c. Pembuatan GeoExplorer

d. Pengembangan aplikasi *mobile* sebagai pendukung.

2. Algoritma *Elliptic Curve Cryptography* (ECC)

Kriptografi kurva eliptik termasuk ke dalam sistem kriptografi kunci publik yang mendasarkan keamanannya pada permasalahan matematis kurva eliptik. Tidak seperti permasalahan matematis logaritma diskrit (*Discrete Logarithm Problem*, DLP) dan pemfaktoran bilangan bulat (*Integer Factorization Problem*, IFP), tidak ada algoritma waktu subeksponensial yang diketahui untuk memecahkan permasalahan matematis logaritma diskrit kurva eliptik (*Elliptic Curve Discrete Logarith Problem*, ECDLP). Karena alasan tersebut, algoritma kriptografi kurva eliptik mempunyai keuntungan jika dibandingkan dengan algoritma kriptografi kunci publik lainnya yaitu dalam hal ukuran panjang kunci yang lebih pendek tetapi memiliki tingkat keamanan yang sama. Ada tiga protokol ECDLP yang diketahui saat ini yaitu *Elliptic Curve Digital Signature Algorithm* (ECDSA), *Elliptic Curve Diffie Hellman* (ECDH), dan *Elliptic Curve ElGamal* (ECElgamal). *Elliptic Curve Cryptography* (ECC) adalah salah satu pendekatan algoritma kriptografi kunci publik berdasarkan pada struktur aljabar dari kurva ellips pada daerah finite.

Penggunaan kurva ellips dalam kriptografi dicetuskan oleh Neal Koblitz dan Victor S. Miller pada tahun 1985. Kurva ellips juga digunakan pada beberapa algoritma pemfaktoran integer yang juga memiliki aplikasinya dalam kriptografi, seperti *Lenstra Elliptic Curve Factorization*. Algoritma kunci publik berdasarkan pada variasi perhitungan matematis yang terbilang sangat sulit dipecahkan tanpa pengetahuan tertentu mengenai bagaimana perhitungan tersebut dibuat. Pembuat algoritma menyimpan kunci privat dan menyebarkan kunci publiknya. Algoritma kunci publik digunakan untuk mengenkripsi pesan dimana hanya pembuat algoritma yang dapat memecahkannya. Sistem kunci publik awal, seperti algoritma RSA, menggunakan dua bilangan prima yang sangat besar: pengguna memilih dua bilangan prima random yang besar sebagai kunci privatnya, dan mempublikasikan hasil dari perhitungannya sebagai kunci publik. Pemfaktoran bilangan-bilangan besar yang sangat sulit dapat menjaga kerahasiaan kunci privat dari publik.

Persoalan lain menyangkut perhitungan aljabar ab = c, dimana a dan c diketahui. Perhitungan semacam itu menyangkut bilangan kompleks atau real yang dapat dengan mudah dipecahkan menggunakan logaritma. Tetapi dalam kumpulan bilangan finite yang besar, menemukan solusi untuk perhitungan semacam itu sangat sulit dan dikenal sebagai "discrete logarithm problem". Kurva ellips dapat ditulis dengan perhitungan matematis sebagai berikut:

$$y^2 = x^3 + ax + b$$

Kumpulan titik pada kurva dapat membentuk kumpulan abelian (dengan titik pada tak terhingga sebagai elemen identitas). Jika nilai x dan y dipilih dari daerah finite yang besar, solusi akan membentuk suatu kumpulan abelian finite. Permasalahan logaritma diskrit pada kumpulan kurva ellips tersebut dipercaya lebih sulit dibandingkan permasalahan yang sama (perkalian bilangan tidak nol) dalam daerah finite. Selain itu, kunci dalam algoritma kriptografi kurva ellips dapat dipilih lebih pendek panjangnya untuk keamanan yang cukup tinggi. Sebagai salah satu kriptosistem kunci publik, belum ada pembuktian matematis untuk tingkat kesulitan dari ECC yang telah dipublikasikan sampai tahun 2006. Tetapi U.S. National Security Agency telah mengesahkan teknologi ECC sebagai algoritma kriptografi yang dianjurkan.

Tidak seperti kriptografi kunci publik konvensional yang didasari oleh aritmatika pada bidang yang terbatas (*finite field*), ECC beroperasi pada kumpulan poin pada sebuah kurva elips yang didefinisikan diatas sebuah bidang terbatas. Operasi kriptografi utamanya adalah scalar point multiplication, yang akan menghitung Q = k P (sebuah titik P dikalikan dengan suatu bilangan bulat k menghasilkan sebuah titik Q pada kurva). Perkalian skalar dilakukan lewat sebuah kombinasi dari penambahan titik dan doubling titik. Sebagai contoh, 11P dapat dijabarkan menjadi 11P = (2((2(2P)) + P)) + P.

El Gamal ECC

Dalam algortima ElGamal ECC, terdapat besaran yang digunakan, yaitu:

1. CBilangan prima p (tidak rahasia)
2. Bilangan acak g, dengan g<p (tidak rahasia)
3. Bilangan acak x, dengan x<p (rahasia)
4. m sebagai plainteks (rahasia)
5. a dan b sebagai chiperteks (tidak rahasia)

Pada algoritma ElGamal ECC terdapat tiga buah prosedur dalam melakukan proses enkripsi, yaitu penentuan kunci, enkripsi, dan dekripsi.

Algoritma pembuatan kunci sebagai berikut:

1. Ditentukan kurva elips yang akan digunakan.
2. Ditentukan elemen Gα sedemikian sehingga Gα merupakan elemen pembangun dari grup G atas Fp.
3. Dipilih bilangan bulat V∈[1, n-1], dengan n merupakan order dari Gα.
4. Dihitung β = (Gα)V
5. Keluaran yang dihasilkan adalah (V, β), dengan V sebagai kunci privat dan β sebagai kunci publik.

Algoritma enkripsi sebagai berikut:

1. Plainteks disusun menjadi blok-blok m1, m2, dan seterusnya dengan setiap blok memiliki nilai antara 0 sampai p-1.
2. Dipilih bilangan acak k yang relatif prima dengan p-1 dan k memiliki rentang antara 0 dan p-1.
3. Setiap blok m dienkripsi dengan rumus

   a = gk mod p

   b = ykm mod p
4. Pasangan (a, b) adalah hasil chiperteks dari setiap blok m. Hal ini membuat ukuran chiperteks menjadi dua kali lipat ukuran plainteks.

Algoritma dekripsi sebagai berikut:

1. Diperoleh beberapa pasang chiperteks yang bersesuaian dengan plainteks.
2. Setiap pasang chiperteks dilakukan perhitungan m_i = b.(a).V, dengan V adalah kunci privat
3. Melakukan konversi m ke dalam plainteks dan dilakukan penggabungan.

Algoritma *Elliptic Curve Digital Signature* (ECDS)

Algortima ECDS menggunakan skema kurva eliptik sebagai dasar keamanannya. Fungsi utama dari algoritma ini adalah sebagai penandatangan sebuah berkas. Hasilnya dapat digunakan untuk menentukan apakah berkas tersebut valid atau tidak.

Pada algoritma ECDS terdapat beberapa parameter domain. Parameter domain tersebut terdiri dari pilihan yang sesuai dengan kurva eliptik E. Kurva E ini didefiniskan melebihi bidang tak hingga Fq dari karakteristik p serta sebuah titik dasar G $\in$ E(Fq). Parameter domain tersebut terdiri dari:

1. Sebuah bidang ukuran q, yang memenuhi salah satu syarat q = p, prima ganjil, atau $q = 2^m$.
2. Sebuah indikasi FR (Field Representation).
3. Dua elemen bidang x_g dan y_g dalam Fq yang mendefiniskan sebuah titik tak hingga G = (x_g, y_g) dari orde prima dalam E(Fq).
4. Orde n dari titik G, dengan $n > 2^{160}$ dan $n > \sqrt[4]{q}$.
5. Kofaktor h = E(Fq)/n

Dalam melakukan proses penandatanganan diperlukan parameter domain D = {q, FR, a, b, G, n, h} dan pasangan kunci rahasia d_A dan kunci publik Q_A. Dalam proses verifikasi diperlukan dokumen d dan kunci publik Q_A.

Proses pembuatan kunci adalah sebagai berikut:

1. Dipilih sebuah bilangan bulat acak d_A yang nilainya antara 1 dan n-1.
2. Dihitung $Q_A = d_A \bullet G = (x_1, y_1)$
3. Dihasilkan kunci pribat d_A dan kunci publik Q_A.

Proses penandatanganan sebagai berikut:

1. Dipilih bilangan bulat acak k yang nilainya antara 1 dan n-1.
2. Dihitung $Q_A = k \bullet G = (x_1, y_1)$ dan $r = x_1 \bmod n$. Jika r = 0 kembali ke langkah 1.
3. Dihitung nilai m = (k-1) mod n.
4. Dihitung e = Hash (m).
5. Dihitung $s = k\text{-}1\{e + d_A \bullet r\} \bmod n$.
6. Diperoleh hasil tandatangan untuk pesan adalah (r,s)

Proses verifikasi adalah sebagai berikut

1. Dilakukan pengecekan untuk r dan s adalah bilangan bulat antara 1 dan n-1.

2. Dihitung e = Hash (m).
3. Dihitung x = (s-1) mod n.
4. Dihitung u_1 = ew mod n dan u_2 = rw mod n.
5. Dihitung $u_1 \bullet G + u_2 \bullet Q_A = (x_1, y_1)$
6. Dihitung v = x_1 mod n.
7. Menerima tandatangan jika dan hanya jika v = r.

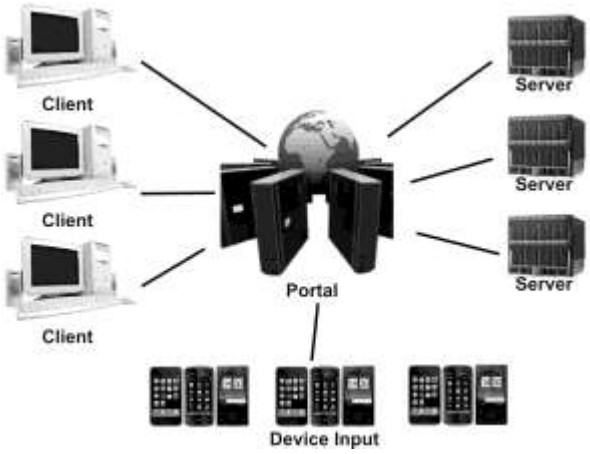
III. ANALISIS PERANCANGAN MODEL

Gambaran sistem pada ESRI secara global

ESRI menyediakan berbagai teknologi yang mendukung Sistem Informasi Geografis (SIG). Fungsi dasar yang diberikan dari teknologi ESRI ini adalah:

1. Sistem mampu menampilkan data spasial
2. Sistem mampu menambah, menghapus, atau mengubah data spasial.
3. Sistem mampu mengintegrasikan data spasial dari beberapa server

Dari teknologi pada ESRI dapat dibuat arsitektur sistem secara global seperti pada gambar 3.1.



Gambar 3.1 Arsitektur umum sistem

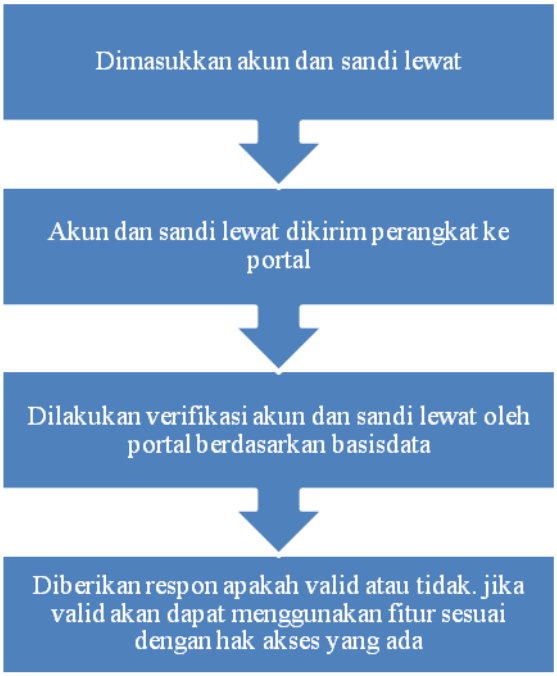
Dari arsitektur tersebut, terdapat beberapa bagian. Bagian yang pertama adalah portal. Portal ini merupakan koordinator dari seluruh bagian yang ada dalam sistem. Portal yang melakukan komunikasi, merespon permintaan, dan menghubungkan antar elemen, misalnya antarserver. Bagian kedua adalah server. Server ini menyimpan data spasial. Pada umumnya satu server menyimpan satu bidang data spasial, misalnya data perhubungan. Dengan satu server dapat ditampilkan data spasial yang lengkap terkait bidang tersebut. Namun data tersebut juga dapat diintegrasikan dengan data spasial dengan bidang lain, misalnya perhubungan dengan pariwisata. Bagian ketiga adalah perangkat nirkabel (*smartphone*) yang digunakan untuk menambah data, menghapus, atau mengubah data spasial pada suatu server. Perangkat ini melakukan komunikasi dengan portal untuk dapat mengakses data pada server. Selain itu, perangkat ini juga dapat menampilkan data spasial dari seluruh server yang terhubung sesuai dengan hak akses pengguna. Bagian terakhir adalah komputer *client* yang berfungsi untuk melihat tampilan data spasial.

Arsitektur tersebut bukan merupakan arsitektur yang statis sehingga dapat dimungkinkan untuk dilakukan pengubahan sesuai dengan kebutuhan yang ada. Namun secara umum arsitektur seperti pada gambar 3.1 sudah dapat menjalankan fungsi SIG secara terintegrasi.

Analisis terkait celah keamanan

Jika dilihat dari arsitektur tersebut, hal yang menjadi fokus adalah keamanan data. Data yang diberikan harus merupakan data yang valid dan hanya bisa dilihat oleh orang yang memilik hak akses. Dimungkinkan terdapat celah keamanan dalam hal ini karena komunikasi data dilakukan dari perangkat nirkabel dengan portal. Ketika jalur komunikasinya dibajak, data akan dapat disadap oleh penjahat. Oleh karena itu, fokus selanjutnya adalah terkait komunikasi antara perangkat nirkabel dengan portal.

Penanganan masalah ini pada umumnya dilakukan dengan otentikasi berupa akun dan sandi lewat. Cara ini cukup baik karena pada awal menjalankan perangkat harus memasukkan akun dan sandi lewat. Proses dari otentikasi tersebut dapat dilihat pada gambar 3.2.



Gambar 3.2 Otentikasi dengan akun dan sandi

Dari analisis prosedur tersebut, masih terdapat celah keamanan. Ketika saluran komunikasi setelah berhasil *login* dibajak, penjahat dapat melakukan modifikasi data. Untuk memperkuat keamanan, diusulkan untuk menambah kriptografi ke dalam komunikasi. Tujuan utamanya adalah untuk menjaga kerahasiaan data dan melakukan verifikasi data.

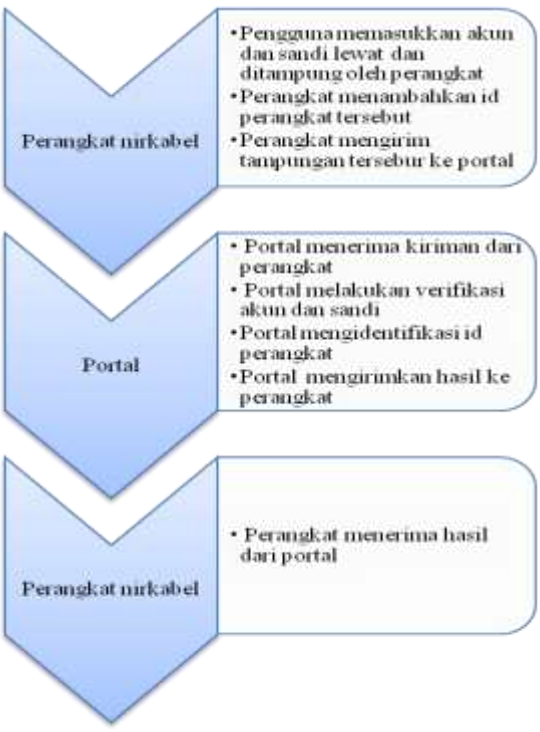
Perancangan ECC ke dalam sistem

Untuk menyisipkan kriptografi ke dalam sistem perlu dilakukan perancangan supaya tujuan utama tercapai. Terdapat dua hal yang akan dilakukan supaya data lebih aman dan terpercaya, yaitu: enkripsi dan penandatanganan. Dua hal ini akan mulai disisipkan ke dalam komunikasi mulai dari awal sampai akhir penggunaan aplikasi sistem ini. Hal penting yang harus ada untuk menunjang rancangan ini adalah:

1. Perangkat nirkabel yang digunakan harus terdaftar pada portal.
2. Setiap perangkat memiliki pasangan kunci privat dan kunci publik yang berbeda satu sama lain. Pasangan kunci tersebut terdiri dari pasangan kunci untuk enkripsi dan pasangan kunci untuk penandatanganan. Pasangan kunci tersebut juga terdaftar dalam portal.

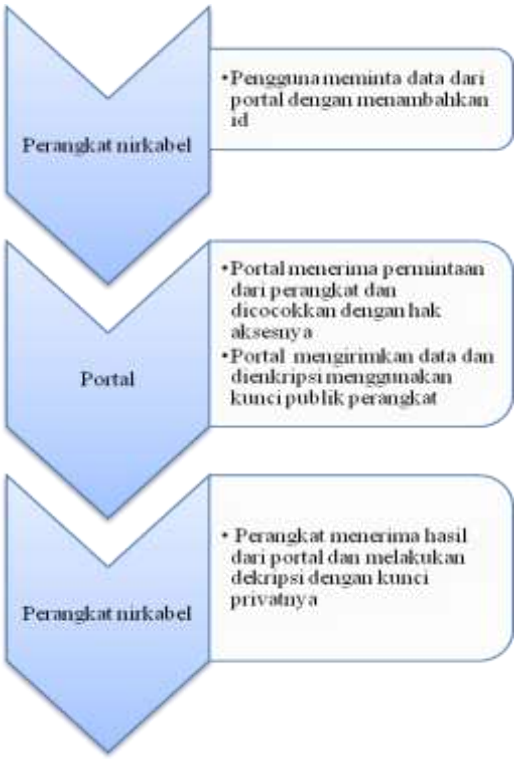
Dengan ketentuan yang sudah ada, terdapat dua proses penting yang ada dalam rancangan ini, yaitu pada saat *login* dan modifikasi data.

Proses pada saat login sebagai berikut:

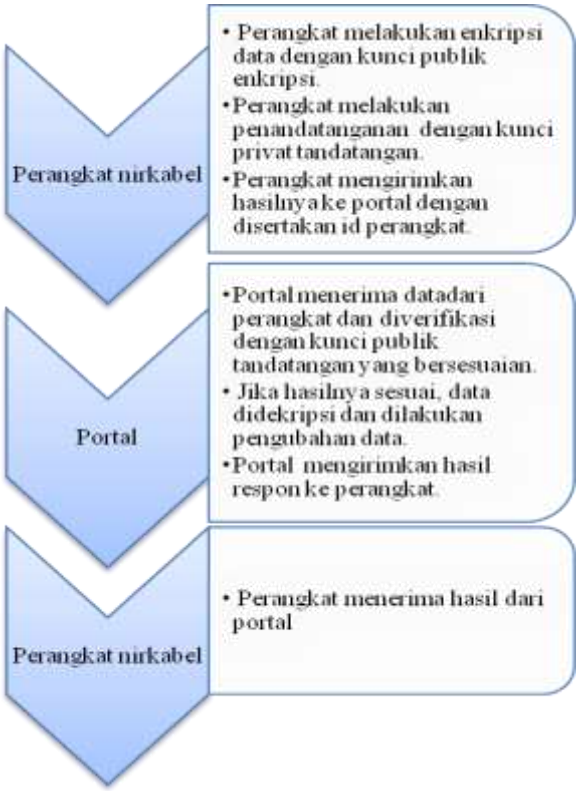


Gambar 3.3 Rancangan komunikasi pada saat *login*

Proses pada saat modifikasi data dibagi menjadi dua bagian, yaitu permintaan data dan pengiriman data.



Gambar 3.4 Rancangan komunikasi pada saat meminta data ke portal



Gambar 3.5 Rancangan komunikasi pada saat mengirimkan data ke portal

IV. PEMBAHASAN

Dari perancangan yang telah diberikan diketahui bahwa terdapat proses tambahan yang memanfaatkan kriptografi, yaitu pada saat login, meminta data, dan mengirim data. Pada saat login, terdapat penambahan pengiriman id. Hal ini ditujukan supaya portal mengenali perangkat yang sedang berkomunikasi dengannya. Hal ini bertujuan supaya perangkat yang digunakan adalah perangkat yang valid, selain penggunanya juga harus valid. Oleh karena itu disisipkan prosedur pengiriman id perangkat.

Selanjutnya, untuk model komunikasi permintaan data, terdapat hal penting yang dilakukan oleh portal dan perangkat, yaitu proses enkripsi dan dekripsi. Proses dilakukan supaya data yang dikirimkan tidak dapat dibaca oleh penyadap. Terkadang informasi ini sangat penting dan bersifat rahasia sehingga harus dijaga keamanannya. Dengan model enkripsi dan dekripsi harapannya dapat membantu menjaga keamanan data. Dalam komunikasi ini, kunci publik dan kunci privat sudah tercatat dalam portal sehingga tidak perlu untuk saling bertukar.

Pada model komunikasi pengiriman data, terdapat tambahan proses yaitu penandatanganan. Dalam proses permintaan data sebelumnya tidak diberikan penandatangan karena data yang diminta hanya ditampilkan. Pada proses pengiriman data ini perlu ada penandatanganan supaya data yang akan disimpan benar-benar valid. Dengan kunci publik dan kunci privat yang hanya diketahui oleh portal dan perangkat maka dapat menjaga kevalidan data.

Dalam penggunaan algoritma, perangkat dapat membagi pesan komunikasi, misalnya berupa xml, ke dalam beberapa blok. Sesuai dengan algoritma ECC, blok tersebut dapat dilakukan enkripsi masing-masing sampai selesai dan digabungkan kembali. Untuk melakukan penandatanganan dapat menggunakan hasil enkripsi tersebut dan disisipkan tandatangannya. Selanjutnya untuk verifikasi dan dekripsi dapat dilakukan sesuai dengan alur yang diberikan. Dari penjelasan tersebut, dapat diketahui bahwa blok pesan dapat diambil dari blok byte pesan keseluruhan. Selanjutnya blok tersebut dapat dioleh sesuai dengan prosedur algoritma. Oleh karena itu, algoritma ECC dapat ini diimplementasikan pada komunikasi pesan ini.

Penggunaan algortima ECC ini sesuai dengan perangkat karena beberapa keunggulannya, yaitu dengan kunci yang pendek dapat memberikan tingkat keamanan yang besar. Selain itu, implementasi algoritma ini cukup ringan dan banyak diimplementasikan dalam perangkat *mobile*.

V. SIMPULAN

Dari pembahasan dalam makalah ini dapat disimpulkan beberapa hal, yaitu:

1. Algoritma *Elliptic Curve Cryptography* dapat digunakan untuk menambah tingkat keamanan Sistem Informasi Geografis.
2. Model keamanan yang dapat diberikan adalah enkripsi dan penandatanganan.

REFERENSI

[1] Adam, Wahab. (2009.). Pemanfaatan Algoritma ECDSA untuk Penandatanganan Digital *Chipertext ElGamal Elliptic Curve Cryptography*. UPN. Jakarta.

[2] Harkenson, Darrel, dkk. (2003.). Guide to Elliptic Curve Cryptography. Springer. Canada.

[3] Mardianto, Eko, dkk. (2009.). Enkripsi SMS Menggunakan ECC. ITS. Surabaya.

[4] http://www.esri.com

[5] http://www.gis.com/content/what-gis

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 14 Mei 2012

Eric Cahya Lesmana (13508097)