ENKRIPSI DAN DEKRIPSI DATA
MENGGUNAKAN ALGORITMA ElGamal ECC
(*ElGamal ELLIPTIC CURVE CRYPTOGRAPHY*)

oleh

WAN KHUDRI

M0198088

SKRIPSI

ditulis dan diajukan untuk memenuhi sebagian persyaratan

memperoleh gelar Sarjana Sains Matematika

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS SEBELAS MARET

SURAKARTA

2005

PENGESAHAN

SKRIPSI
ENKRIPSI DAN DEKRIPSI DATA
MENGGUNAKAN ALGORITMA ElGamal ECC
(*ElGamal ELLIPTIC CURVE CRYPTOGRAPHY*)

yang disiapkan dan disusun oleh
WAN KHUDRI
M0198088

dibimbing oleh

Pembimbing I,	Pembimbing II,
Dr. Sutanto, DEA.	Drs. Sutrima, M.Si.
NIP. 132 149 079	NIP. 132 046 018

telah dipertahankan di depan Dewan Penguji
pada hari Jum'at, tanggal 15 April 2005
dan dinyatakan telah memenuhi syarat.

Anggota Tim Penguji	Tanda Tangan
1. Drs. Bambang Harjito, M.App.Sc. NIP. 131 947 765	1.
2. Sri Kuntari, M.Si. NIP. 132 240 173	2.
3. Dewi Retno SS, M.Kom. NIP. 132 163 902	3.

Surakarta, 15 April 2005

Disahkan oleh
Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Sebelas Maret

Dekan,	Ketua Jurusan Matematika,
Drs. Marsusi, M.S.	Drs. Kartiko, M.Si.
NIP. 130 906 776	NIP. 131 569 203

ABSTRAK

Wan Khudri, 2005. ENKRIPSI DAN DEKRIPSI DATA MENGGUNAKAN ALGORITMA ElGamal ECC (*ElGamal ELLIPTIC CURVE CRYPTOGRAPHY*). Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Sebelas Maret.

Kriptografi adalah ilmu pengetahuan untuk menjaga keamanan informasi, termasuk didalamnya terdapat proses enkripsi dan dekripsi. Enkripsi adalah suatu proses untuk mengubah *plaintext* menjadi *chipertext* dan dekripsi adalah proses untuk mengembalikan *chipertext* menjadi *plaintext.* Algoritma yang digunakan dalam enkripsi dan dekripsi disebut algoritma kriptografi. Berdasarkan jenis kuncinya, algoritma kriptografi dibagi menjadi dua, yaitu algoritma simetri dan asimetri (*public key algorithm*). Tujuan penulisan skripsi ini adalah untuk menjelaskan salah satu jenis *public key algorithm*, yaitu algoritma ElGamal ECC (*ElGamal Elliptic Curve Cryptography*).

Metode yang digunakan dalam penulisan skripsi ini adalah studi literatur dan implementasi program. Melalui studi literatur, dipelajari teori-teori yang berhubungan dengan kriptografi kurva *elliptic*, khususnya ElGamal ECC. Kemudian membuat program implementasinya.

Kekuatan ElGamal ECC tergantung pada panjang kunci yang digunakan dalam proses enkripsi dan dekripsi serta pemilihan parameter-parameter domainnya. Parameter-parameter tersebut dipilih sehingga diperoleh order *basic point* yang terbesar. Algoritma ElGamal ECC membutuhkan waktu yang lebih lama dibandingkan dengan *public key algorithm* yang lain, terutama operasi perkalian skalar kurva *elliptic* dan representasi *plaintext* menjadi titik. Tetapi memiliki tingkat keamanan yang tinggi dengan panjang kunci terpendek.

ABSTRACT

Wan Khudri, 2005. ENCRYPTION AND DECRYPTION DATA USING ElGamal ECC ALGORITHM. Faculty of Mathematics and Natural Sciences, Sebelas Maret University.

Cryptography is a science to keep information security, includes encryption and decryption. Encryption is a process to change plaintext into chipertext and decryption is a process to rechange chipertext into plaintext. The algorithm which is used in encryption and decryption called cryptographic algorithm. Based on the type of key, cryptographic algorithm is divided into two types, they are symmetry algorithm and asymmetry algorithm (public key algorithm).The purpose of this project is to explain one of the type of public key algorithm, that is ElGamal ECC algorithm.

The method of this writing project is literature study and implementation programme. Through literature study, learned the theories which is relevant to elliptic curve cryptography, especially ElGamal ECC. Then made the implementation programme.

The strenght of ElGamal ECC depend on the length of key which is used in encryption and decryption and also selection of the domain parameters. The parameters selected so that obtained the biggest of order basic point. ElGamal ECC algorihm needs longer time than the other public key algorithm, especially elliptic curve scalar multiplication and representation plaintext into point. But it has a high security level with the shortest key length.

MOTO

" Di mana saja kamu berada, kematian akan mendapatkan kamu,
kendatipun kamu di dalam benteng yang tinggi lagi kokoh…… "
(Surat Annisaa'. Ayat 78)

" Dan Hadapkanlah mukamu kepada agama dengan tulus dan ikhlas …. "
(Surat Yunus. Ayat 105)

"Orang lain hanya dapat menunjukkan pintunya.
Aku sendiri yang harus melewatinya "
(Penulis)

KATA PENGANTAR

Alhamdulillah, puji syukur penulis panjatkan kehadirat Allah SWT yang telah melimpahkan rahmat, hidayah dan inayah-Nya sehingga penulis dapat menyelesaikan skripsi ini.

Dalam kesempatan ini penulis ingin menyampaikan terima kasih yang sebesar-besarnya kepada

1. Bapak Dr. Sutanto, DEA, sebagai Pembimbing I yang telah memberikan bimbingan, motivasi, kritik dan saran dalam penulisan skripsi ini.
2. Bapak Drs. Sutrima, M.Si, sebagai Pembimbing II yang telah memberikan bimbingan, motivasi, kritik dan saran dalam penulisan skripsi ini.
3. Bapak dan Ibu serta adik-adiku: Oji dan Tri, yang telah memberikan doa, perhatian, dukungan dan kasih sayangnya kepada penulis.
4. Bapak L. Yohanes Stefanus, PhD, yang telah memberikan bimbingan dan saran dalam penulisan skripsi.
5. Komunitas Fasilkom UI: Kharolin "Olin" Situmorang, Yusri "Bong" dan Wiratna, terima kasih atas saran, referensi dan diskusinya di dunia maya.
6. Mas Rosi, terima kasih atas referensi, saran dan bantuannya.
7. Hengky, Atie, Ina, Teh Im, Jantu, Diani, Aan, Tiis, Opix, Yaman, 2-Bagus, Yudo, terima kasih atas kebersaman dan persahabatannya selama ini. Kalian telah mendewasakanku dan memberikan warna dalam hidupku.
8. Ani "Ndutz", terima kasih atas bantuan dan fasilitas komputer dalam pengujian program skripsiku. Astri "Oecrit", thanks atas dukungannya.
9. Rahmat, Dawieg, Sableng, Si Doel, Retno, Ayiz, Memy, Dwi "Nanda", Heny "Manahan", Diana dan rekan-rekan Math '98, terima kasih atas bantuan dan kebersamaannya selama ini.
10. Yudhistira *Family*: Rahmat, Wahyu, Nunu, Hendrong, Yo2k, Odien, Henry, Boy, terima kasih atas bantuan, dukungan dan ketentraman yang diberikan.
11. Semua pihak yang telah membantu terselesaikannya penulisan skripsi ini.

Surakarta, Maret 2005

Penulis

DAFTAR ISI

Halaman

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR ALGORITMA

Halaman

DAFTAR LAMPIRAN

Halaman

DAFTAR NOTASI DAN SIMBOL

$\mathbb{R}$: Himpunan bilangan real

p : Bilangan prima

F_p : Lapangan berhingga prima, F_p = { 0,1,2,3,…, p-1 }

F_2^m : Lapangan karakteristik 2

A, B : Koefisien persamaan kurva *elliptic* $y^2 = x^3 + Ax + B \ (mod\ p)$

$E(A,B)$: Persamaan kurva *elliptic* $y^2 = x^3 + Ax + B \ (mod\ p)$

$E_p(A,B)$: Grup *Elliptic* atas F_p

$\boldsymbol{O}$: *Point at infinity* (identitas grup *elliptic*)

QR_p : Himpunan *quadratic residue modulo p*

Δ : Gradien garis antara dua titik kurva *elliptic*

$\#E$: Banyaknya titik kurva *elliptic*

ε : Banyaknya percobaan representasi titik

G_E : *Basic point* (elemen pembangun grup *elliptic* $E_p(A,B)$)

N_G : Order dari *basic point*

h : Kofaktor. $h = \#E / N_G$

T : Parameter-parameter domain kurva *elliptic*.
$T = (p,A,B,G_E,N_G,h)$

P_M : Representasi titik kurva *elliptic* dari *plaintext*

P_C : *Chipertext pair of point*

V : *Private key*

β : *Public key*

BAB I
PENDAHULUAN

1.1. Latar Belakang

Dunia semakin canggih dan teknologi informasi semakin berkembang. Perkembangan tersebut secara langsung maupun tidak langsung mempengaruhi sistem perdagangan, transaksi dan sistem informasi selama ini. Terutama di era internet ini, semua informasi terkirim dengan bebas melalui suatu jaringan dengan tingkat keamanan yang relatif rendah. Untuk itulah peranan teknologi keamanan informasi benar-benar dibutuhkan. Keamanan informasi *(information security)* merupakan bagian yang sangat penting dari sebuah sistem dalam jaringan komputer terutama yang terhubung dengan internet. Sebuah sistem yang mempermudah dan memanjakan pengguna tidak akan berguna tanpa didukung oleh sistem keamanan yang tinggi. Oleh karena itu, informasi atau data rahasia yang akan dikirim harus disandikan agar tidak dapat dibaca oleh orang lain.

Teknik untuk mengubah informasi yang dapat dibaca/teks asli *(plaintext)* menjadi kode-kode tertentu disebut sebagai enkripsi *(encryption)* dan hasilnya disebut *chipertext*. Sedangkan teknik untuk mengubah *chipertext* menjadi *plaintext* disebut dekripsi *(decryption)*. Algoritma yang digunakan untuk proses enkripsi dan dekripsi adalah algoritma kriptografi *(cryptographic algorithm)* atau sering disebut *chiper*. Algoritma kriptografi ini bekerja dengan menggunakan kunci *(key)* seperti kata, nomor maupun frase tetentu. Jika dilakukan enkripsi pada *plaintext* yang sama dengan menggunakan kunci yang berbeda, maka akan menjadi *chipertext* yang berbeda [11].

Menurut Menezes *et al.* [10], Doraiswamy *et al*. [6] dan Kurniawan [9], kriptografi *(cryptography)* adalah seni dan ilmu pengetahuan untuk menjaga keamanan informasi. Orangnya disebut sebagai *cryptographer*. Kebalikan dari kriptografi adalah *cryptanalysis,* yaitu seni dan ilmu untuk memecahkan *chipertext* menjadi *plaintext* tanpa melalui cara yang seharusnya. Orangnya disebut sebagai *cryptanalyst.*

Berdasarkan jenis kuncinya, algoritma kriptografi dapat dibagi menjadi

dua kelompok yaitu algoritma simetri (konvensional / *private key algorithm*) dan algoritma asimetri *(public key algorithm)*. Menurut Kurniawan [9], algoritma simetri adalah algoritma yang menggunakan kunci enkripsi yang sama dengan kunci dekripsinya. Pada algoritma ini, pengirim dan penerima harus menyetujui suatu kunci tertentu yang dinamakan kunci rahasia *(secret key)*. Contohnya adalah *DES (Data Encryption Standard), Rijndael, Blowfish* dan lain-lain. Sedangkan algoritma asimetri didesain sedemikian sehingga kunci yang digunakan untuk enkripsi berbeda dengan kunci untuk dekripsi. Kunci yang digunakan untuk enkripsi disebut kunci publik *(public key)* dan dapat diketahui oleh orang lain. Sedangkan kunci untuk dekripsi dinamakan kunci rahasia atau sering disebut sebagai *private key* dan hanya diketahui oleh pemiliknya. Contohnya adalah ElGamal, RSA *(Rivest-Shamir-Adleman),* ECC *(Elliptic Curve Cryptography)* dan lain-lain.

Istilah "kunci rahasia" pada algoritma simetri digunakan untuk menyatakan kunci enkripsi sekaligus kunci dekripsi dan disebut *secret key*. Sedangkan pada algoritma asimetri, kunci rahasia hanya digunakan untuk menyatakan kunci dekripsi dan sering disebut sebagai *private key*. Hal ini dapat mengakibatkan kesalahan penafsiran pada istilah "kunci rahasia". Karena itu, untuk pernyataan-pernyataan berikutnya digunakan istilah aslinya.

Menurut Purbo dan Wahyudi [11], saat ini terdapat tiga macam *public key algorithm* yang aman dan efisien berdasarkan permasalahan matematis, yaitu *Integer Factorization Problem* (IFP)*, Discrete Logarithm Problem* (DLP) dan *Elliptic Curve Discrete Logarithm Problem*(ECDLP).

Jika diberikan bilangan bulat n yang merupakan hasil kali dua buah bilangan prima p dan q sehingga $n=p.q,$ maka permasalahan matematis dalam IFP adalah mencari faktor dari n , yaitu p dan q. Contohnya adalah RSA.

DLP merupakan masalah yang didefinisikan pada aritmetika modular. Misalkan dipilih bilangan prima p dan diberikan bilangan bulat g ($0<g<p-1$) serta y merupakan pemangkatan dari g, sehingga $y=g^x \pmod p$. Permasalahan matematis dalam DLP adalah mencari $x,$ jika diberikan pasangan bilangan g dan y. Contohnya adalah ElGamal, Diffie-Hellman, DSA (*Disgital Signature Algorithm*).

Jika F_p himpunan lapangan berhingga (*finite field*) , p bilangan prima, $P(x_P,y_P)$ titik pada kurva elliptik, dipilih V secara random sehingga $Q=V.P$. Permasalahan matematis dalam ECDLP adalah mencari V, jika diketahui titik P dan Q**.** Contohnya adalah ElGamal ECC (*ElGamal Elliptic Curve Cryptography*), ECDSA (*Elliptic Curve Digital Signature Algorithm*).

Algoritma ECC menggunakan ECDLP dan dikenalkan pertama kali oleh Koblitz dan Miller pada tahun 1985. ECC dapat digunakan untuk beberapa keperluan seperti skema enkripsi (contohnya ElGamal ECC), tanda tangan digital (contohnya ECDSA) dan protokol pertukaran kunci (contohnya Diffie Hellman ECC). Salah satu hal yang menarik mengenai ECC terletak pada tingkat keamanannya. ECC dapat menggunakan ukuran kunci yang lebih kecil dibandingkan dengan kriptografi lainnya dan memiliki tingkat keamanan yang sama. Kemampuan ini membuat ECC mempunyai keamanan yang terkuat dengan panjang kunci terpendek. Sebagai perbandingan, 160 bit ECC mempunyai tingkat keamanan yang sama dengan 1024 bit RSA atau DSA dan 224 bit ECC memiliki tingkat keamanan yang sama dengan 2048 bit RSA atau DSA [6,9,11].

Kemampuan dan keamanan ECC ini yang membuat penulis tertarik untuk mengkaji lebih dalam tentang salah satu skema enkripsinya, yaitu ElGamal ECC (*ElGamal Elliptic Curve Cryptography*) dan membuat program aplikasinya.

1.2. Perumusan Masalah

Berdasarkan latar belakang masalah, rumusan masalah dalam penulisan skripsi ini adalah

1. Bagaimana menentukan *private key* dan *public key* algoritma ElGamal ECC ?
2. Bagaimana menentukan proses enkripsi dan dekripsi menggunakan algoritma ElGamal ECC ?
3. Bagaimana membuat program aplikasi komputer yang dapat melakukan enkripsi dan dekripsi berdasarkan algoritma ElGamal ECC ?

1.3. Batasan Masalah

Batasan masalah dalam penulisan skripsi ini adalah

1. Persamaan kurva *elliptic* yang digunakan dalam implementasi adalah $y^2 = x^3 + Ax + B \pmod{p}$ pada lapangan berhingga prima F_p .
2. Selama proses pengiriman sandi, tidak ada gangguan pada saluran informasi.

1.4. Tujuan

Tujuan yang ingin dicapai dalam penulisan skripsi ini adalah

1. Dapat menentukan *private key* dan *public key* algoritma ElGamal ECC.
2. Dapat menentukan proses enkripsi dan dekripsi menggunakan algoritma ElGamal ECC.
3. Dapat membuat program aplikasi komputer yang dapat melakukan enkripsi dan dekripsi berdasarkan algoritma ElGamal ECC.

1.5. Manfaat

Manfaat yang diharapkan dalam penulisan skripsi ini adalah

1. Manfaat teoritis

   Secara teoritis manfaat yang diperoleh dari penulisan skripsi ini adalah dapat memahami proses enkripsi dan dekripsi menggunakan algoritma ElGamal ECC (*ElGamal Elliptic Curve Cryptography*).

2. Manfaat praktis

   Manfaat praktis dari hasil penulisan skripsi ini adalah dapat mengetahui, mempermudah dan mempercepat proses enkripsi dan dekripsi ElGamal ECC menggunakan program komputer. Aplikasinya dapat dikembangkan dalam berbagai bidang, yaitu transaksi *online*, *internet banking*, tanda tangan digital (*digital signature*) dan lain sebagainya.