Studi dan Implementasi Algoritma *Elliptic Curve* pada *Mobile Devices*

Jonathan Marcel (13507072)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl Ganesha 10 Bandung 4013, Indonesia
cel_tum@yahoo.co.id

ABSTRAK

Sejak Diffie-Hellman memperkenalkan algoritma kriptografi kunci publik pada tahun 1976, banyak yang mempercayai bahwa algoritma ini dapat menggantikan kriptografi kunci simetri karena memiliki keunggulan komputas yang lebih baik. Sejak saat itu implementasi kriptografi kunci publik semakin meluas pada berbagai bidang.
Penggunaan mobile device seperti telepon genggam dan ponsel pintar sudah sangat meluas di masyarakat. Berbagai macam informasi dengan mudah dapat berpindah dari satu tangan ke tangan lainnya. Adakalanya informasi tersebut dapat disadap oleh orang lain dan dicuri oleh orang lain, sehingga masyarakat membutuhkan sistem pengamanan pada setiap mobile device yang dimilikinya.
Salah satu sistem pengamanan yang dapat dimanfaatkan ialah sistem kriptografi *Elliptic Curve*. Sistem ini berdasarkan pada permasalahan logaritma diskrit pada bidang berhingga, dalam hal ini ialah titik pada kurva eliptik diatas bidang berhingga. Hal ini dipilih untuk pengamanan mobile device karena algoritma ini menyebabkan panjang kunci yang sangat minimal tetapi menawarkan keamanan yang sangat baik. Sistem inilah yang akan dibahas pada makalah ini.

KATA KUNCI: Kriptografi Kunci Publik, Mobile Devices, Algoritma Kriptografi Elliptic Curve

PENDAHULUAN

Kriptografi adalah ilmu dan seni yang mempelajari bagaimana mengamankan pesan dari orang yang tidak diinginkan. Pada prinsipnya ada dua proses kriptografi, yaitu enkripsi yaitu mengubah plainteks menjadi cipherteks, dan dekripsi yaitu kebalikannya yaitu mengubah cipherteks menjadi plainteks.

Di dalam kriptografi dikenal istilah kunci, yaitu suatu representasi karakter ataupun angka yang dapat digunakan untuk mengenkripsikan dan mendekripsikan pesan.
Kriptografi terus berkembang hingga saat ini, dan seiring dengan perkembangan ilmu kriptografi, penggunaan kriptografi semakin meluas untuk pengamanan bukan hanya pesan saja, tetapi data-data yang tersimpan di dalam komputer.
Kriptografi kunci publik diharapkan dapat menggantikan kriptografi simetri karena memiliki kepraktisan yaitu cukup mengingat sebuah kunci saja, dalam hal ini ialah kunci dekripsi.
Salah satu algoritma kriptografi kunci publik yang terkenal ialah Elliptic Curve. Algoritma ini berdasarkan pada fakta bahwa sangat sukar untuk memecahkan persoalan logaritma diskrit pada kurva eliptik di bidang berhingga. Selain itu, algoritma ini dianggap sangat efisien dan tidak membutuhkan ruang memori yang besar, sehingga dapat diimplementasikan ke dalam berbagai mobile device.
Seperti yang kita ketahui bahwa mobile device memiliki kemampuan pemrosesan yang sangat terbatas dan daya hidup yang terbatas, oleh karena itu sistem kriptografi Elliptic Curve sangatlah cocok untuk lingkungan *hardware* tersebut.

DASAR TEORI

Algoritma Kriptografi Kunci Publik
Algoritma kriptografi kunci publik disebut juga dengan algoritma kriptografi asimetri. Apabila algoritma kriptografi simetri menggunakan kunci enkripsi dan dekripsi yang sama, maka algoritma kriptografi kunci publik menggunakan sepasang kunci, satu untuk enkripsi dan satu untuk dekripsi.

Pada algoritma kriptografi kunci publik, kunci untuk enkripsi diumumkan kepada publik, oleh karena itu tidak rahasia, sehingga dinamakan kunci publik. Sedangkan kunci untuk dekripsi bersifat rahasia sehingga dinamakan kunci privat.

Sistem kriptografi kunci publik didasarkan pada fakta bahwa:

1. Komputasi untuk enkripsi/dekripsi pesan mudah dilakukan
2. Secara komputasi hampir tidak mungkin menurunkan kunci privat bila diketahui kunci publik pasangannya

Kelebihan kriptografi kunci publik antara lain:

1. Hanya kunci privat yang perlu dijaga kerahasiaannya oleh setiap entitas yang berkomunikasi
2. Pasangan kunci publik/kunci privat tidak perlu diubah, bahkan dalam periode waktu yang panjang
3. Dapat digunakan untuk mengamankan pengiriman kunci simetri
4. Beberapa algoritma kunci-publik dapat digunakan untuk memberi tanda tangan digital pada pesan

Sedangkan kelemahan kriptografi kunci-publik antara lain:

1. Enkripsi dan dekripsi data umumnya lebih lambat daripada sistem simetri, karena enkripsi dan dekripsi menggunakan bilangan yang besar dan melibatkan operasi perpangkatan yang besar
2. Ukuran cipherteks lebih besar daripada plainteks
3. Ukuran kunci relatif lebih besar daripada ukuran kunci simetri
4. Karena kunci publik diketahui secara luas dan dapat digunakan setiap orang, maka cipherteks tidak memberikan informasi mengenai otentikasi pengirim
5. Tidak ada algoritma kunci-publik yang terbukti aman

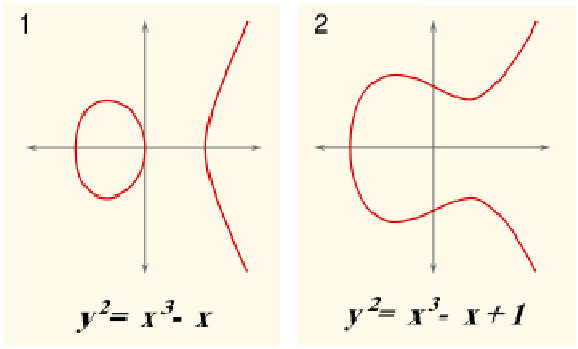
Kurva Eliptik

Dalam bidang matematika, kurva eliptik adalah kurva halus, merupakan kurva aljabar proyektif dari genus satu, dimana terdapat titik O. Faktanya, kurva eliptik ini ialah sebuah varietas abelian – yaitu memiliki sebuah perkalian yang terdefinisikan secara aljabar dalam sebuah grupnya, dan titik O berfungsi sebagai elemen identitas. Bahkan kurva tanpa titik O tersebut juga disebut kurva eliptik.

Dengan menggunakan teori fungsi eliptik, dapat ditunjukkan bahwa kurva eliptik terdefinisikan diatas bilangan kompleks yang berkorespondensi untuk menggabungkan torus dengan bidang proyektif kompleks. Torus ini juga merupakan varietas abelian, dan penggabungan ini juga merupakan grup *isomorphism*.

Penggunaan kurva eliptik sangatlah penting dalam teori bilangan, dan memiliki peran di dalam berbagai penelitian saat ini. Sebagai contoh, teori kurva eliptik digunakan untuk membuktikan teori terakhir Fermat oleh Andrew Wiles, selain itu juga dimanfaatkan untuk keperluan kriptografi (seperti yang dibahas dalam makalah ini), kemudian faktorisasi integral.

Perlu diingat bahwa kurva eliptik bukanlah elips.



Algoritma Elliptic Curve

Algoritma Elliptic Curve merupakan salah satu algoritma kriptografi kunci publik. Algoritma ini berbasiskan pada struktur aljabar dari kurva eliptik diatas bidang yang terbatas. Ide algoritma ini berawal dari pemikiran Neal Koblitz dan Victor S Miller pada tahun 1985.

Algoritma kunci publik lainnya misalnya algoritma RSA. Kesukaran memecahkan algoritma RSA ialah sulitnya memfaktorkan bilangan integer berukuran besar yang terdiri atas dua atau lebih faktor prima. Sedangkan pada algoritma Elliptic Curve, diasumsikan bahwa menemukan logaritma diskrit dari sebuah elemen kurva eliptik sembarang sangatlah tidak mungkin.

Penelitian membuktikan bahwa keamanan yang diberikan oleh sistem berbasis RSA dengan bilangan modulus yang besar adalah sama dengan keamanan yang diberikan oleh sistem Elliptic Curve dengan kurva

eliptik berukuran kecil. Atas dasar inilah algoritma Elliptic Curve dianggap lebih mangkus karena menggunakan ruang memori dan transmisi yang lebih kecil dibandingkan RSA.

Untuk keperluan kriptografi, sebuah kurva eliptik ialah kurva bidang datar yang terdiri atas titik-titik dan memenuhi persamaan:

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

Mobile Device

Mobile Device, atau disebut juga perangkat mobile, adalah devais komputasi yang berukuran kecil, biasanya memiliki sebuah layar tampilan dengan input sentuhan ataupun keyboard mini. Beberapa mobile device yang sangat populer antara lain smartphone, atau disebut juga ponsel pintar dan PDA (Personal Digital Assistant).

Perangkat-perangkat yang termasuk di dalam mobile device antara lain:

- Mobile computer, termasuk laptop, netbook, tablet PC, dan ultra mobile PC
- Personal digital assistant/enterprise digital assistant, termasuk perangkat ponsel pintar
- Graphing calculator
- Handheld game consoles, misalnya Nintendo Game Boy, Nintendo DS, Sony Playstation Portable (PSP)
- Digital still camera
- Digital video camera/digital camcorder
- Portable media player
- E-book reader
- Pager
- Personal navigation devices

Permasalahan Logaritma Diskrit (PLD) pada Kurva Eliptik

Permasalahan inilah yang menyebabkan diciptakannya algoritma kriptografi Elliptic Curve. Diberikan sebuah kurva eliptik E di bidang terhingga GF(p) dan group pertambahan siklik G = E(F_q) yang selalu ditambahkan modulo p. Maka permasalahan PLD ialah sebagai berikut:

Diberikan P ∈ G dan elemen Q ∈ <P>, temukan bilangan integer m, sehingga Q = [m]P[12]

IMPLEMENTASI ALGORITMA *ELLIPTIC CURVE*

Sebelum diimplementasikan, pertama-tama harus ditentukan karakteristik bidang ganjil atau genap, dan juga bagaimana merepresentasikan titik-titik pada kurva eliptik. Penentuan ini akan berakibat pada kecepatan komputasi.

Menentukan karakteristik bidang

Ada dua buah karakteristik yaitu genap dan ganjil.Karakteristik ganjil misalnya pada bidang GF(p) dimana p adalah bilangan bilangan prima besar. Sedangkan pada bidang GF(2^m) adalah karakteristik ganjil.

Ada 4 macam operasi pada GF(2^m) yaitu, penjumlahan yang dilakukan dengan operasi bitwise XOR, perkalian, perpangkatan kuadrat, dan pembagian.

Ada beberapa alasan kenapa karakteristik genap lebih dipilih dibandingkan karakteristik ganjil. Pertama-tama, jumlah elemen dari karakteristik genap direpresentasikan sebagai bit-string dengan panjang m. Hal ini memudahkan implementasi pada hardware. Selain itu operasi perpangkatan juga lebih mudah dengan operasi rotasi sederhana dari elemen vektor. Faktor terakhir juga ialah lebih mudah didesain dengan bit serial multiplier yang efisien.

Representasi Titik-Titik

Ada dua macam representasi titik yang akan didiskusikan, yaitu affine dan koordinat proyektif. Kita akan menggunakan formula dari penjumlahan titik di dalam bidang prima (karakteristik ganjil) untuk mengilustrasikan berbagai *cost* di dalam memperhitungkan aritmatika titik pada dua macam representasi tersebut.

Koordinat affine dijabarkan dalam persamaan berikut:

$$y^2 = x^3 + axz^2 + bz^3$$

Dimana a dan b merupakan elemen GF(p)

Sedangkan koordinat proyektif dijabarkan dalam persamaan Weierstrass berikut:

Dimana a dan b merupakan elemen F_p. Ketika $z \neq 0$, titik proyektif akan berkorespondensi dengan titik affine. Dengan koordinat proyektif, operasi inversi akan digantikan dengan perkalian. Koordinat proyektif akan lebih efisien ketika diimplementasikan pada grup operasi [12].

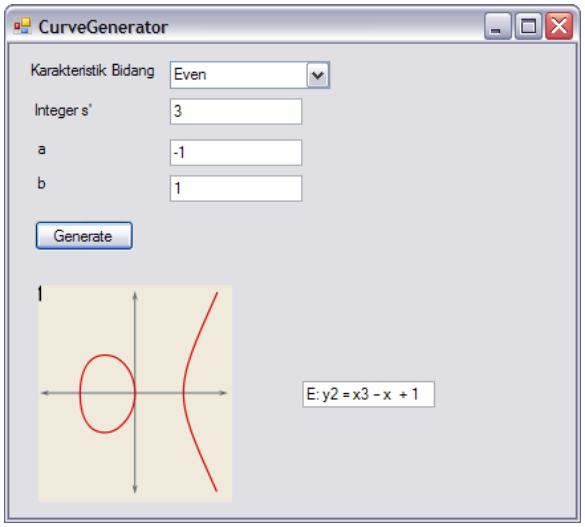
Pemilihan kurva

Metode yang paling baik untuk meng-*generate* kurva yang baik adalah secara acak. Kurva yang dibangkitkan secara acak adalah kurva dengan koefisien yang diambil dari output dari generator bilangan acak. Berikut ini merupakan salah satu algoritma untuk memilih kurva pada bidang F_P[12].

```
Input: Bidang F_P dan bilangan integer positif kecil s'
Output: kurva eliptik E pada bidang F_P sehingga E(F_P) = s.r, s<=s' dan r prima
Boolean b = true
While(b){
Gambar E acak dengan koefisien pada F_P
Hitung order E, #E(F_P)
Cek MOV dan kondisi anomalous.
Berusaha untuk memfaktorkan #E(F_P) dalam waktu yang reasonable
If(#E(F_P) = s.r, s<=s', dan r prima) then return E
Else(b = false)
}
```

Langkah terakhir bertujuan untuk memastikan bahwa $\#E(F_P)$ memiliki faktor prima yang besar. Hal ini dilakukan untuk menghindari serangan Pohlig-Hellman. Jadi, bagaimana konfigurasi Elliptic Curve Cryptosystem pada mobile device?
Parameter sistemnya ialah suatu bidang berhingga F, koefisien kurva eliptik E, dan sebuah titik di kurva E yang disebut generator G, serta ord(G).
Kunci publik ialah sebuah titik pada kurva P = kG, untuk k yang dirahasiakan.

Sedangkan kunci privat ialah bilangan integer k, dimana 0<k<q, q = ord(P). Kunci privat ini merupakan bilangan integer k yang diambil secara acak.
Kriptografi Elliptic Curve dapat digunakan untuk sekelompok user mobile device, dimana setiap user akan memiliki sebuah pasangan kunci publik dan kunci privat.
Berikut adalah tampilan program sederhana pemilihan kurva eliptik.



Beberapa pertimbangan dalam pemilihan bidang berhingga dan kurva eliptik antara lain:

Pemilihan Panjang Kunci
Setiap kurva dipilih sehingga memiliki kofaktor 1, 2, atau 4. Hal ini digunakan untuk memastikan tercapainya efisiensi dalam komputasi. Sehingga, kunci publik dan kunci privat akan memiliki panjang kira-kira bit blok-18.

Pemilihan Bidang
Setiap bidang dipilih sehingga panjang dari urutan bit paling kurang dua kali lipat panjang kunci privat pada blok cipher. Hal ini dilakukan karena metode exhaustive search pada k-bit blok cipher diharapkan memiliki waktu komputasi yang sama dengan solusi pada Elliptic Curve apabila kita menggunakan algoritma Pollard untuk kurva eliptik pada bidang berhingga dengan urutan panjang 2k[20].

Pemilihan p pada GF(p) dan m pada $GF(2^m)$
Untuk bidang biner $GF(2^m)$ m dipilih sehingga terdapat kurva Kolbitz hampir prima pada bidang $GF(2^m)$.

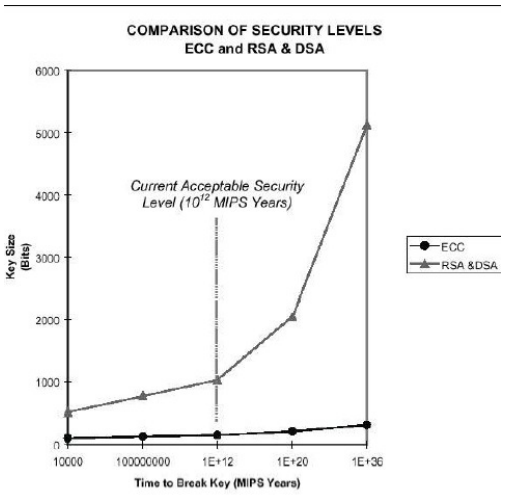
Koefisien dari kurva eliptik
Kurva yang dipilih ialah yang memenuhi persamaan:

Dimana nilai a = -3

ANALISIS

Keunggulan sistem kriptografi Elliptic Curve

Pada tahun 2002, kunci enkripsi sepanjang 109 bit dengan sistem kriptografi Elliptic Curve yang menggunakan kurva lemah dapat dipecahkan oleh 10000 buah komputer yang dijalankan 24 jam sehari selama 549 hari. Penelitian menunjukkan bahwa untuk memecahkan kunci sepanjang 163 bit dengan kurva eliptik yang baik memerlukan waktu ratusan juta kali lipat lebih lama dibandingkan pemecahan sebelumnya. Fakta ini menunjukkan betapa tingginya sekuritas sistem kriptografi Elliptic Curve.
Perbedaan yang sangat mendasar dari sistem kriptografi Elliptic Curve dengan algoritma lainnya seperti RSA ialah dengan pemilihan kurva eliptik yang tepat maka pemecahan persoalan logaritma diskrit pada kurva eliptik dapat diselesaikan dengan metode eksponensial. Hal ini berbeda dengan sistem kriptografi biasa yang diselesaikan dengan metode sub-eksponensial. Hal ini mengakibatkan waktu untuk menyelesaikan perhitungan dengan kriptografi Elliptic Curve lebih singkat. Akibatnya juga panjang kunci pada algoritma Elliptic Curve lebih pendek dibandingkan pendekatan lainnya seperti RSA. Hal ini dapat dilihat pada grafik berikut:



Grafik tersebut diambil dari referensi [1].

Algoritma Elliptic Curve sudah diimplementasikan ke berbagai mobile devices, antara lain:

Internet
Algoritma ini mulai diimplementasikan oleh SUN Microsystem untuk digunakan pada OpenSSL. OpenSSL adalah kakas untuk pengembangan protokol Secure Socket Layer dan protokol Transport Layer Security.

Smart Cards
Smart Cards adalah salah satu devais terpopuler yang mengimplementasikan sistem kriptografi Elliptic Curve. Penggunaan kriptografi ini biasanya untuk pengimplementasian tandatangan digital. Perusahaan yang mengimplementasikannya antara lain Fujitsu dan DataKey. Smart Card ini dapat digunakan untuk kartu kredit atau kartu debit, tiket elektronik, dan kartu identitas.

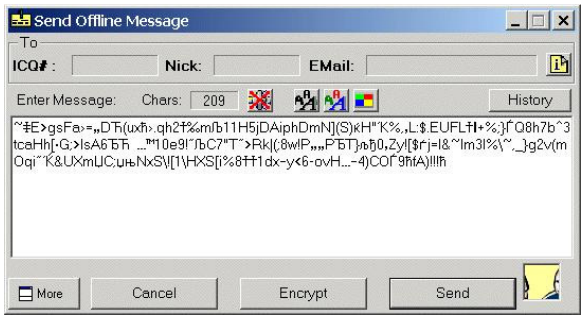
Personal Digital Assistant (PDA)
PDA merupakan devais yang sangat cocok untuk diimplementasikan sistem kriptografi Elliptic Curve karena memiliki kemampuan komputasi yang lebih baik dibandingkan mobile device lainnya.

PC (Personal Computer)
Beberapa perusahaan telah mengimplementasikan sistem kriptografi Elliptic Curve kepada komputer antara lain untuk pengamanan data, enkripsi surat elektronik, bahkan enkripsi pesan instan. Salah satu perusahaan komputer yang menggunakan sistem ini

ialah PC Guardian Technologies. Sebelumnya perusahaan ini menggunakan algoritma RSA dan Diffie-Hellman, tetapi sekarang telah menggunakan kriptografi Elliptic Curve untuk pengamanan email.

Selain itu juga terdapat aplikasi Top Secret Messenger yang mengimplementasikan sistem kriptografi Elliptic Curve untuk mengenkripsi pesan instant pada Yahoo client dan MSN client. Selain itu juga bisa untuk mengenkripsi e-mail client seperti Microsoft Outlook dan Outlook Express.

Dibawah ini merupakan tampilan program Top Secret Messenger.



KESIMPULAN

1. Algoritma Elliptic Curve merupakan salah satu algoritma kriptografi kunci publik
2. Algoritma Elliptic Curve dibuat berdasarkan kesukaran persoalan logaritma diskrit pada kurva eliptik
3. Ada beberapa pertimbangan yang diperlukan untuk membuat algoritma Elliptic Curve yang mangkus, antara lain pemilihan panjang kunci dan pemilihan bidang berhingga.
4. Semakin panjang kunci maka akan semakin tinggi sekuritas algoritma tersebut.
5. Dibandingkan algoritma kriptografi kunci publik lainnya, algoritma Elliptic Curve memiliki keunggulan dalam waktu komputasi serta sekuritas.
6. Algoritma Elliptic Curve sudah diimplementasikan untuk pengamanan data ke dalam berbagai mobile devices, seperti PDA dan komputer.

REFERENSI

[1]Wendy Chou, *Elliptic Curve Cryptography*, University of Maryland

[2]Andre Weimerskirch, *Elliptic Curve Cryptography on a Palm OS*, 2001

[3]M. Aydos, *An Elliptic Curve Cryptography based Authentication and Key Agreement Protocol for Wireless Communication*, Oregon State University

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, 16 Mei 2010

Jonathan Marcel 13507072