Studi dan Analisis Elliptic Curve Cryptography

Kevin Tirtawinata – 135 07 097
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
kevin.tirtawinata@gmail.com

Abstrak – Makalah ini akan membahas tentang salah satu pendekatan kriptografi dengan sekumpulan algoritma tertentu untuk melakukan proses enkripsi dan juga dekripsi sebuah pesan dengan sistem kriptografi kunci asimtrik yang dikenal dengan seebutan Elliptic Curve Cryptography. Elliptic Curve Cryptography diyakini merupakan salah satu algoritma kriptografi yang mampu melakukan enkripsi dan dekripsi yang memiliki tingkat keeamanan yang jauh lebih baik dibandingkan dengan algoritma – algoritma lain yang sama-sama menggunakan kunci asimetrik. Walaupun masih merupakan suatu algoritma yang berbentuk pendekatan Elliptic Curve Cryptography sudah terbukti lebih baik dibanding pendekatan lain secara matematikal.

1. PENDAHULUAN

Sudah sejak lama informasi menjadi salah satu aspek penting dalam kehidupan ini. Walaupun teknik komunikasi berkembang, namun tidak ada salah satu alat komunikasi jarak jauh yang aman untuk mengirimkan suatu informasi yang pentin atau dirahasiakan. Segala pihak dari berbagai lingkup kehidupan sangat membutuhkan keamanan informasi, di saat informasi tersebut adalah informasi yang menjadi sebuah rahasia, yang tidak boleh diketahui oleh pihak lain. Untuk mengamankan informasi yang sifatnya rahasia, dikembangkan salah satu cabang ilmu pengetahuan yang bernama kriptografi.

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya, begitulah dahulu kriptografi muncul pada saat informasi yang perlu dijaga hanyalah sebatas pesan. Seiiring berkembangnya teknologi informasi kripografi berkembang sehingga ia tidak lagi sebatas mengenkripsi pesan tetapi juga memberikan aspek keamanan untuk berbagai jenis informasi yang ada.

Di sisi lain, dikembangkan juga salah satu ilmu lain, yaitu kriptanalisis, yang merupakan ilmu dan seni untuk memecahkan cipherteks menjadi plainteks tanpa mengetahui kunci yang diberikan, pelaku dari kriptanalisis, disebut kriptanalis. Dengan adanya kriptanalisis, maka kebutuhan akan amannya pesan meningkat dan kriptografi pun harus menggunakan algoritma-algoritma baru yang tidak mudah dipecahkan.

Untuk hal tersebuatlah kriptografi, sebuah cabang imu yang bertujuan untuk mengamanakan data dipelajari dan diterapkan dalam dunia komputer dan telekomunikasi aga data yang ada aman dan juga valid baik untuk pengirim dan penerima data.

Berbagai jenis teknik pengenkripsian pesan sudah ada dan beberapa sudah dapat dipecahkan. Selama masih ada orang yang mnginginkan data orang lain, keamanan data pada jaringan internet tidaklah aman sehingga dibutuhkan sistem kriptografi yang dapat diandalkan.

Sistem kriptografi yang umumnya digunakan sebagai pengamanan pada pengiriman data terutama yang berguna untuk menjaga keaslian data yang digunakan adaah kriptografi dengan kunci asimetrik. Penggunaan kunci kriptografi asimetrik memiliki kekuatan bergantung pada panjangnya kunci dan pendekatan algoritma yang digunakan. Semakin panjang kunci yang digunakan, semakin aman data yang dikirim dan dengan semakin rumit algoritma yang digunakan maka hasil enkripsi data yang ada juga sangatlah aman atau dengan kata lain teknik kriptografi tersebut memiliki kekuatan yang memadai untuk digunakan dalam menjamin kebenaran dari data yang dikomunikasikan pada jaringan internet.

2. LANDASAN TEORI

2.1 Elliptic Curve Cryptography

Pendekatan yang dilakukan untuk menhasilkan algoritma Elliptic Curve Cryptography adalah dengan meggunakan struktur matematika yang sangat unik yang memungkinkan pemrosesan titik dengan memiliki dua buah titik dalam sebuah kurva eliptik dan menghasilkan sebuah titik lain yang ada pada kurva tersebut. Struktur yang nik ini memberikan

keuntungan dalam kriptografi dikarenakan kesulitan untuk menemukan 2 buah titik yang menentukan sebuah titik tertentu tersebut tidak dapat ditemukan dengan mudah. Tingkat kesulitan untuk menemukan 2 buah titik termasuk dalam golongan yang rumit sama seperti kesulitan untuk memperhitungkan variasi eksponensial yang digunakan dalam algoritma RSA yang telah banyak diimplementasikan. Untuk memecahkan Elliptic Curve Cryptography sendiri dibutuhkan perhitungan matematis yang sangat tinggi.

Elliptic Curve Cryptography terdiri dari beberapa operasi basic dan juga aturan yang mendefinisikan penggunaan dari operasi operasi basic seeperti penambahan, pengurangan, perkalian dan perpangkatan yang didefinisikan sesuai dengan kurva-kurva yang ada.

2.2 Dasar Matematika pada Elliptic Curve Cryptography

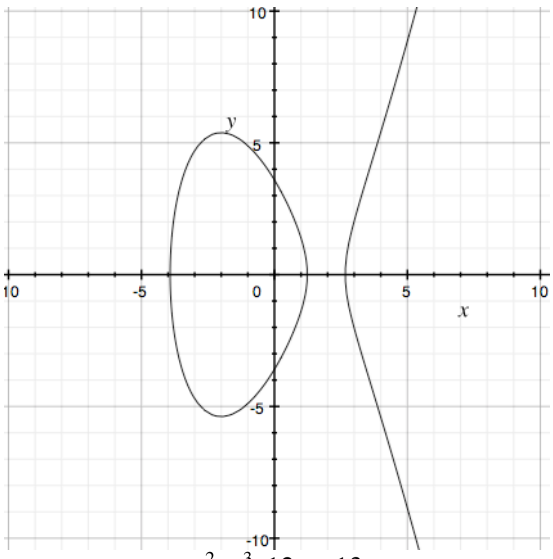
Operasi matematika yang digunakan pada Elliptic Curve Cryptography didefinisikan dngan persamaan

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

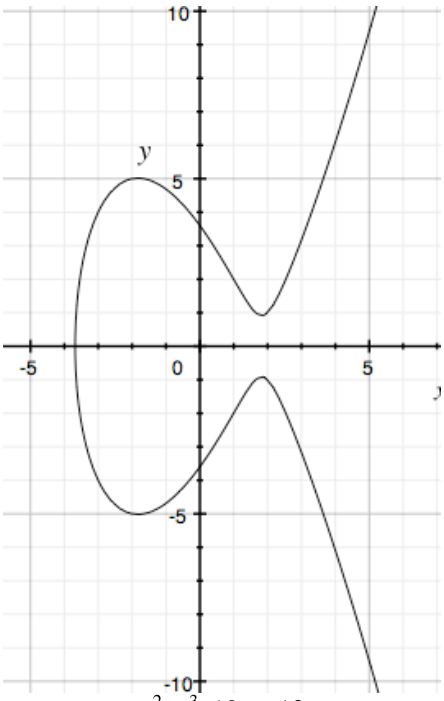
dengan

$$4a^3+27b^2 \neq 0$$

Setiap prubahan nilai dari ‘a’ dan’b’ akan menghasilkan elliptic curve yang berbeda. Contoh Elliptic Curve



$y^2=x^3-12x+13$



$y^2=x^3-10x+13$

Setiap kurva liptik akan mendefinisikan kumpulan titik pada bidang dan dapat membentuk kumpulan albelian (kumpulan titik dangan titik tak hingga sebagai elemen identitas). Jika nilai x dan y yang dipilih adalah daerah finit yang besar, solusi akan menghasilkan suatu albelian finite.

Kurva ellips yang digunakan dalam Elliptic Curve Cryptography didefinsikan dengan dua buah bidang terbatas.

2.3 Bidang Terbatas (Finite Field)

Bidang terbatas (finite field) atau yang biasa disebut dengan Galois Field (GF) adalah bidang yang hanya memiliki elemen bilangan yang terbatas yang ditentukang dengan suatu pembatasan yang abstrak. Derajat atau sering disbuat juga dengan order dari sebuah finite field adalah banyaknya elemen yang ada di dalam bidang yang didefinisikan. Jika q adalah sebuah pangkat prima (prime power), maka hanya ada satu bidang terbatas dengan derajat q. Bidang tersebut dilambangkan dengan F_q atau GF(q). Banyak cara untuk merepresentasikan elemen dari F_q, jika $q=p^m$, dimana p adalah bilangan prima dan m adalah bilangan integer positif, maka p disebut sebagai karakteristik yang unik dari F_q dan m disebut sebagai derajat perluasan (extension degree) dari F_q. Bidang terbatas yang digunakan dalam kriptografi adalah q=p, dimana p adalah bilangan prima ganjil, yang dilambangkan dengan F_p (odd prime), dan $q=2^m$, dimana m adalah integer lebih besar dari satu, yang dilambangkan dengan F_{2m} (characteristic two or even).

Bidang Terbatas F_p merupakan sebuah bidangyang

beranggotakan bilangan integer {0,1,...,p-1}, dan p merupakan bilangan prima, setiapperhitungan dikalkulasikan dengan modulo pagar hasilnya tetap berada dalam daerah F_p.

Bidang terbatas F_{2m} biasa disebut dengan bidang terbatas biner (*binary finite field*), dapat dipandang sebagai ruang vektor berdimensi m pada F_2. Karena itu ada himpunan yang beranggotakan m elemen $\{\alpha_0, \alpha_1,... \alpha_{m-1}\}$di dalam F_{2m} sedemikian rupa msehingga setiapa $\in F_{2m}$ dapat ditulis secara unik ke dalam bentuk: $a = a_0 \alpha_0+a_1\alpha_1+...+a_{m-1}\alpha_{m-1}$, untuk ai $\in \{0,1\}$ Salah satu cara untuk merepresentasikan elemen-melemen pada F_{2m} adalah dengan representasi basis polinomial. Pada representasi basis polinomial elemen pada F_{2m} merupakan polinomial dengan derajat lebih kecil dari m, dengan koefisien bilangan 0 atau 1 $\{a_{m-1}x_{m-1} + ... + a_2x_2 + a_1x_1 + a_0x_0 \mid a_i : 0,1\}$

3.PERHITUNGAN ARITMATIKA PADA ECC

ECC menggunakan aritmatika modular atau aritmatika polinom untuk operasi, tergantung pada bidang yang dipilih. aritmatika yang melibatkan jumlah besar di kisaran 100s bit.

3.1 Modular Arimatika

Adalah aritmatika polynomial yang hasil operasinya brgantung dari area yang dipilih, modular aritmatka yang ada pada ECC adalah

- Addition
- Substraction
- Multiplication
- Divisio
- Multiplicative Inverse
- Finding x mod y

Beberapa penjelasan dari operasi modular aritmatika ini berlaku dalam bidang terbatas F_p dengan beberapa penjelasan sebagai berikut:

1. Penjumlahan (*Addition*), jika a,b $\in F_p$, maka a + b = r, dimana r adalah sisa pembagian a + b dengan bilangan prima p, $0 \le r \le p-1$. Penjumlahan seperti ini disebut penjumlahan modulo p (mod p).
2. Perkalian (*Multiplication*), jika a,b $\in F_p$, maka a• b = s, dimana s adalah sisa pembagian a • b dengan bilangan prima p, $0 \le s \le p-1$. Perkalian seperti ini disebut perkalian modulo p (mod p).

3.2 Polinomial Aritmatika

Operasi aritmatika polynomial akan brlaku untuk bidang trbatas F_{2m}:

- Addition
- Substraction
- Multiplication
- Divisio
- Multiplicative Inverse
- Irreducible polynimial

Beberapa penjalasan dari operasi yang berlaku dalam bidang terbatas F_{2m} representasi basis polynomial yang juga digunakan dalam ECC:

1. Penjumlahan (*Addition*), $(a_{m-1}...a_1a_0) + (b_{m-1}..b_1b_0) = (c_{m-1}...c_1c_0)$ dimana $c_i = a_i + b_i$. Operasi penjumlahan dapat menggunakan deretan komponen $(a_{m-1}...a_1a_0)$ yang di XOR-kan dengan $(b_{m-1}..b_1b_0)$.
2. Perkalian (*Multiplication*), (am-1...a1a0) • (bm-1..b1b0) = $(r_{m-1}...r_1 r_0)$ dimana $r_{m-1}x_{m-1} + ... + r_1x + r_0$ adalah sisa dari pembagian $(a_{m-1}x_{m-1} + ... + a_1x + a_0)$. $(b_{m-1}x_{m-1} + ... + b_1x + b_0)$ dibagi dengan polinomial f(x) pada F_2 (setiap koefisien polinomial direduksi ke modulo 2).

4. JENIS – JENIS ELLIPTIC CURVE CRYPTOGRAPHY

4.1 ECDSA – Elliptic Curve Digital Signature Algorithm

Algoritma pnandatanganan pesan menggunakan ECC yang disbutkan sebadi ECDSA adalah salah satu variasi dari Digital Signature Algorithm yang beroperasi dengan kelompok kurva elliptic sebagai basis perhitungan dari proses penandatanganan.

Agar dapat menyamakan suatu tandatangan digital dari sbuah psan yang dikirim oleh dua orang, maka kedua orang tersebut harus memiliki kurva elliptik yang sama. Seorang pngirim pesan yang akan ditandatangani akan memiliki sebuah kunci pribadi yang merupakan sbuah integer yang dipilih acak kurang dari n yangmerupakan urutan kurva, padametr kurva eliptik domain. Dan kunci publik yang merupakan titik yang digenrasikan dengan kurva eliptik domain dngan perhitungan sebagai berikut QA = dA * G

Proses ECDSA

1. Hitung e = Hash (m), di mana Hash adalah suatu fungsi hash kriptografi, seperti SHA-1
2. Pilih sebuah integer k secara acak dari [1, n - 1]
3. Hitung r = x1 (n mod), dimana (x1, y1) = k * G. Jika r = 0, lanjutkan ke langkah 2
4. Hitung s = k - 1 (e + dar) (mod n). Jika s = 0, lanjutkan ke langkah 2
5. tanda tangan adalah pasangan (r, s)

Proses Verivikasi dari ECDSA

1. Verifikasi bahwa r dan s adalah bilangan bulat pada [1, n - 1]. Jika tidak, tanda tangan tersebut tidak valid .
2. Hitung e = Hash (m), di mana Hash merupakan fungsi yang sama digunakan dalam signature
   generasi
3. Hitung w = s -1 (mod n)
4. Hitung U1 = ew (mod n) dan u2 = rw (mod n)

5. Hitung (x1, y1) = u1G + u2QA
6. tanda tangan ini berlaku jika x1 = r (mod n), dinyatakan tidak valid

Seperti dengan kriptografi kurva eliptik pada umumnya, ukuran bit dari kunci publik diyakini diperlukan untuk ECDSA adalah sekitar dua kali ukuran tingkat keamanan, dalam bit. Sebagai perbandingan, pada tingkat keamanan 80 bit, berarti penyerang membutuhkan sekitar setara dengan sekitar 280 generasi tanda tangan untuk menemukan kunci pribadi, ukuran kunci DSA publik setidaknya 1024 bit, sedangkan ukuran sebuah kunci publik ECDSA akan menjadi 160 bit. Di sisi lain, ukuran tanda tangan adalah sama untuk kedua DSA dan ECDSA: 4t bit, dimana t adalah tingkat keamanan yang diukur dalam bit, yaitu, sekitar 320 bit untuk tingkat keamanan 80 bit.

4.2 Elliptic Curve Diffie Hellman

ECDH-Elliptic Curve Diffie Hellman adalah sebuah protokol perjanjian kunci yang memungkinkan dua pihak pngirim dan penrima , yang pada awalnya masing-masing memiliki kurva eliptik sepasang kunci publik-swasta masing –masing, dan mengininkan sebuah kunci rahasia bersama melalui saluran yang tidak aman. Berbagi rahasia ini mungkin langsung digunakan sebagai tombol, atau lebih baik lagi, untuk mendapatkan kunci lain yang kemudian dapat digunakan untuk mengenkripsi komunikasi berikutnya menggunakan cipher kunci simetris. Ini adalah varian dari protokol Diffie-Hellman yang digunakan untuk menyamakan kunci untuk menggunakan kriptografi kurva eliptik.

Misalkan Pengirim ingin mendirikan sebuah kunci bersama dengan Penerima, tapi saluran hanya tersedia bagi mereka mungkin menguping oleh pihak ketiga. Awalnya, parameter domain (yaitu (p, a, b, G, n, h) dalam kasus perdana atau (m, f (x), a, b, G, n, h) dalam kasus biner) harus disepakati. Selain itu, masing-masing pihak harus memiliki sepasang kunci yang cocok untuk kriptografi kurva eliptik, terdiri dari sebuah kunci pribadi d: (a integer yang dipilih secara acak dalam interval [1 n - 1]), dan kunci publik Q (mana Q = DG). sepasang kunci Mari Pengirim akan (dA, QA) dan sepasang kunci Penerima akan (dB, QB). Setiap pihak harus memiliki kunci publik pihak lain (pertukaran harus terjadi).

Pengirim menghitung (xk, yk) dAQB =. Penerima menghitung k = dBQA. Kunci berbagi adalah xk (koordinat x dari titik tersebut).

Jumlah dihitung oleh kedua belah pihak adalah sama, karena dAQB = dAdBG = dBdAG = dBQA.

Protokol aman karena tidak ada yang diungkapkan (kecuali untuk kunci publik, yang tidak rahasia), dan tidak ada pihak yang dapat menurunkan kunci pribadi yang lain kecuali dapat memecahkan prosesor aritmatika Kurva Logaritma Diskrit Soal.

Kunci publik baik statis (dan dipercaya, mengatakan melalui sertifikat) atau singkat. Singkat tombol yang tidak harus dikonfirmasi, jadi jika otentikasi yang diinginkan, itu harus diperoleh dengan cara lain. Statis kunci publik tidak memberikan kerahasiaan maju atau tombol-kompromi ketahanan peniruan, antara lain sifat keamanan yang canggih. Pemegang kunci pribadi statis harus memvalidasi kunci publik lainnya, dan harus menerapkan fungsi derivasi aman kunci Diffie-Hellman baku berbagi rahasia untuk menghindari bocornya informasi tentang kunci pribadi statis. Untuk skema dengan sifat keamanan lebih lanjut lihat ECMQV.

5. HAL-HAL YANG PRLU DIPRERHATIKAN DALAM PENERAPAN ELLIPTIC CURVE CHRYPTOGRAPHY

Domain Parameter Kurva Ellips yang digunakan dalam ECC

Untuk menggunakan ECC semua pihak harus setuju pada semua elemen mendefinisikan kurva elliptic, yaitu parameter domain skema. lapangan didefinisikan oleh p dalam kasus utama dan sepasang m dan f dalam kasus binari. Kurva eliptik didefinisikan oleh konstanta a dan b yang digunakan dalam persamaan yang menentukan. Akhirnya, subgrup siklik didefinisikan oleh generator nya (aka. titik dasar) G. Untuk aplikasi kriptografi urutan G, yang adalah non-negatif terkecil n sehingga ng = O, harus prima. Karena n adalah ukuran subkelompok E (mathbb \ (F) _p) maka dari teorema Lagrange bahwa nomor h = \ frac (| E |) (n) adalah integer. Dalam aplikasi kriptografi ini h nomor, disebut kofaktor, harus kecil (h \ le 4) dan, sebaiknya, h = 1. Mari kita meringkas: dalam kasus perdana parameter domain bisa di-(n p, a, b, G,, h) dan dalam hal biner mereka (m, f, a, b, G, n, h). Kecuali ada jaminan bahwa parameter domain yang dihasilkan oleh salah satu pihak dipercaya sehubungan dengan penggunaan mereka, parameter domain harus divalidasi sebelum digunakan.

Pembuatan parameter domain tersebut tidak dilakukan oleh masing-masing pengirim atau penerima karena ini melibatkan menghitung jumlah titik pada kurva yang memakan waktu dan sulit untuk diterapkan. Akibatnya dipilih beberapa standar parameter domain kurva eliptik untuk beberapa ukuran lapangan yang umum, antara lain:

- NIST, Fitur Curves prosesor aritmatika untuk

Penggunaan Pemerintah

- SECG, 2 SEC: Fitur Domain Parameter Kurva untuk memproses aritmatika baik polynomial maupun modular.

Panjang Kunci

Skema ECC terkuat yang sudah berhasil diretas sampai saat ini memiliki sebuah kunci 112-bit untuk kasus dengan penggunaan umum dan sebuah kunci 109-bit untuk kasus dengan operasi biner. Untuk kasus pengenkripsian secara baisa rusak pada bulan Juli 2009 dengan menggunakan sekelompok lebih dari 200 PlayStation 3 game konsole dan bisa selesai dalam 3,5 bulan menggunakan cluster saat menjalankan terus menerus .Untuk kasus dengan pengoperasian biner, itu rusak pada bulan April 2004 dengan menggunakan 2.600 komputer selama 17 bulan operasi komputer.

Symmetric Key Size (bits)	RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Table 1: NIST Recommended Key Sizes

Security Level (bits)	Ratio of DH Cost : EC Cost
80	3:1
112	6:1
128	10:1
192	32:1
256	64:1

Table 2: Relative Computation Costs of Diffie-Hellman and Elliptic Curves[1]

Lisensi dan Ijin

Meskipun banyak keuntungan dari kurva eliptik dan meskipun adopsi kurva eliptik oleh banyak pengguna, banyak pengembang dan akademisi melihat lingkungan sekitarnya kekayaan intelektual kurva eliptik sebagai hambatan utama untuk pelaksanaan dan digunakan. Berbagai aspek dari kriptografi kurva eliptik telah dipatenkan oleh berbagai orang dan perusahaan di seluruh dunia. Terutama perusahaan Kanada, Inc Certicom memegang lebih dari 130 paten yang berkaitan dengan kurva eliptik dan kriptografi kunci publik pada umumnya.

Sebagai cara untuk membuka jalan bagi pelaksanaan kurva eliptik untuk melindungi AS dan sekutu informasi pemerintah, National Security Agency yang dibeli dari Certicom lisensi yang mencakup semua kekayaan intelektual mereka dalam bidang yang terbatas digunakan. Lisensi akan terbatas pada implementasi yang untuk keperluan keamanan nasional dan sertifikasi FIPS 140-2 atau telah disetujui oleh NSA. Selanjutnya, lisensi akan terbatas hanya bidang utama kurva mana perdana lebih besar dari 2255. Pada daftar NIST kurva 3 dari 15 fit bidang ini menggunakan: kurva bidang utama dengan bilangan prima dari 256 bit, 384 bit dan 521 bit. Certicom diidentifikasi 26 paten yang membahas hal ini bidang penggunaan. lisensi NSA meliputi hak untuk mensublisensikan ini 26 paten untuk pengembang produk bangunan dibatasi dalam bidang penggunaan. Certicom juga mempertahankan hak untuk pengembang lisensi baik dalam bidang penggunaan dan dengan persyaratan lain yang mereka dapat bernegosiasi dengan pengembang.

Komersial pengembang dapat menerima lisensi dari NSA menawarkan produk mereka cocok dalam bidang penggunaan lisensi NSA. Atau, pengembang komersial dapat menghubungi Certicom untuk lisensi untuk 26 hak paten yang sama. Certicom berencana untuk mengembangkan dan menjual toolkit perangkat lunak yang mengimplementasikan kriptografi kurva eliptik di bidang penggunaan. Dengan toolkit pengembang juga akan menerima lisensi dari Certicom untuk menjual lisensi teknologi oleh NSA di pasar komersial umum. Pengembang ingin menerapkan kurva eliptik di luar lingkup lisensi NSA perlu bekerja dengan Certicom jika mereka ingin menggunakan ECC.

KESIMPULAN

Kriptografi Kurva eliptik menyediakan keamanan yang lebih besar dan lebih efisien dalam hal penggunaan dibandingkan dengan generasi pertama teknik kunci publik (RSA dan Diffie-Hellman) sekarang digunakan. Sebagai vendor melihat ke upgrade sistem mereka seharusnya serius mempertimbangkan kurva eliptik alternatif untuk keuntungan komputasi dan penggunaan jaringan dengan tingkat keamanan yang sebanding dengan RSA dan Diffie Hellman.

REFERENCE

[1] Issues in Elliptic Curve Cryptography Implementation. Marisa W. Paryasto, Kuspriyanto, Sarwono Sutikno and Arif Sasongko School of Electrical Engineering and Informatics Institut Teknologi Bandung (ITB), Indonesia

[2]

[3] Elliptic Curve Cryptography : An Implementation Guide , Anoop MS , anoopms@tataelxsi.co.in , FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, Digital Signature Standard (DSS)

[4]

[5] SEC 1: Elliptic Curve Cryptography, Version 1.0, September 20, 2000.

[6]

[7] http://www.nsa.gov/business/programs/elliptic_curve.shtml

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, 17 Mei 2010

Nama dan NIM