Elliptic Curve Cryptography (Ecc) Pada Proses Pertukaran Kunci Publik Diffie-Hellman

Metrilitna Br Sembiring[1]

Abstrak

Elliptic Curve Cryptography (ECC) pada Proses Pertukaran Kunci Publik Diffie-Hellman. Dalam tugas akhir ini dibahas mengenai algoritma kriptografi kurva elliptik untuk enkripsi dan dekripsi data. Metode yang digunakan adalah dengan menggunakan kunci publik Diffie-Hellman. Hasil yang telah dilakukan bahwa hasil pertukaran kunci antara dua user menggunakan pertukaran Diffie-Hellman memberikan titik ke tiga (kunci private bersama) yang sama antara ke dua user tersebut.

Kata kunci: *Kriptografi, Kriptografi Kurva Eliptik, Diffie-Hellman*

[1] Metrilitna Br Sembiring, Mahasiswa S2 Matematika, FMIPA, Universitas Sumatera Utara, Email: metrilitna@gmail.com

Pendahuluan

Kemajuan dan perkembangan teknologi informasi dewasa ini telah berpengaruh pada hampir semua aspek kehidupan manusia, tak terkecuali dalam hal berkomunikasi. Dengan adanya internet, komunikasi jarak jauh dapat dilakukan dengan cepat dan murah. Namun disisi lain, ternyata internet tidak terlalu aman karena merupakan media komunikasi umum yang dapat digunakan oleh siapapun sehingga sangat rawan terhadap penyadapan informasi oleh pihak-pihak yang tidak berhak mengetahui informasi tersebut. Oleh karena pengguna internet yang sangat luas seperti pada bisnis, perdagangan, bank, industri, dan pemerintahan yang umumnya mengandung informasi yang bersifat rahasia, keamanan informasi menjadi faktor utama yang harus dipenuhi. Berbagai hal telah dilakukan untuk mendapatkan jaminan keamanan informasi menjadi suatu kode-kode yang tidak dimengerti. Apabila disadap, maka akan kesulitan untuk memahami isi informasi yang sebenarnya.

Salah satu sistem pengamanan yang dapat dimanfaatkan ialah sistem kriptografi kurva eliptik. Kriptografi kurva eliptik termasuk kedalam sistem kriptografi asimetris yang mendasarkan keamanannya pada permasalahan matematis kurva eliptik. Pada sistem ini digunakan masalah logaritma diskrit kurva eliptik dengan menggunakan grup kurva eliptik. Struktur kurva eliptik digunakan sebagai grup operasi matematis untuk melangsungkan proses enkripsi dan dekripsi. Kelebihan algoritma asimetris ini adalah proses pendistribusian kunci pada media yang tidak aman seperti internet, tidak memerlukan kerahasiaan. Karena kunci yang didistribusikan adalah kunci publik. Sehingga jika kunci ini sampai hilang atau diketahui oleh orang lain yang tidak berhak, maka pesan sandi yang dikirim akan tetap aman. Sedangkan kunci privat tetap disimpan (tidak didistribusikan).

Elliptic Curve Cryptography (ECC) mempunyai keuntungan jika dibandingkan dengan kriptografi asimetris lainnya yaitu dalam hal ukuran panjang kunci yang lebih pendek tetapi memiliki tingkat keamanan yang sama. Sebagai perbandingan, 160 bit Elliptic Curve Cryptography mempunyai tingkat keamanan ($3.8.10^{10}$ MIPS/Million Instruction per Second year) yang sama dengan 1024 bit RSA mempunyai tingkat keamanan (3.10^{12} MIPS year). Sehingga kecepatannya lebih tinggi, konsumsi daya yang lebih rendah, adanya penghematan bandwith. Keuntungan-keuntungan tersebut sangat berguna untuk aplikasi-aplikasi yang memiliki keterbatasan pada bandwith, kapasitas pemrosesan, ketersediaan sumber tenaga dan ruang. Aplikasi-aplilkasi tersebut antara lain: kartu chip, kartu kredit atau kartu debit, tiket elektronik, telepon selular, pager dan kartu identitas.

Diffie-Hellman pertama kali memperkenalkan algoritma kunci publik pada tahun 1976 atas hasil kerja sama antara Whitfield Diffie dan Martin Hellman. Metode

ini merupakan metode partikal pertama untuk menciptkan sebuah rahasia bersama antara dua belah pihak melalui sebuah jalur komunikasi yang tidak terjaga. Algoritma Diffie-Hellman ini memiliki keamanannya dari kesulitan menghitung algoritma diskrit dalam *finite field*, dibandingkan kemudahan dalam menghitung bentuk eksponensial dalam *finite field* yang sama. Algoritma ini dapat digunakan dalam mendistribusikan kunci publik yang dikenal dengan protokol pertukaran kunci.

Kriptografi kurva eliptik(Elliptic Curve Cryptography) menggunakan dua kunci yaitu kunci publik dan kunci privat. Kunci publik pada kriptografi adalah sebuah titik pada kurva eliptik dan kunci privatnya adalah sebuah angka random. Kunci publik diperoleh dengan melakukan opersai perkalian terhadap kunci privat dengan titik generator G pada kurva eliptik. Titik generator G digunakan untuk melakukan pertukaran kunci Diffie-Hellman. Sehingga menjadi dasar untuk memilih pertukaran kunci Diffie-Hellman.

Metode Penelitian

Langkah-langkah yang dilakukan peneliti dalam penelitian ini adalah sebagai berikut.

1. Menguraikan teori-teori dasar kriptografi.
2. Menyajikan masalah Elliptic Curve Cryptography (ECC) pada proses pertukaran kunci publik Diffie-Hellman.
3. Menganalisa proses pertukaran kunci publik Diffie-Hellman.
4. Mengambil kesimpulan.

Hasil dan Pembahasan

Pendekatan yang dilakukan untuk menghasilkan algoritma kriptografi kurva eliptik (Elliptic Curve Cryptography) adalah dengan menggunakan struktur matematika yang sangat unik yang memungkinkan pemrosesan titik dengan memiliki dua buah titik dalam sebuah kurva eliptik dengan menghasilkan sebuah titik lain yang ada pada kurva tersebut. Kriptografi kurva eliptik (Elliptic Curve Cryptography) menggunakan dua kunci yaitu kunci publik dan kunci privat. Kunci publik pada kriptografi kurva eliptik adalah sebuah titik pada kurva eliptik dan kunci privatnya adalah sebuah angka random. Kunci publik diperoleh dengan melakukan operasi perkalian terhadap kunci privat dengan titik generator G pada kurva eliptik. Titik generator G digunakan untuk melakukan pertukaran kunci Diffie-Hellman.

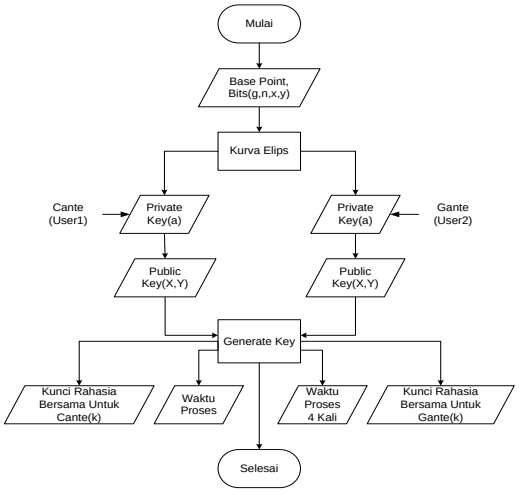
Algoritma Pertukaran Kunci Diffie - Hellman

Diffie-Hellman merupakan suatu algoritma kunci publik yang pertama kali ditemukan pada tahun 1976, meskipun NSA mengaku telah menemukan algoritma asimetrik jauh-jauh hari sebelumnya. Algoritma ini memperoleh keamanannya dari sulitnya menghitung logaritma diskrit pada bilangan yang sangat besar. Algoritma Diffie-Hellman hanya dapat digunakan untuk pertukaran kunci (simetri) dan tidak dapat digunakan untuk enkripsi dan dekripsi maupun untuk tanda tangan digital. (Dony Ariyus, 2006)

Diffie-Hellman pertama kali memperkenalkan algoritma kunci publik pada tahun 1976 dan sebelumnya ditemukan oleh Malcolm Williamson pada tahun 1974. Algoritma ini memiliki keamanannya dari kesulitan menghitung logaritma diskrit dalam *finite field*, dibandingkan kemudahan dalam menghitung bentuk eksponensial dalam *finite field* yang sama. Algoritma ini dapat digunakan dalam mendistribusikan kunci publik yang dikenal dengan protokol pertukaran kunci.

Sistem ini dipakai untuk menyandikan pertukaran pesan antar dua pihak secara interaktif. Pada awalnya, masing-masing pihak mempunyai sebuah kunci rahasia yang tidak diketahui pihak lawan bicara. Dengan berdasar pada masing-masing kunci rahasia ini, ke dua pihak dapat membuat sebuah kunci sesi (session key/kunci rahasia untuk komunikasi dengan kriptografi simetri) yang akan dipakai untuk pembicaraan selanjutnya.

Pembuatan kunci sesi ini dilakukan seperti halnya suatu tanya jawab matematis, hanya pihak yang secara aktif ikut dalam tanya jawab ini sajalah yang bisa mengetahui kunci sesinya. Penyadap yang secara aktif mengikuti tanya jawab ini tidak akan bisa mengetahui kunci sesi ini. (Andri Kristanto, 2003).



Gambar 1. Struktur Kunci Diffie-Hellman

Parameter umum:

1. Misalkan dua orang user yang berkomunikasi: user1 dan user2.
2. Mula-mula user1 dan user2 menyepakati bilangan prima yang besar, n dan g sedemikian sehingga g < n.
3. Bilangan n dan g tidak perlu rahasia. Bahkan, user1 dan user2 dapat membicarakannya melalui saluran yang tidak aman sekalipun.

Berikut ini algoritma pertukaran kunci Difiie-Hellman yang diilustrasikan dua orang user (user1 dan user2):

1. User1 memilih secara acak sebuah bilangan integer x yang besar dan mengirimkannya ke user2.

   $X = g^x \bmod p$

2. User2 memilih secara acak sebuah bilangan integer y yang besar dan mengirimkannya ke user1.

   $Y = g^y \bmod p$

3. User1 menghitung nilai $k1 = Y^x \bmod p$

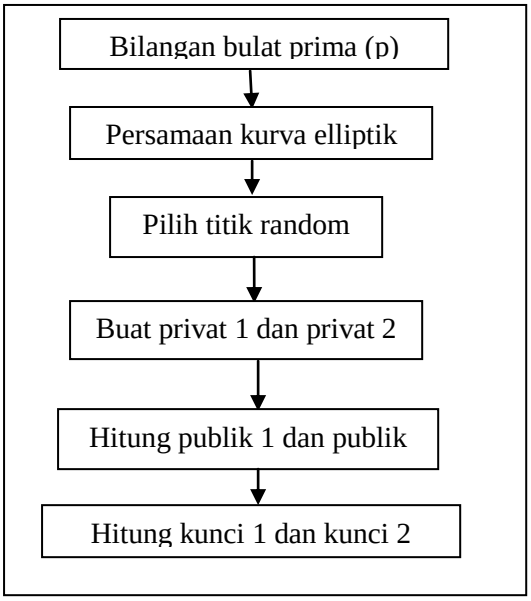
4. User2 menghitung nilai k2 = X^y mod p

Jika perhitungan dengan benar, maka k1 = k2.

5. Baik k1 dan k2 sama dengan g^{xy} mod p.
6. Penyadap yang menyadap pembicaraan antara user1 dan user2 tidak dapat menghitung k. Ia hanya memiliki informasi n, g, X dan Y, tetapi ia tidak mempunyai informasi nilai x dan y.
7. Untuk mengetahui x dan y, ia perlu melakukan perhitungan logaritma diskrit, yang mana sangat sulit dikerjakan.

Proses Pertukaran Kunci Diffie-Hellman pada Elliptic Curve Cryptography

Tahapan-tahapan dalam prosedur pertukaran kunci Diffie-Hellman untuk memperoleh kunci privat bersama:



Gambar 2 Diagram dari proses pertukaran kunci Diffie-Hellman

Dari gambar 2 penulis dapat menjabarkan langkah-langkah sebagai berikut:

1. **Menentukan bilangan prima (p) dengan syarat p > 3 untuk F_p**

Misalkan diambil sembarang bilangan prima = 13 bilangan prima atau bukan. Kemudian diambil nilai n = 2 karena PBB atau pembagi bersama terbesar (13, 2) = 1

$n^{p-1} \equiv 1 \pmod p = 2^{13-1} = 8191 \equiv 1 \pmod{13}$

Dengan demikian 13 adalah bilangan prima karena tidak habis dibagi, sehingga didapat p = 13.

2. **Menentukan bentuk persamaan kurva eliptik**

Persamaan kurva eliptik $y^2 = x^3 + ax + b \pmod p$ dan nilai a, b dibuat secara acak (random) untuk koefisiennya. Misalkan a = 4, b = 9 dan p = 13, persamaan kurva eliptik menjadi:

$y^2 = x^3 + 4x + 9 \pmod{13}$

Sehingga:

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

$4.4^3 + 27.9^2 \pmod{13}$

$= 2443 \pmod{13}$

$= 12 \neq 0 \pmod{13}$.

Cara mencari kurva dengan persamaan diatas adalah:

Misalkan diambil sembarang titik:

Misalkan: x = 0

$y^2 = x^3 + 4x + 9$

$y^2 = 0^3 + 4.0 + 9$

$y^2 = 9y = \pm\sqrt{9}$

$y_1 = 3$ dan $y_2 = -3$

misalkan: x = 1

$y^2 = x^3 + 4x + 9$

$y^2 = 1^3 + 4.1 + 9$

$y^2 = 1 + 4 + 9$

$y^2 = 14$

$y = \pm\sqrt{14}$

$y_1 = \sqrt{14}$ dan $y_2 = -\sqrt{14}$

misalkan: x = 2

$y^2 = x^3 + 4x + 9$

$y^2 = 2^3 + 4.2 + 9$

$y^2 = 8 + 8 + 9$

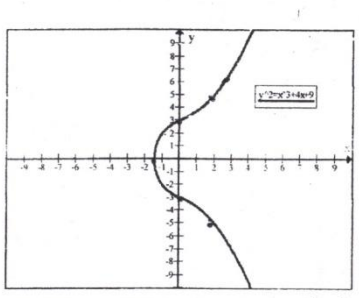
$y^2 = 25$

$y = \pm\sqrt{25}$

$y_1 = 5$ dan $y_2 = -5$

dengan cara yang sama untuk menghitung nilai x dan y nya sehingga dalam bentuk kurva ditunjukkan dalam gambar berikut ;

Gambar kurva eliptik pada persamaan $y^2 = x^3 + 4x + 9$



Gambar 3. Kurva eliptik dengan persamaan $y^2=x^3+4x+9$

Proses untuk menentukan bentuk persamaan kurva eliptik dengan mengembangkan koefisien a, b secara acak dengan a = acak (p) dan b = acak (p), bilangan prima (p) di sini telah dihitung sebelumnya pada (**Gambar 3)** di mana a, b € F_p dan a, b ≠ 0. Kemudian melakukan pengecekan dengan memasukkan ke dua koefisien tersebut ke dalam persamaan diskriminan. Jika hasil $4a^3 + 27b^2 = 0$ (mod p), maka akan dilakukan proses perulangan kembali mulai dari mengembangkan nilai a dan b sampai didapatkan hasil dari nilai diskriminannya tidak sama dengan nol.

3. Menentukan titik utama pada kurva

Menentukan titik-titik utama pada kurva, kemudian pilih satu titik p secara sembarang pada kurva $E(F_p)$. Bilangan prima p = 13. Selanjutnya dicari elemen-elemen grup eliptik E_{13} atas F_p, dengan F_p = {0,1,2,3,4,5,6,7,8,9,10,11,12}. Sebelum menentukan elemen-elemen E_{13} (4,9), terlebih dahulu mencari quadratic residue 13 (QR_{13}).

Tabel 1 QR_{13}

F_p	y^2 (mod 13)	R_{13}
0	0^2 (mod 13)	0
1	1^2 (mod 13)	1
2	2^2 (mod 13)	4
3	3^2 (mod 13)	9
4	4^2 (mod 13)	3
5	5^2 (mod 13)	12
6	6^2 (mod 13)	10
7	7^2 (mod 13)	10
8	8^2 (mod 13)	12
9	9^2 (mod 13)	3
10	10^2 (mod 13)	9
11	11^2 (mod 13)	4
12	12^2 (mod 13)	1

Berdasarkan Tabel 1 himpunan QR_{13} = {0,1,3,4,9,10,12}. Kemudian menentukan elemen grup *eliptik* E_{13} (4,9) yang merupakan penyelesaian dari persamaan $y^2 = x^3 + 4x + 9$ (mod 13). Untuk x € F_{13} dan y^2 € QR_{13}.

Tabel 2. Untuk Mencari Elemen E_{13} (4,9)

X € F_{13}	$y^2 = x^3 + 4x + 9$ (mod 13)	y^2 € QR_{13}	(x,y) x € E_{13}(4,9)
0	9	Ya	(0,1) dan (0,10)
1	1	Ya	(1,1) dan (1,12)
2	12	Ya	(2,5) dan (2,8)
3	9	Ya	(3,3) dan (3,10)
4	11	Bukan	-
5	11	Bukan	-
6	2	Bukan	-
7	3	Ya	(7,4) dan (7,9)
8	7	Bukan	-
9	7	Bukan	-
10	9	Ya	(10,3) dan (10,10)
11	6	Bukan	-
12	4	Ya	(12,2) dan (12,11)

Berdasarkan Tabel 2 untuk x = 0, diperoleh y2= 0 + 0 + 0 + 4.0 + 9 (mod 13) = 9. Sehingga diperoleh nilai y = 3 dan y = 10. Karena berdasarkan Tabel 4.1, 3^2 (mod 13) = 9 dan 10^2 (mod 13) = 9. Perhitungan untuk nilai x dan y yang lain, dilakukan dengan cara yang sama. Sehingga didapatkan elemen-elemen grup *eliptik* modulo 13 atas $F_{13,}$ yaitu F_{13} (4,9)

= {(0,3), **(0,10)**, (1,1), (1,12), (2,5), (2,8), (3,3), (3,10), (7,4), (7,9), (10,3), (10,10), (12,2), (12,11), ***O***}. Jumlah titik utama pada kurva = 14 titik selain dari titik *infinity* (**O**). Misal titik yang dipilih adalah p = **(0,10).**

4. Menghitung privat1 dan privat2.

Menentukan nilai acak kunci privat user1(privat1) dan user2(privat2), dengan privat1, privat2 elemen {2,3,...p-1} dalam F_p. Misal privat1 = 3 dan privar2 = 4. Prosedur untuk menentukan kunci privat ke dua user dengan menentukan nilai dari privat1 = random (p-1) + 3 dan privat2 = random (p-1) + 4 secara random. Jka privat1, privat2 < 1, maka akan terus terjadi perulangan mulai dari awal sampai didapatkan privat1, privat2 ≥ 1.

5. Menghitung publik1 dan publik2

Pembangkitan kunci publik oleh ke dua user dan menghitung kunci publik masing-masing.

User1 menghasilkan publik1 = privat1*p.

Publik1 = privat1*p = 3 * (0,10) + (0,10) + (0,10) = ...

P = (0,10), karena titiknya sama, maka P = Q.

$$\lambda = \frac{3x^2 + a}{2y_1}$$

$$\lambda = \frac{3(0^2)+4}{2.10} = 4*(20^{-1}) = 8 \pmod{13}$$

$x_3 = \lambda^2 - x_1 - x_2$

$x_3 = 8^2 - 0 - 0 = 64 =$ **12** (mod 13)

$y_3 = \lambda(x_1 - x_3) - y_1$

$y_3 = 8(0 - 12) - 10 = -106 = -2 =$ **11** (mod 13)

jadi publik1 = (x_3,y_3) = **(12,11)**

User2 menghasilkan kunci publik (publik2) = privat2*p.

Publik2 = privat2*p = 4*(0,10) = (0,10) + (0,10) + (0,10) = (12,11) + (0,10)

Karena titiknya berbeda, maka P ≠ Q.

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

$$\lambda = \frac{11-10}{12-0} = 1*(12^{-1}) = 12 \pmod{13}$$

$x_3 = \lambda^2 - x_1 - x_2$

$x_3 = 12^2 - 0 - 12 = 132 = 2$ (mod 13)

$y_3 = \lambda(x_1 - x_3) - y_1$

$y_3 = 12(0 - 2) - 10 = -34 = 5$ (mod 13)

Jadi, publik2 = (x_3,y_3) = (2,5).

6. Menghitung kunci1 dan kunci2

Ke dua user saling menukar kunci publik mereka masing-masing untuk menghasilkan kunci privat yang sama. Pada tahapan ini dibuktikan bahwa kunci1 = kunci2.

User1 menghasilkan,

Key1 = privat1*publik2

= 3*(2.5) = (10,10)

User2 menghasilkan,

Key2 = privat2*publik1

= 4*(12,11) = (10,10)

Sehingga nilai kunci1 = kunci2 = (10,10).

Penutup

Adapun kesimpulan yang dapat diperoleh adalah:

1. Keunggulan dari kriptigrafi kurva eliptik adalah proses transformasi plaintext menjadi titik-titik dalam kurva eliptik sebelum dilkakukan enkripsi. Proses enkripsinya dilakukan dengan menggunakan aturan penjumlahan pada kurva eliptik. Proses ini tentunya akan memberikan tingkat keamanan yang lebih baik.

2. Hasil yang telah dilakukan bahwa hasil pertukaran kunci antara dua user menggunakan pertukaran Diffie-Hellman memberikan titik ke tiga (kunci private bersama) yang sama antara ke dua user tersebut.

Daftar Pustaka

Ariyus, Dony, 2006, *Kriptografi Keamanan Data dan Komunikasi*. Yogyakarta: Penerbit Graha Ilmu.

Ariyus, Dony, 2008, *Pengantar Ilmu Kriptografi Teori, Analisis dan Implementasi.* Yogyakarta: Penerbit Andi.

Juhana, Nana, 2005, *Implementasi Elliptic Curves Cryptosystem (ECC) Pada Proses Pertukaran Kunci Diffie-Hellman dan Skema Enkripsi ElGamal*, Institut Teknologi Bandung, Bandung.

Kristanto, Andri, 2003, *Keamanan Data pada Jaringan Komputer.* Yogyakarta: Gava Media.

Triwiinarko, Andi, 2004, Elliptic *Curve Signature Algorithm (ECDSA).* Departemen Teknik Informatika, Institut Teknologi Bandung, Bandung.