Implementasi *Elliptic Curve Cryptography* (ECC) Dalam Jalur Komunikasi Aplikasi Chatting

Muhammad Reza Nur Fauzi, 18219064 (*Author*)
Study Program System and Technology Information
School Technique Electro and informatics
Institute Bandung Technology , Street Ganesha 10 Bandung
Email : mrezanurfauzi@gmail.com

***Abstract* — Mengirim pesan atau data sering kali kita lakukan tanpa kita ketahui resikonya. Untuk melindungi data/informasi tersebut, diperlukan suatu mekanisme yang dapat membuat data tersebut tidak dapat diakses oleh siapa pun selain penerima yang dituju. peningkatan keamanan Untuk mencapai enkripsi dan dekripsi asimetris, masing-masing pihak harus memiliki kunci pribadi dan kunci publik. Aplikasi *chatting* menjadi salah satu platform yang digunakan masyarakat untuk menyampaikan informasi kepada pengguna lain. Tentu saja, informasi yang dikirimkan oleh aplikasi tersebut menjadi sesuatu yang ingin kita jaga agar tetap aman dari aktor jahat. Penggunaan Kriptografi Kurva Elliptik untuk mengamankan informasi penting di dalam komunikasi aplikasi *chatting* akan dibahas dalam artikel ini.**

Keywords— ***keamanan; Kriptografi; ECC; aplikasi chatting***

I. PENDAHULUAN

Dunia digital sudah mulai berkembang dari tahun ke tahun, perkembangan dunia digital ini memberi dampak positif dan negatif terhadap segala aktivitas masyarakat dalam pemenuhan kebutuhan mereka. Dengan adanya jaringan internet, perangkat digital, platform komunikasi, media sosial, dan aplikasi-aplikasi yang mendukung kebutuhan pengguna. Perkembangan dunia digital memberikan dampak terhadap bentuk teknologi yang digunakan oleh masyarakat kearah yang serba digital. Dengan demikian perkembangan teknologi digital juga memberkan dampak positif terhadap sistem informasi di dalam kehidupan masyarakat. Sistem informasi yang turut berkembang memberikan peningkatan performa dalam berbagai sektor kebutuhan masyarakat, mulai dari perekonomian, perkantoran, pendidikan, dan berbagai sektor lainnya. Perkembangan dunia digital juga memberi kemudahan bagi masyarakat untuk saling terhubung tanpa dibatasi dengan adanya ruang dan waktu. Hal tersebut tidak menutup kemungkinan bahwa masyarakat melakukan pertukaran informasi melalui media digital, salah satu pilihan dari masyarakat dalam menyampaikan informasi adalah melalui *chatting*. Aplikasi *chatting* adalah sebuah platform digital yang memungkinkan pengguna untuk bertukar informasi melalui jaringan internet dengan pengguna lainnya yang menggunakan platform digital yang sama. Namun, tidak menutup kemungkinan bahwa informasi yang disampaikan merupakan informasi penting dan sangat rahasia, sehingga dibutuhkan tingkat keamanan yang tinggi untuk dapat menghindari terjadinya penyadapan oleh pihak ketiga yang ingin mendapatkan informasi atau data-data yang ditransmisikan.

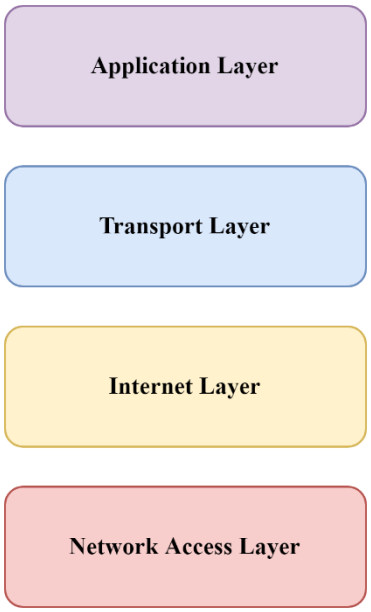
Untuk mengirim data sensitif seperti identitas pengguna, lokasi, dan data rahasia lainnya ke sesama pengguna. Tanpa perlindungan yang tepat, transfer data atau informasi rentan terhadap penyadapan. Untuk mengamankan data/informasi, diperlukan suatu teknik yang dapat menghasilkan data yang tidak diketahui oleh siapa pun selain penerima yang dituju dari data yang dipermasalahkan. Metode harus dapat mengamankan data. Untuk mengamankan akses data dari pihak yang tidak berwenang, diperlukan enkripsi dan deskripsi [1]. Untuk mendapatkan keamanan yang tinggi dalam menjaga informasi yang dikirimkan melalui jaringan internet diperlukan sebuah teknik enkripsi dan dekripsi sebagai cara untuk mengamankan data yang ditransimisikan melalui jaringan internet. Dengan demikian, *Elliptic Curve Cryptography (ECC)* menjadi algoritma atau metode pilihan yang akan digunakan pada aplikasi *chatting*. Pada makalah ini akan mengeksplorasi implementasi *Elliptic Curve Cryptography* (ECC) pada jalur komunikasi aplikasi *chatting*.

II. TEORI DASAR

A. *Tansmission Control Protocol/Internet Protocol* (TCP/IP)

Protokol merupakan sebuah standar yang mengatur bagaimana sebuah hubungan, penyampaian data, dan komunikasi antar dua atau lebih perangkat. Protokol dapat digunakan diberbagai jenis platform digital sebagai standar komunikasi perangkat. TCP/IP merupakan salah satu jenis protokol komunikasi data mulai dikembangkan pada tahun 1970-an sampai dengan tahun 1980-an untuk digunakan sebagai standar komunikasi data antar komputer dan jaringan secara luas. Konsep kerja dari protokol ini adalah menggunakan sebuah alamat yang dinamakan IP sebagai identitas tujuan dari proses komunikasi data. Sehingga, protokol ini dapat menghubungkan perangkat digital dalam

jumlah yang banyak tanpa adanya kesalahan dalam penyampaian data yang dilakukan.



Gambar I.1 Lapisan Protocol TCP/IP

Didalam sebuah perotokol TCP/IP teradapat berbagai macam lapisan komunikasi yang dibagi ke dalam empat lapisan yang diantaranya yaitu:

1. Protokol komunikasi lapisan aplikasi yang berguna untuk memberikan akses kepada sebuah platform digital untuk menggunakan layanan jaringan TCP/IP
2. Protokol komunikasi lapisan antar host yang berguna untuk membuat komunikasi yang akan dilakukan ke dalam sesi koneksi yang bersifat *connection-oriented*, dalam hal ini juga terdapat protokol-protokol lain yang digunakan dalam lapisan ini yaitu, Transmission Control Protocol (TCP) dan User Datagram Protocol (UDP).
3. Protokol komunikasi lapisan inter-network yang berguna untuk melakukan pemetaan dan membungkus pakat-paket data informasi menjadi sebuah paket-paket IP yang akan ditransmisikan. Dalam lapisan ini juga terdapat beberapa protokol yang digunakan yaitu *Internet Protocol* (IP), *Internet Control Message Protocol* (ICMP), *Address Resolution Protocol* (ARP), dan *Internet Group Management Protocol* (IGMP).
4. Protokol komunikasi lapisan interface jaringan yang bertanggung jawab untuk memetakan paket-paket IP di atas media jaringan yang akan digunakan, beberapa jenis transport yang dapat digunakan oleh TCP/IP yaitu LAN, *Integrated Services Digital Network* (ISDN), *Asychronous Transfer Mode* (ATM), dan sebagainya.

TCP/IP juga berguna untuk memberikan layanan pengiriman berkas data dengan melalui *File Transfer Protocol* (FTP) sehingga setiap client di dalam jaringan dapat bertukar berkas dengan metode otentikasi melalui *username* dan *password*.

B. Kriptografi

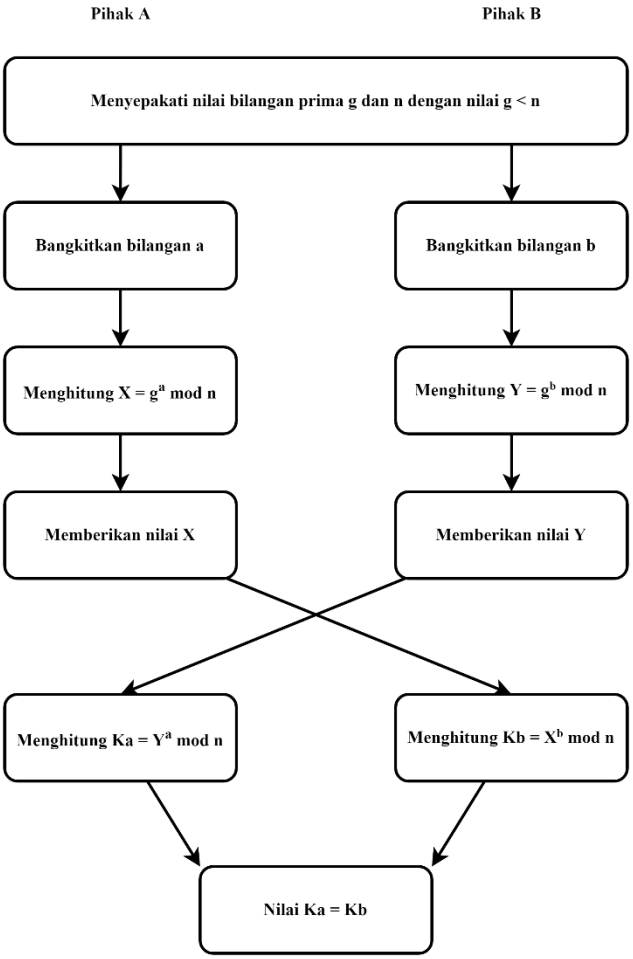
Kriptografi (*cryptography*) berasal dari bahasa Yunani yaitu crypto yang berarti tulisan yang tersembunyi, dan graphein yang berarti tulisan (*writing*). Penulisan rahasia dapat diartikan dengan begitu mudahnya (*secret writing*). Kriptografi kadang-kadang didefinisikan sebagai studi yang menyelidiki strategi matematika yang terkait dengan masalah keamanan informasi termasuk kerahasiaan, integritas data, dan otentikasi. Kriptografi adalah ilmu dan seni menjaga pesan tetap aman ketika dipindahkan dari satu lokasi ke lokasi lain, menurut terminologinya [8]. Algoritma kriptografi memiliki tiga fungsi utama: enkripsi, dekripsi, dan pembangkitan kunci. Proses penyamaran komunikasi data dengan mengubah plaintext menjadi ciphertext dikenal sebagai enkripsi. Dekripsi, di sisi lain, berusaha untuk memahami pesan, dan kuncinya adalah mekanisme yang digunakan untuk enkripsi dan dekripsi. Enkripsi tidak harus rumit atau melalui tahapan-tahapan yang sulit dipahami pada level kriptografi saat ini. Kriptografi, serta aplikasi kriptografi, dapat dibuat portabel bahkan pada periode saat ini.

Dalam hal menjaga komunikasi di desktop atau data seluler, aplikasi yang dibuat untuk kriptografi adalah alat yang memungkinkan enkripsi dan dekripsi. Keamanan perangkat berlapis-lapis berkat penggunaan program kriptografi ini. Untuk membuka gadget, seseorang harus melewati berbagai set kunci yang telah dikeluarkan untuk mengamankan perangkat tersebut. Jelas, seseorang yang menggunakan enkripsi dalam aplikasi mereka memiliki privasi yang sangat besar. Aplikasi yang menggunakan kriptografi dianggap penting untuk digunakan demi kerahasiaan dan privasi. Orang dengan niat jahat akan kehilangan kesabaran selama dekonstruksi karena adanya lapisan keamanan berlapis.

C. Diffie-Hellman Algorithm

Whitfield Diffie dan Martin Hellman pada tahun 1976 mempublikasikan sebuah karya publik pertama yang mengusulkan konsep sebuah kriptografi dengan pasangan kunci publik dan kunci pribadi. Algoritma Diffie-Hellman adalah sebuah algoritma pertukaran kunci yang akan digunakan untuk melakukan enkripsi dan dekripsi informasi yang dimana kunci tersebut akan dibangkitkan oleh pengirim dan penerima informasi melalui pertukaran sebuah angka acak yang disepakati bersama sebagai salah satu parameter untuk membangkitkan kunci publik dan kunci pribadi. Kunci yang disampaikan melalui algoritma Diffie-Helman merupakan kunci yang dapat disebarkan secara bebas tanpa mengkhawatirkan keamanan dari informasi yang telah dienkripsi. Karena kunci tersebut hanya dapat digunakan oleh pihak yang mengetahui salah satu parameter yang akan digunakan dalam proses dekripsi informasi yang sudah diekripsi. Hal tersebut dikarenakan pada proses pertukaran dengan algoritma Diffie-Hellman tidak terjadi

pertuksran kunci yang akan digunakan untuk melakukan enkripsi dan dekripsi, sehingga keamanan dari informasi yang disampaikan sudah dapat terjamin keamanannya. Sehingga, pihak ketiga yang ingin mendapatkan informasi tersebut sangat tidak memungkingkan untuk mendapatkan kunci yang digunakan untuk melakukan enkripsi dan dekripsi terhadap informasi yang disamapaikan.



Gambar I.2 Proses pertukaran kunci dengan algoritma Diffie-Helman.

Secara umum langkah-langkah dalam melakukan pertukaran kunci melalui algoritma Diffie-Helman, yaitu:

1. Pihak A dan Pihak B menyepakati sebuah bilangan prima yang besar yaitu n dan g, sedemikian sehingga nilai g < n. Bilangan g dan n bukanlah bilangan yang perlu dirahasiakan.
2. Pihak A membangkitkan satu buah bilangan acak yang nilainya besar yang disebut sebagai bilangan a.
3. Bilangan a tersebut disubtitusikan ke dalam fungsi
$$X = g^a \bmod n$$
Hasil dari perhitungan nilai X tersebut diberikan kepada pihak B.
4. Pihak B membangkitkan satu buah bilangan acak yang nilainya besar yang disebut sebagai bilangan b.
5. Bilangan b tersebut disubtitusikan ke dalam sebuah fungsi
$$Y = g^b \bmod n$$
Hasil dari perhitungan nilai Y tersebut diberikan kepada pihak A.
6. Pihak A menerima hasil perhitungan nilai Y dari pihak B lalu menghitung nilai kunci dengan menggunakan fungsi
$$Ka = Y^a \bmod n$$
Hasil dari perhitungan nilai Ka tersebut menghasilkan sebuah kunci enkripsi simetri.
7. Pihak B menerima hasil perhitungan nilai X dari pihak A lalu menghitung nilai kunci dengan menggunakan fungsi
$$Kb = X^b \bmod n$$
Hasil dari perhitungan nilai Kb tersebut menghasikan sebuah kunci enkripsi simetri.
8. Nilai Ka dan Kb dari hasil perhitungan pihak A dan B merupakan sebuah kunci enkripsi simetri yang akan digunakan sebagai kunci untuk melakukan enkripsi dan dekripsi terhadap informasi yang dirahasiakan.

D. Elliptic Curve Cryptography (ECC)

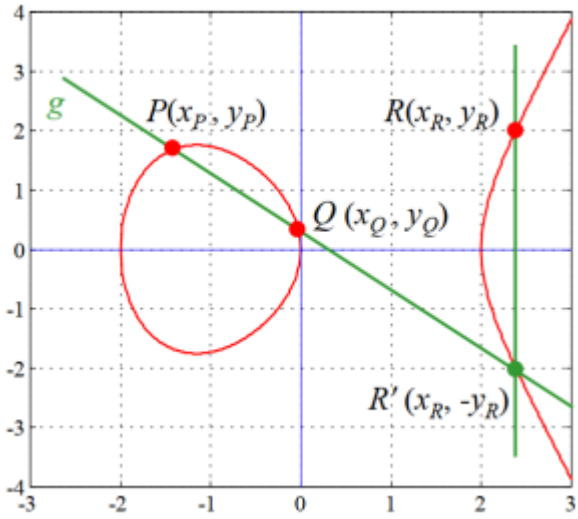
Neal Koblitz dan Victor Miller dari Universitas Washington menemukan Elliptic Curce Cryptosystem (ECC) pada tahun 1985. Kurva elips memiliki kesulitan tersendiri untuk menangani kesulitan logaritmik. Kriptografi kurva elips adalah sistem kriptografi kunci publik yang keamanannya didasarkan pada masalah matematika kurva eliptik. Masalah logaritma yang berbeda ada untuk kurva eliptik, yang sulit untuk dipecahkan. Kriptografi kurva elips adalah teknik kriptografi kunci publik yang aman. Teknik Kriptografi Kurva Elliptik dikembangkan menggunakan struktur matematika yang sangat tidak biasa yang memungkinkan pemrosesan titik dengan menggunakan dua titik pada kurva eliptik untuk menghasilkan titik lain pada kurva.

Kriptografi kurva eliptik adalah kriptografi kunci publik. Setiap pengguna atau perangkat yang berpartisipasi dalam komunikasi memiliki pasangan kunci, khususnya kunci publik dan kunci pribadi, dalam kriptografi kunci publik. Kunci pribadi yang cocok hanya dapat digunakan oleh pengguna yang cocok, sedangkan kunci publik dibagikan dengan entitas yang mengirim data. Faktor-faktor berikut menyebabkan pemilihan Kriptografi Kurva Elliptik ECC sebagai pendekatan kriptografi untuk perlindungan dokumen:

1. Ukuran bidang di mana kurva elips diposisikan dapat dipilih untuk membuat Kriptografi Kurva Elliptik lebih mudah diterapkan dalam rentang tertentu.
2. Karena teknik Kriptografi Kurva Elliptik menghasilkan kunci besar yang tidak terlalu besar, maka tidak memerlukan banyak memori tambahan.
3. Untuk menekan biaya implementasi, prosedur kriptografi Kriptografi Kurva Elliptik tidak memerlukan prosesor tertentu.

Karena sulit untuk menemukan dua titik yang menunjukkan titik tertentu, struktur yang tidak biasa ini

memberikan keuntungan dalam kriptografi. Kesulitan menemukan dua poin, serta kesulitan menghitung fluktuasi eksponensial dalam teknik RSA yang banyak digunakan, keduanya termasuk dalam kategori rumit. Kriptografi Kurva Elliptik melibatkan perhitungan matematis yang sangat kompleks untuk dipecahkan. Kriptografi Kurva Elliptik terdiri dari berbagai operasi dasar serta aturan yang menentukan bagaimana menggunakan operasi dasar seperti penambahan, pengurangan, perkalian, dan kekuatan berdasarkan kurva yang ada.



Gambar II.1 Kurva eliptik penjumlahan titik [3]

Rumus standar yang digunakan dalam membangun sebuah kurba eliptik pada algoritma ECC, yaitu

$$y^2 = x^3 + ax + b \qquad (1)$$

File kunci umum yang berisi kurva eliptik E, titik P yang berada di E, bilangan bulat prima p Fp, dan kunci publik pengguna lain Q = d*P dibaca terlebih dahulu dalam prosedur enkripsi. File data kemudian dibaca oleh blok (M) dan dienkripsi dengan: 2,...,p-1, yang bervariasi untuk setiap blok data, dan k*Q dan k*P dihitung.

$$M' = [k * P, M\ X\ (k * Q)] \qquad (2)$$

Keterangan :
M = data yang akan dienkripsi (*plaintext*).
M' = blok data yang telah dienkripsi (*ciphertext*).
k = suatu bilangan random yang akan digunakan sebagai session key dengan k ∈ {2,…,p-1}
Q = d*P
P = suatu point pada kurva E(Fp)
X(k*Q) = koordinat X untuk point yang dihasilkan dari perkalian k*Q.

Kami membaca file kunci publik yang terdiri dari kurva eliptik E, titik P di E, dan bidang bilangan prima p untuk memulai proses dekripsi. Kemudian untuk menghitung d*(k*P), di mana d adalah kunci pribadi pengguna dalam bentuk frasa sandi, dan k*P adalah teks sandi. Kemudian satu blok data (M') dibaca. Metode dekripsi kemudian dilakukan untuk menghasilkan M, menggunakan

$$M = [M` \oplus X(d * (k * P))] \qquad (3)$$

M` di-xor-kan dengan absis point yaitu d*(k*P) sehingga diperoleh suatu string. Hasilnya (M) lalu ditulis ke berkas.

III. Analisis Permasalahan

Pada umumnya komunikasi melalui perangkat digital sangat rentan terhadap penyadapan oleh pihak ketiga. Saranan komunikasi melalui aplikasi *chatting* menjadi salah satu pilihan masyarakat umum sebagai salah satu alternatif jalur komunikasi. Namun bukan tidak mungkin, komunikasi tersebut dapat mengandung data sensitif seperti nama pengguna, lokasi, dan informasi pribadi. Orang yang tidak berwenang dapat mencegat transmisi data komunikasi antar pengguna untuk mendapatkan informasi tersebut. Makalah ini akan membahas salah satu teknik untuk meningkatkan keamanan pada aplikasi *chatting* antar pengguna melalui perangkat digital.

IV. Usulan Solusi

Untuk mengatasi masalah ini, makalah ini menyarankan penggunaan algoritma ECC sebagai lapisan keamanan di dalam aplikasi *chatting* untuk menyediakan sistem kriptografi kunci publik. Karena banyak aplikasi komunikasi yang menggunakan algoritma lain untuk melakukan enkripsi dan dekripsi terhadap data yang akan ditransmisikan, namun dengan tingkat daya komputasi yang tinggi, maka metode ini dipilih. ECC membutuhkan sumber daya komputasi yang lebih sedikit daripada metode kriptografi kunci publik lainnya seperti RSA atau Elgamal. Selain itu, ECC memberikan keamanan yang lebih baik untuk panjang kunci yang sama seperti algoritma yang terdaftar sebelumnya, sehingga Anda dapat menggunakan panjang kunci yang sama untuk keamanan yang lebih besar atau panjang kunci yang lebih rendah untuk keamanan yang sama seperti algoritma RSA dan Elgamal.

Skemanya adalah sebagai berikut secara umum.

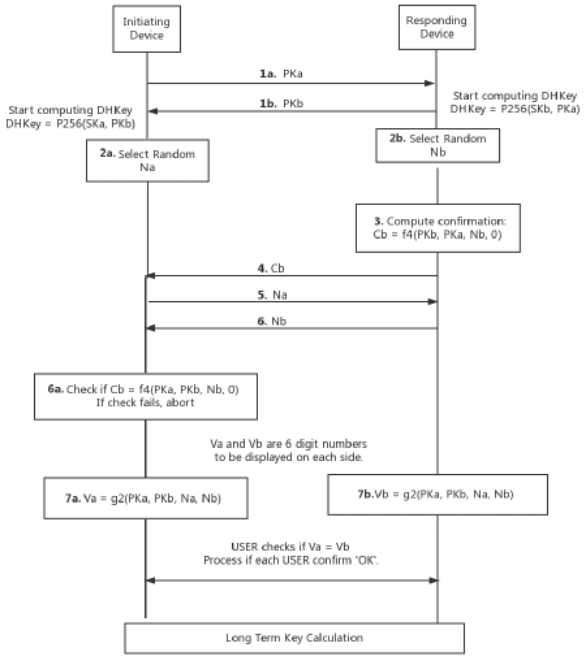
1. Buat koneksi dengan menggunakan ECDH.
2. Kunci yang diperoleh dari ECDH digunakan untuk mengenkripsi dan mendekripsi paket.

A. *Elliptic Curve Diffie Hellman*

Elliptic Curve Diffie Hellman (ECDH) adalah komponen kunci yang memungkinkan dua pihak pengirim dan penerima untuk bertukar kunci rahasia di saluran yang tidak aman, yang masing-masing memiliki sepasang kunci publik dan kunci pribadi dari kurva eliptik. Rahasia bersama ini dapat digunakan sebagai kunci secara langsung, atau lebih baik lagi, dapat digunakan untuk menghasilkan kunci lain yang dapat digunakan untuk mengenkripsi komunikasi berikutnya menggunakan cipher kunci simetris. Ini adalah variasi Diffie-Hellman yang menggunakan kriptografi kurva eliptik untuk membuat kunci yang sama. Katakanlah

Pengirim ingin membuat kunci bersama dengan Penerima, tetapi satu-satunya saluran mereka rentan terhadap penyadapan pihak ketiga. Parameter domain pertama-tama harus ditentukan (yaitu (p, a, b, G, n, h) dalam kasus prima atau (m, f(x), a, b, G, n, h) dalam kasus biner). Selanjutnya, setiap pihak harus memiliki pasangan kunci kurva eliptik yang terdiri dari kunci privat d: (bilangan bulat yang dipilih secara acak dalam interval [1 n - 1]) dan kunci publik Q (di mana Q = DG). Biarkan pasangan kunci Pengirim adalah (dA, QA), sedangkan pasangan kunci Penerima adalah (dB, QB). Masing-masing pihak harus memiliki kunci publik pihak lain (pertukaran harus terjadi). (xk, yk) dAQB = dihitung oleh pengirim. k = dBQA dihitung oleh penerima. xk adalah kunci berbagi (x-koordinat titik)

Karena dAQB = dAdBG = dBdAG = dBQA, kedua sisi menghitung jumlah yang sama. Tidak ada yang terungkap (menyimpan kunci publik, yang tidak rahasia), dan tidak ada pihak yang dapat menyimpulkan kunci pribadi pihak lain sampai memecahkan Masalah prosesor aritmatika Kurva Logaritma Diskrit. Kunci publik dapat berupa statis (dan karenanya tepercaya) atau fana (dan karenanya tidak tepercaya). Kunci pendek tidak perlu diautentikasi, jadi jika Anda ingin otentikasi, Anda harus mendapatkannya dengan cara lain. Kunci publik statis tidak memiliki kualitas keamanan tingkat lanjut seperti kerahasiaan tingkat lanjut dan resistensi peniruan kompromi kunci. Untuk menghindari kebocoran informasi tentang kunci privat statis, pemegang kunci privat statis harus memvalidasi kunci publik lainnya dan menerapkan fungsi derivasi kunci Diffie-Hellman standar untuk bertukar rahasia. Lihat ECMQV untuk skema dengan fitur keamanan ekstra.



`Gambar IV.1 Proses Elliptic Curve Dilfie Hellman menggunakan kurva P-256. [3]

B. Inisiasi Koneksi

Secara default, jalur komunikasi aplikasi *chatting* mengirimkan data dengan cara yang tidak aman. Diperlukan metode untuk mengamankan data sensitif. Akibatnya, penggunaan ECC sebagai mekanisme enkripsi untuk data yang disampaikan melalui paket data diusulkan dalam penelitian ini. Pendekatan ini dimaksudkan untuk bekerja dengan baik pada perangkat pengguna karena kebutuhan komputasi ECC lebih rendah daripada algoritma kunci publik lainnya. ECDH yang digunakan untuk menukar kunci brankas dan kunci pembangkit. Karena untuk mengoptimasikan pengiriman data antar perangkat digital dengan mengecilkan data yang akan dikirimkan sehingga proses transmisi dapat berlangsung dalam waktu yang lebih singkat, maka ukuran paket dibatasi hingga 20 byte atau 160 bit. Karena kunci 160 bit yang panjang dipilih, satu standar yang dapat digunakan untuk menghasilkan kunci adalah standar SECP160k2, yang memiliki variabel berikut.

A = 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFAC70
B = 0xB4E134D3FB59EB8BAB57274904664D5AF50388BA
P = 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFAC73
G = (0x52DCB034293A117E1F4FF11B30F7199D3144CE6D, 0xFEAFFEF2E331F296E071FA0DF9982CFEA7D43F2E)
n = (0x0100000000000000000351EE786A818F3A1A16B)
h = 1

V. KESIMPULAN

Dibandingkan dengan metode kunci publik generasi pertama (RSA dan Diffie-Hellman). Elliptic Curve Cryptography (ECC) memberikan lebih banyak keamanan dan lebih efisien dalam hal penggunaan. Kurva eliptik alternatif untuk keuntungan komputasi dan konsumsi jaringan dengan tingkat keamanan yang mirip dengan RSA dan Diffie Hellman harus dipertimbangkan secara aktif oleh produsen yang ingin meningkatkan sistem mereka. Secara default, jalur komunikasi aplikasi *chatting* mengirimkan data dengan cara yang tidak aman. Diperlukan metode untuk mengamankan data sensitif. Akibatnya, penggunaan ECC sebagai mekanisme enkripsi untuk data yang disampaikan melalui paket data diusulkan dalam penelitian ini. Pendekatan ini dimaksudkan untuk bekerja dengan baik pada perangkat pengguna karena kebutuhan komputasi ECC lebih rendah daripada algoritma kunci publik lainnya. Elliptic Curve Cryptography (ECC) adalah pendekatan kriptografi asimetris lain yang mengenkripsi dan mendekripsi data menggunakan dua kunci berbeda. Kunci pribadi yang digunakan untuk enkripsi data dan kunci publik yang digunakan untuk dekripsi data adalah dua kunci. Algoritma enkripsi kunci publik lainnya, seperti RSA atau Elgamal, membutuhkan daya komputasi yang lebih sedikit. Lebih lanjut, ECC memberikan keamanan yang lebih baik untuk panjang kunci yang sama seperti algoritma yang terdaftar sebelumnya, sehingga Anda dapat

menggunakan panjang kunci yang sama untuk keamanan yang lebih besar atau panjang kunci yang lebih rendah untuk keamanan yang sama dengan algoritma RSA dan Elgamal.

REFERENCES

[1] L. . Harnaningrum and F. W. Nurwiyati, "Komunikasi Data Mobile Device Dengan Near Field Communication," in *Seminar Nasional SRITI*, 2016, pp. 164–169.

[2] S. A. Mulia, I. T. Bandung, and J. G. Bandung, "Penggunaan Elliptic Curve Cryptography pada Enkripsi Paket Bluetooth Low Energy," 2021, vol. 1.

[3] T. S. Sollu, "Aplikasi dan Tinjauan Teknis Bluetooth Untuk Komunikasi Tanpa Kabel," *SMARTek*, no. Vol 4, No 4 (2006), 2016, [Online]. Available: http://jurnal.untad.ac.id/jurnal/index.php/SMARTEK/article/view/447.

[4] Rahmad Yesa Surya, "Enkripsi Asimetris Pada Transfer Data Antar Perangkat IoT Menggunakan Protokol HTTP dan MQTT," 2020, vol. 6.

[5] A. H. A. Alfarjat, J. Hanumanthappa, and H. S. A. Hamatta, "Implementation of Bluetooth Secure Simple Pairing (SSP) using Elliptic Curve Cryptography (ECC)," *Int. J. Comput. Sci. Netw. Secur.*, vol. 21, no. 3, pp. 60–70, 2021.

[6] B. Daryatmo, "Implementasi Bluetooth Instant Messaging Pada Perangkat Seluler," 2017, vol. 3, pp. 1–8.

[7] E. I. Sari, "Perancangan Aplikasi Kriptografi Asimetris Dengan Menerapkan Metode Elliptic Curve Cryptography," in *MEANS (Media Informasi Analisa dan Sistem)*, 2018, vol. 3, no. 1, pp. 24–28, [Online]. Available: http://dx.doi.org/10.54367/means.v3i1.221.

[8] Ahmad Kamsyakawuni, Ahmad Husnan Fanani, and Abduh Riski, "Pengamanan Citra Dengan Algoritma Diffie-Hellman Dan Algoritma Simplified Data Encryption Standard (S-Des)", Jurnal Ilmiah Matematika dan Pendidikan Matematika (JMP), vol. 10, no. 2, pp. 63-80, Dec 2018.

[9] Moch. Bahrul Ulum, "Aplikasi Chatting Menggunakan Kriptografi Berbasis Android", Jurnal Mahasiswa Teknik Informatika, vol. 1, no. 1, Mar 2017.

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, 25 Mei 2022

Muhammad Reza Nur Fauzi (18219064)