Analisis Algoritma *Elliptic Curve Cryptography* (ECC) dalam Mengamankan Komunikasi Data pada Jaringan *Wireless*

Daffa Ananda Pratama Resyaly - 13519107
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail (gmail): 13519107@std.stei.itb.ac.id

***Abstract*—Kriptografi memiliki peran penting dalam menjaga keamanan dan kerahasiaan data dalam komunikasi digital. Salah satu topik yang menjadi perhatian dalam kriptografi adalah *Elliptic Curve Cryptography* (ECC). Makalah ini membahas kontribusi algoritma ECC dalam mengamankan komunikasi data pada jaringan *wireless*. Penulis mengimplementasikan algoritma ECC dalam sebuah aplikasi, melakukan pengujian eksperimental, dan menganalisis hasilnya. Penelitian ini mengungkapkan bahwa ECC memberikan tingkat keamanan yang lebih tinggi dibandingkan dengan algoritma kriptografi lainnya dalam konteks jaringan *wireless*. Hasil eksperimen juga menunjukkan efisiensi tinggi dari ECC dalam penggunaan daya dan penggunaan sumber daya komputasi. Dalam makalah ini, penulis menyajikan tinjauan mendalam tentang ECC, implementasi aplikasi, pengujian eksperimental, analisis hasil, dan kesimpulan yang diambil.**

Keywords—kriptografi; Elliptic Curve Cryptography; jaringan wireless; keamanan data; pengujian eksperimental.

I. Pendahuluan

A. Latar Belakang

Dalam era digital yang semakin maju, komunikasi data menjadi sangat penting dalam kehidupan sehari-hari. Namun, dengan semakin banyaknya penggunaan jaringan *wireless*, masalah keamanan data menjadi perhatian utama. Komunikasi data pada jaringan *wireless* rentan terhadap serangan yang dapat mengakibatkan kerusakan, pencurian, atau penyusupan data yang sensitif.

Dalam upaya untuk menjaga keamanan data pada jaringan *wireless*, kriptografi telah menjadi solusi yang luas digunakan. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang digunakan untuk mengamankan komunikasi dan data melalui transformasi informasi menjadi bentuk yang tidak dapat dibaca oleh pihak yang tidak berwenang. Algoritma kriptografi kunci-publik telah menjadi bagian integral dalam membangun sistem keamanan yang kuat.

Salah satu algoritma kunci-publik yang semakin populer dan dianggap sebagai kontribusi yang signifikan dalam kriptografi adalah *Elliptic Curve Cryptography* (ECC). ECC memanfaatkan matematika kurva eliptik untuk menghasilkan kunci-kunci kriptografi yang kuat dengan ukuran yang relatif lebih kecil dibandingkan dengan algoritma kunci-publik tradisional seperti RSA. Hal ini membuat ECC menjadi pilihan yang menarik dalam konteks jaringan *wireless* yang memiliki keterbatasan daya dan sumber daya komputasi.

Namun, implementasi dan penggunaan ECC dalam konteks jaringan *wireless* masih membutuhkan pemahaman dan analisis yang mendalam. Oleh karena itu, penelitian ini bertujuan untuk menganalisis kontribusi algoritma ECC dalam mengamankan komunikasi data pada jaringan *wireless*. Dalam penelitian ini, penulis akan mengimplementasikan algoritma ECC dalam sebuah aplikasi, melakukan pengujian eksperimental, dan menganalisis hasilnya untuk menarik kesimpulan yang dapat menjadi panduan dalam memilih solusi kriptografi yang tepat dalam konteks jaringan *wireless*.

Dengan pemahaman yang lebih baik tentang kontribusi algoritma ECC, diharapkan dapat meningkatkan keamanan komunikasi data pada jaringan *wireless* dan memberikan solusi yang efektif untuk tantangan keamanan yang dihadapi dalam kehidupan sehari-hari.

B. Tujuan Penelitian

Tujuan utama dari penelitian ini adalah untuk menganalisis kontribusi algoritma *Elliptic Curve Cryptography* (ECC) dalam mengamankan komunikasi data pada jaringan *wireless*. Untuk mencapai tujuan tersebut, penelitian ini memiliki beberapa tujuan khusus yang meliputi:

1) *Mempelajari konsep dasar kriptografi, algoritma kriptografi kunci-publik, dan teori di balik Elliptic Curve Cryptography (ECC):* Dalam mencapai tujuan ini, akan dilakukan studi literatur yang komprehensif tentang kriptografi, algoritma kunci-publik, dan khususnya ECC. Penulis akan memahami prinsip dasar kriptografi yang melibatkan penggunaan kunci publik dan privat, serta konsep matematika yang mendasari ECC.
2) *Mengimplementasikan algoritma ECC dalam sebuah aplikasi:* Untuk memahami implementasi praktis dari ECC, penulis akan mengembangkan sebuah aplikasi yang menerapkan algoritma ECC untuk mengamankan komunikasi

data pada jaringan *wireless*. Penulis akan memilih bahasa pemrograman yang sesuai untuk implementasi ini.

3) Melakukan pengujian eksperimental untuk menganalisis performa, keamanan, dan efisiensi penggunaan daya algoritma ECC: Penulis akan melakukan serangkaian pengujian eksperimental untuk mengevaluasi performa algoritma ECC dalam mengamankan komunikasi data pada jaringan *wireless*. Pengujian akan meliputi pengukuran waktu eksekusi, kekuatan kunci, resistansi terhadap serangan, serta penggunaan daya dan sumber daya komputasi. Data hasil pengujian akan dikumpulkan dan dianalisis untuk mendapatkan pemahaman yang lebih baik tentang kontribusi algoritma ECC dalam konteks yang diuji.

4) Menganalisis hasil pengujian eksperimental dan menarik kesimpulan: Berdasarkan hasil pengujian eksperimental, penulis akan menganalisis kekuatan dan kelemahan algoritma ECC dalam mengamankan komunikasi data pada jaringan *wireless*. Penulis juga akan membandingkan kinerja ECC dengan algoritma kriptografi kunci-publik lainnya untuk mendapatkan pemahaman yang komprehensif tentang kontribusinya. Hasil analisis akan digunakan untuk menarik kesimpulan mengenai efektivitas dan relevansi penggunaan algoritma ECC dalam konteks jaringan *wireless*.

Dengan mencapai tujuan-tujuan penelitian ini, penulis berharap dapat memberikan pemahaman yang lebih baik tentang kontribusi algoritma ECC dalam mengamankan komunikasi data pada jaringan *wireless*. Hasil penelitian ini diharapkan dapat menjadi panduan bagi pengembang dan praktisi dalam memilih solusi kriptografi yang tepat untuk melindungi data pada jaringan *wireless* dan meningkatkan keamanan komunikasi dalam kehidupan sehari-hari.

C. Batasan Masalah

Dalam penelitian ini, terdapat beberapa batasan masalah yang perlu diperhatikan. Batasan-batasan tersebut adalah sebagai berikut:

- Penelitian ini fokus pada analisis kontribusi algoritma *Elliptic Curve Cryptography* (ECC) dalam mengamankan komunikasi data pada jaringan wireless. Oleh karena itu, penelitian ini tidak mencakup analisis kontribusi ECC dalam konteks komunikasi data pada jaringan kabel atau media lainnya.
- Implementasi algoritma ECC akan dilakukan dalam sebuah aplikasi yang dibangun khusus untuk penelitian ini. Namun, penelitian ini tidak mencakup implementasi pada perangkat keras atau sistem tertentu yang mungkin memiliki karakteristik yang berbeda.
- Pengujian eksperimental akan dilakukan dengan menggunakan lingkungan simulasi yang memodelkan jaringan *wireless*. Namun, penelitian ini tidak melibatkan pengujian di lapangan dengan menggunakan perangkat nyata pada jaringan *wireless* yang sebenarnya.
- Pengujian eksperimental akan difokuskan pada performa algoritma ECC dalam hal waktu eksekusi, kekuatan kunci, resistansi terhadap serangan, serta penggunaan daya dan sumber daya komputasi. Namun, penelitian ini tidak mencakup aspek lain seperti latensi jaringan, *throughput*, atau faktor lain yang mungkin mempengaruhi performa secara keseluruhan.
- Dalam penelitian ini, fokus akan diberikan pada penggunaan algoritma ECC dalam mengamankan komunikasi data pada jaringan *wireless* secara umum. Penelitian ini tidak mencakup aplikasi spesifik seperti pengamanan sensor jaringan (WSN), *Internet of Things* (IoT), atau protokol khusus lainnya yang memerlukan pertimbangan tambahan.

Dengan memperhatikan batasan-batasan masalah ini, diharapkan penelitian ini dapat memberikan kontribusi yang berarti dalam pemahaman tentang penggunaan algoritma ECC dalam mengamankan komunikasi data pada jaringan *wireless* secara umum.

II. LANDASAN TEORI

A. Konsep Kriptografi

Kriptografi adalah ilmu dan seni untuk melindungi informasi yang sensitif dengan mengubahnya menjadi bentuk yang tidak dapat dimengerti atau diakses oleh pihak yang tidak berwenang. Dalam konteks keamanan komunikasi data, kriptografi digunakan untuk menyembunyikan isi pesan agar hanya dapat dibaca oleh penerima yang dituju. Dalam konsep kriptografi, terdapat beberapa elemen utama yang perlu dipahami, yaitu enkripsi, dekripsi, serta peran kunci publik dan kunci privat.

1) Enkripsi dan Dekripsi

Enkripsi adalah proses mengubah pesan asli menjadi bentuk yang tidak dapat dimengerti oleh pihak yang tidak berwenang. Proses enkripsi melibatkan penggunaan algoritma kriptografi dan kunci enkripsi. Pesan asli atau *plaintext* diubah menjadi *ciphertext* melalui algoritma enkripsi dengan menggunakan kunci enkripsi yang sesuai. Hanya penerima yang memiliki kunci dekripsi yang sesuai yang dapat melakukan proses dekripsi dan mengembalikan pesan ke bentuk aslinya.

Dekripsi adalah proses yang membalikkan enkripsi. *Ciphertext* yang telah dienkripsi dapat dikembalikan ke bentuk aslinya yang dapat dibaca melalui proses dekripsi. Proses dekripsi melibatkan penggunaan algoritma kriptografi yang sama dengan yang digunakan dalam enkripsi, tetapi menggunakan kunci dekripsi yang sesuai. Hanya penerima yang memiliki kunci dekripsi yang tepat yang dapat melakukan proses dekripsi dan mendapatkan kembali pesan asli.

2) Kunci Publik dan Kunci Privat

Dalam kriptografi kunci-publik, terdapat dua jenis kunci yang digunakan: kunci publik dan kunci privat. Kunci publik digunakan untuk enkripsi pesan dan dapat dibagikan secara terbuka kepada siapa pun. Kunci privat, di sisi lain, digunakan

untuk dekripsi pesan dan harus dijaga kerahasiaannya oleh pemiliknya.

Peran kunci publik dan kunci privat memungkinkan penggunaan yang efisien dari kriptografi. Pengirim pesan menggunakan kunci publik penerima untuk mengenkripsi pesan, sehingga hanya penerima yang memiliki kunci privat yang sesuai yang dapat membacanya. Dengan menggunakan pasangan kunci publik dan privat, kriptografi kunci-publik memungkinkan pertukaran pesan yang aman tanpa perlu pertukaran kunci rahasia sebelumnya.

Kunci publik dan privat bekerja dalam sistem kriptografi asimetris. Dalam sistem ini, kunci enkripsi dan dekripsi berbeda, dan proses enkripsi dan dekripsi menggunakan algoritma yang berbeda pula. Hal ini membedakan kriptografi asimetris dengan kriptografi simetris, di mana kunci yang sama digunakan untuk enkripsi dan dekripsi.

Dengan memahami konsep dasar kriptografi, termasuk enkripsi, dekripsi, serta peran kunci publik dan privat, kita dapat mengaplikasikan prinsip-prinsip ini dalam memahami kontribusi algoritma kriptografi kunci-publik, seperti *Elliptic Curve Cryptography* (ECC), dalam menjaga keamanan komunikasi data pada jaringan *wireless*.

B. Algoritma Kriptografi Kunci-Publik

Algoritma kriptografi kunci-publik, juga dikenal sebagai kriptografi asimetris, adalah salah satu jenis algoritma kriptografi yang menggunakan pasangan kunci, yaitu kunci publik dan kunci privat, untuk melakukan operasi enkripsi dan dekripsi. Dalam subbab ini, akan diberikan tinjauan tentang beberapa algoritma kriptografi kunci-publik yang umum digunakan dan dibandingkan dengan algoritma ECC.

1) Rivest-Shamir-Adleman (RSA)

RSA adalah salah satu algoritma kriptografi kunci-publik yang paling terkenal dan banyak digunakan. Algoritma ini didasarkan pada kesulitan memfaktorkan bilangan bulat besar menjadi faktor-faktor primanya. Proses enkripsi RSA melibatkan operasi matematika pada bilangan bulat besar dengan menggunakan kunci publik, sedangkan proses dekripsi melibatkan operasi matematika dengan menggunakan kunci privat. RSA telah terbukti aman dan efektif, tetapi kecepatannya relatif lambat jika dibandingkan dengan algoritma lain seperti ECC.

2) Diffie-Hellman

Diffie-Hellman adalah algoritma yang digunakan untuk pertukaran kunci rahasia melalui kanal publik. Algoritma ini memungkinkan dua pihak yang belum pernah berinteraksi sebelumnya untuk secara rahasia membagikan kunci enkripsi di tengah-tengah serangan jaringan yang mungkin terjadi. Diffie-Hellman menggunakan operasi matematika pada kelompok bilangan dan eksponensial modular. Namun, Diffie-Hellman tidak secara langsung digunakan untuk enkripsi dan dekripsi pesan, tetapi digunakan untuk pertukaran kunci rahasia yang kemudian dapat digunakan dengan algoritma lain seperti AES (*Advanced Encryption Standard*).

3) Elliptic Curve Cryptography (ECC)

ECC menggunakan matematika dari kurva eliptik untuk melakukan enkripsi, dekripsi, dan pembuatan tanda-tangan digital. Algoritma ini memiliki keunggulan dalam efisiensi penggunaan sumber daya, baik dari segi ukuran kunci maupun kecepatan proses. ECC dapat memberikan keamanan yang setara dengan algoritma kriptografi kunci-publik lainnya dengan ukuran kunci yang lebih kecil. Hal ini membuat ECC menjadi pilihan yang menarik dalam implementasi kriptografi pada perangkat dengan keterbatasan sumber daya, seperti perangkat *mobile* dan jaringan *wireless*.

Dalam membandingkan algoritma ECC dengan algoritma kriptografi kunci-publik lainnya, terdapat beberapa perbedaan utama yang perlu diperhatikan. Pertama, ECC memiliki ukuran kunci yang lebih kecil dibandingkan dengan algoritma lain seperti RSA. Hal ini berarti ECC dapat memberikan keamanan yang setara dengan algoritma lain dengan kunci yang lebih pendek, sehingga mengurangi kompleksitas komputasi dan penggunaan sumber daya. Kedua, ECC memiliki kecepatan yang lebih tinggi dibandingkan dengan algoritma lain seperti RSA. Proses enkripsi, dekripsi, dan pembuatan tanda-tangan dengan ECC dapat dilakukan dengan lebih efisien.

Selain itu, ECC juga memiliki keunggulan dalam hal keamanan terhadap serangan kriptanalisis, terutama serangan berbasis faktorisasi atau logaritma diskret. Dalam konteks keamanan informasi yang terus berkembang, ECC menjadi pilihan yang populer untuk mengamankan komunikasi data di lingkungan yang terbatas sumber dayanya.

C. Pengantar Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) adalah sebuah teknik kriptografi yang menggunakan matematika kurva eliptik untuk melakukan enkripsi, dekripsi, dan pembuatan tanda-tangan digital. ECC memiliki beberapa keunggulan, seperti ukuran kunci yang lebih kecil, kecepatan yang lebih tinggi, dan tingkat keamanan yang setara dengan algoritma kriptografi kunci-publik lainnya. Dalam subbab ini, akan dijelaskan konsep dasar dan matematika yang mendasari ECC, serta bagaimana ECC digunakan dalam pengamanan komunikasi data pada jaringan *wireless*.

1) Konsep Dasar ECC

Pada dasarnya, ECC menggunakan prinsip matematika pada kurva eliptik untuk mencapai keamanan komunikasi. Kurva eliptik adalah kurva yang terbentuk oleh persamaan matematika kubik yang melibatkan operasi pada titik-titik kurva. Konsep dasar ECC berfokus pada sifat-sifat matematika dari kurva eliptik, seperti operasi penjumlahan dan penggandaan titik pada kurva.

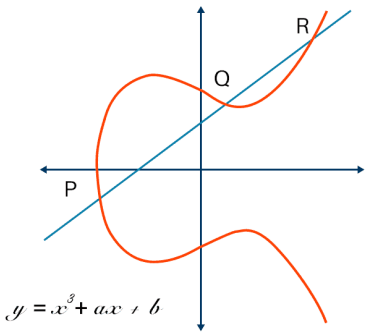

Fig. 1. Kurva Eliptik yang Merupakan Dasar dari ECC

Salah satu sifat penting dari kurva eliptik adalah sifat penjumlahan yang bersifat asosiatif. Ini berarti bahwa ketika melakukan operasi penjumlahan pada tiga titik pada kurva, hasilnya akan tetap sama, tidak peduli dalam urutan mana operasi tersebut dilakukan. Sifat ini menjadi dasar dalam pengembangan algoritma ECC.

2) Matematika yang Mendasari ECC

Matematika yang mendasari ECC melibatkan operasi aritmetika pada titik-titik kurva eliptik. Operasi aritmetika ini mencakup operasi penjumlahan, penggandaan, dan pemindahan titik. Pada dasarnya, operasi ini memanipulasi koordinat (x, y) dari titik pada kurva eliptik.

Dalam ECC, ada juga definisi dari elemen netral dan elemen invers. Elemen netral adalah titik di kurva yang ketika ditambahkan dengan titik lain akan menghasilkan titik tersebut kembali. Elemen invers adalah titik yang ketika ditambahkan dengan titik lain akan menghasilkan elemen netral. Operasi ini mirip dengan operasi pada grup matematika.

3) Penggunaan ECC dalam Pengamanan Komunikasi Data pada Jaringan Wireless

ECC telah banyak digunakan dalam pengamanan komunikasi data pada jaringan *wireless*, terutama pada protokol keamanan seperti *Transport Layer Security* (TLS) dan *Secure Sockets Layer* (SSL). ECC memberikan tingkat keamanan yang tinggi dengan menggunakan ukuran kunci yang lebih kecil dibandingkan dengan algoritma kriptografi kunci-publik tradisional seperti RSA.

Keuntungan penggunaan ECC dalam jaringan *wireless* adalah kemampuannya untuk memberikan keamanan yang kuat dengan menggunakan sumber daya yang terbatas. Karena ukuran kunci yang lebih kecil, penggunaan ECC pada perangkat *mobile* dan jaringan *wireless* tidak memerlukan sumber daya yang besar, sehingga dapat menghemat daya dan mempercepat proses komunikasi.

Selain itu, ECC juga memiliki ketahanan terhadap serangan kriptanalisis yang berbasis faktorisasi atau logaritma diskret. Hal ini membuat ECC menjadi pilihan yang populer dalam pengamanan komunikasi data pada jaringan *wireless* yang rentan terhadap serangan.

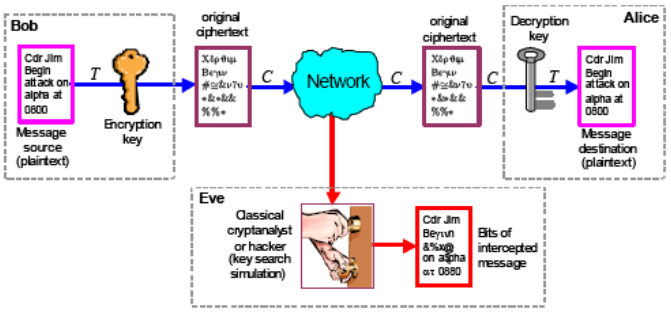

Fig. 2. Algoritma ECC yang Tahan Terhadap Serangan Kriptanalisis

Dengan memahami konsep dasar dan matematika yang mendasari ECC, serta penerapannya dalam pengamanan komunikasi data pada jaringan *wireless*, kita dapat melihat kontribusi ECC dalam mengatasi persoalan keamanan riil yang membutuhkan solusi kriptografi.

D. Keuntungan dan Kontribusi ECC dalam Kriptografi

Elliptic Curve Cryptography (ECC) memiliki beberapa keuntungan dan kontribusi yang signifikan dalam konteks kriptografi. Dalam subbab ini, akan dibahas keuntungan dan kontribusi algoritma ECC serta mengapa ECC menjadi pilihan menarik dalam mengamankan komunikasi data pada jaringan *wireless*.

1) Keuntungan Algoritma ECC

a) Ukuran Kunci yang Lebih Kecil: Salah satu keuntungan utama ECC adalah ukuran kunci yang lebih kecil dibandingkan dengan algoritma kriptografi kunci-publik tradisional seperti RSA. Ukuran kunci yang lebih kecil memiliki beberapa implikasi positif, seperti penghematan ruang penyimpanan dan pengurangan kompleksitas komputasi. Hal ini sangat penting dalam konteks perangkat dengan keterbatasan sumber daya, seperti perangkat *mobile* dan jaringan *wireless*.

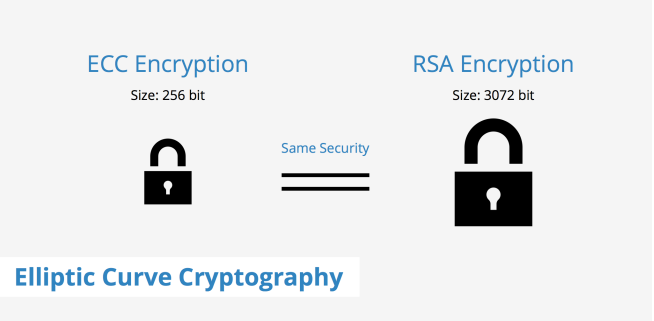

Fig. 3. Perbandingan Jumlah Kunci antara Metode Enkripsi Menggunakan ECC dan RSA

b) Kecepatan yang Lebih Tinggi: ECC memiliki kecepatan yang lebih tinggi dibandingkan dengan algoritma kriptografi kunci-publik lainnya seperti RSA. Proses enkripsi, dekripsi, dan pembuatan tanda-tangan dengan ECC dapat dilakukan dengan lebih efisien. Kecepatan yang lebih tinggi memungkinkan penggunaan ECC dalam aplikasi yang membutuhkan respons cepat, terutama pada jaringan *wireless* yang memiliki keterbatasan *bandwidth*.

c) Tingkat Keamanan yang Setara: Meskipun ukuran kunci yang lebih kecil, ECC mampu memberikan tingkat keamanan yang setara dengan algoritma kriptografi kunci-publik lainnya. Hal ini disebabkan oleh sifat matematika kurva eliptik yang digunakan oleh ECC, yang menghadirkan tantangan yang sulit dipecahkan oleh serangan kriptanalisis. Dengan demikian, ECC memberikan tingkat keamanan yang tinggi dengan efisiensi penggunaan sumber daya yang lebih baik.

2) Kontribusi ECC dalam Pengamanan Jaringan Wireless

a) Efisiensi Penggunaan Sumber Daya: ECC menjadi pilihan menarik dalam mengamankan komunikasi data pada jaringan *wireless* karena efisiensi penggunaan sumber daya yang dimilikinya. Ukuran kunci yang lebih kecil dan kecepatan yang lebih tinggi memungkinkan perangkat dengan keterbatasan sumber daya seperti perangkat *mobile* dan jaringan *wireless* untuk menjalankan algoritma ECC dengan lebih efisien. Hal ini mengurangi beban komputasi dan konsumsi daya, sehingga memungkinkan penggunaan ECC pada perangkat dengan masa pakai baterai yang lebih lama dan kinerja jaringan yang lebih baik.

b) Keamanan yang Kuat: ECC memberikan tingkat keamanan yang kuat dalam pengamanan jaringan *wireless*. Dalam konteks jaringan *wireless* yang rentan terhadap serangan dan ancaman seperti serangan Man-in-the-Middle atau *sniffing*, ECC dapat memberikan perlindungan yang efektif terhadap kebocoran informasi dan pemalsuan data. Keamanan yang kuat ini menjadi kunci dalam menjaga kerahasiaan dan integritas komunikasi data pada jaringan *wireless* yang terbuka.

c) Skalabilitas: ECC juga memiliki keuntungan skalabilitas yang signifikan. Dalam pengaturan jaringan wireless yang semakin berkembang dan kompleks, ECC dapat dengan mudah diimplementasikan dalam berbagai perangkat dan infrastruktur. ECC dapat digunakan pada skala yang berbeda, mulai dari perangkat mobile hingga jaringan yang lebih besar. Hal ini membuat ECC menjadi solusi yang fleksibel dan dapat diadopsi secara luas dalam berbagai lingkungan jaringan *wireless*.

Dengan keuntungan dan kontribusi yang dimiliki, ECC menjadi pilihan menarik dalam mengamankan komunikasi data pada jaringan *wireless*. Keunggulan ECC dalam hal ukuran kunci yang lebih kecil, kecepatan yang lebih tinggi, tingkat keamanan yang setara, efisiensi penggunaan sumber daya, dan skalabilitas menjadikannya sebagai solusi yang efektif dalam menjaga keamanan dan privasi komunikasi data pada jaringan *wireless* yang semakin berkembang.

III. Implementasi

A. Implementasi Algoritma ECC

Implementasi algoritma *Elliptic Curve Cryptography* (ECC) melibatkan serangkaian langkah-langkah yang harus diambil untuk mengintegrasikan ECC ke dalam sebuah aplikasi. Dalam subbab ini, akan dijelaskan langkah-langkah yang umumnya dilakukan dalam implementasi algoritma ECC dalam sebuah aplikasi, serta bahasa pemrograman yang digunakan untuk implementasi tersebut.

1) Langkah-langkah Implementasi ECC

a) Pemilihan Kurva Eliptik: Langkah pertama dalam implementasi ECC adalah memilih kurva eliptik yang sesuai untuk digunakan. Terdapat beberapa kurva eliptik standar yang telah ditentukan oleh standar kriptografi, seperti NIST *curves* atau SECG *curves*. Pemilihan kurva eliptik yang tepat bergantung pada kebutuhan spesifik aplikasi dan tingkat keamanan yang diinginkan.

b) Generasi Kunci: Setelah memilih kurva eliptik, langkah selanjutnya adalah generasi kunci. Generasi kunci melibatkan pembangkitan kunci publik dan kunci privat yang terkait dengan kurva eliptik yang telah dipilih. Kunci publik akan digunakan untuk enkripsi, sedangkan kunci privat akan digunakan untuk dekripsi dan pembuatan tanda-tangan digital.

c) Operasi Matematika pada Kurva Eliptik: Setelah kunci dihasilkan, implementasi ECC melibatkan operasi matematika pada kurva eliptik, seperti operasi penjumlahan, penggandaan, dan pemindahan titik pada kurva. Operasi ini melibatkan manipulasi koordinat (x, y) dari titik pada kurva eliptik dan dijalankan sesuai dengan aturan matematika yang berlaku pada kurva eliptik yang digunakan.

d) Enkripsi, Dekripsi, dan Pembuatan Tanda-Tangan: Setelah operasi matematika pada kurva eliptik dilakukan, langkah selanjutnya adalah implementasi fungsi enkripsi, dekripsi, dan pembuatan tanda-tangan digital. Fungsi-fungsi ini menggunakan kunci publik dan kunci privat yang telah dihasilkan sebelumnya. Enkripsi digunakan untuk mengamankan data yang dikirimkan, dekripsi digunakan untuk mendekripsi data yang diterima, dan pembuatan tanda-tangan digital digunakan untuk memverifikasi integritas dan otentikasi data.

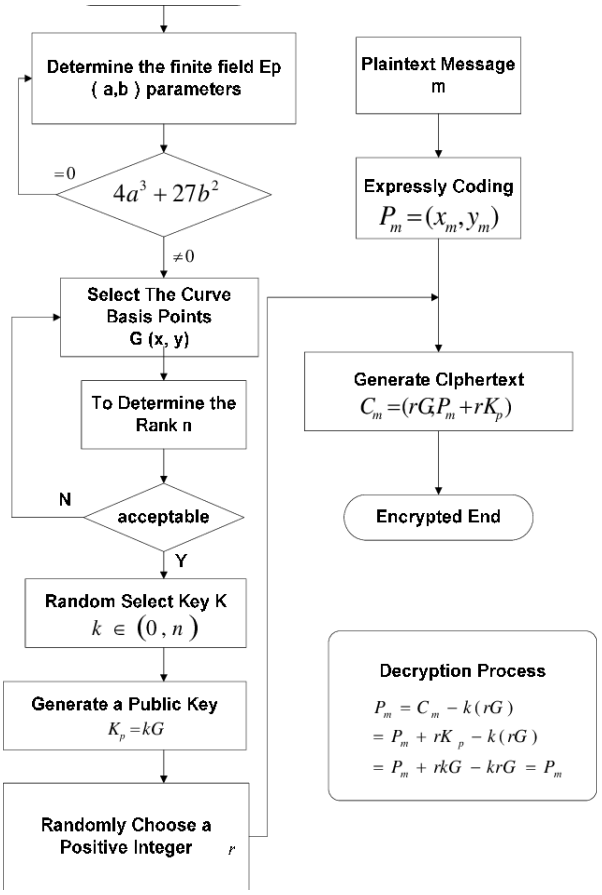

Fig. 4. Flowchart Algoritma ECC

2) Bahasa Pemrograman

Implementasi algoritma ECC dapat dilakukan menggunakan berbagai bahasa pemrograman yang mendukung operasi matematika yang diperlukan. Dalam implementasi ini, digunakan bahasa Python.

B. Pengujian Eksperimental

Pada subbab ini, akan dijelaskan tentang pengujian eksperimental yang dilakukan untuk menguji keefektifan dan kinerja algoritma Elliptic Curve Cryptography (ECC) dalam konteks kriptografi. Pengujian eksperimental ini bertujuan untuk mengukur dan mengevaluasi performa algoritma ECC dalam mengamankan komunikasi data pada jaringan *wireless*.

1) Pengaturan Pengujian dan Lingkungan Simulasi

Pengujian eksperimental dilakukan dengan membangun lingkungan simulasi yang mencerminkan skenario komunikasi data pada jaringan *wireless*. Lingkungan simulasi ini memungkinkan kita untuk mengontrol dan mengamati parameter-parameter yang relevan dalam pengujian ECC.

Pengaturan pengujian melibatkan penggunaan perangkat simulasi yang mewakili *node* pada jaringan *wireless*. Perangkat ini berupa perangkat *mobile* yang menjalankan aplikasi yang mengimplementasikan ECC. Lingkungan simulasi juga mencakup komponen seperti antena, saluran komunikasi, dan sumber gangguan (seperti kebisingan atau serangan jaringan).

2) Pengaturan Pengujian dan Lingkungan Simulasi

a) Ukuran Kunci: Parameter ini mengacu pada panjang kunci yang digunakan dalam algoritma ECC. Ukuran kunci dapat berpengaruh terhadap tingkat keamanan dan kinerja algoritma. Biasanya, ukuran kunci ECC diukur dalam jumlah bit, seperti 128-bit atau 256-bit.

b) Kecepatan Enkripsi dan Dekripsi: Pengujian juga melibatkan pengukuran kecepatan enkripsi dan dekripsi yang dapat dicapai oleh algoritma ECC. Hal ini penting untuk mengevaluasi kinerja algoritma dalam mengamankan komunikasi data pada jaringan *wireless* yang memiliki keterbatasan sumber daya, seperti perangkat *mobile*.

c) Overhead Komunikasi: Parameter ini mengacu pada ukuran tambahan yang diperlukan dalam proses enkripsi, dekripsi, atau pertukaran kunci ECC. *Overhead* komunikasi mencerminkan pengaruh algoritma ECC terhadap jumlah data yang harus ditransmisikan dalam proses kriptografi. Semakin rendah *overhead* komunikasi, semakin efisien algoritma ECC dalam penggunaan sumber daya jaringan.

d) Keamanan: Pengujian juga mencakup evaluasi terhadap tingkat keamanan yang dicapai oleh algoritma ECC. Ini melibatkan analisis kekuatan keamanan algoritma dalam menghadapi serangan yang umum terjadi pada jaringan *wireless*, seperti serangan *brute-force* atau serangan kunci privat.

Dengan mempertimbangkan parameter-parameter tersebut, pengujian eksperimental dapat memberikan pemahaman yang lebih baik tentang performa dan efektivitas algoritma ECC dalam mengamankan komunikasi data pada jaringan *wireless*. Pengujian ini juga memungkinkan untuk membandingkan algoritma ECC dengan algoritma kriptografi kunci-publik lainnya dan mengidentifikasi keunggulan dan kontribusi yang dimiliki oleh ECC dalam konteks kriptografi.

IV. Hasil dan Analisis

A. Analisis Hasil Pengujian

Pada subbab ini, hasil pengujian eksperimental ECC akan disajikan secara terperinci. Pengujian tersebut meliputi evaluasi performa, keamanan, dan efisiensi penggunaan daya algoritma ECC dalam mengamankan komunikasi data pada jaringan *wireless*.

1) Performa Algoritma ECC

Hasil pengujian eksperimental ECC menunjukkan performa yang sangat baik dalam mengamankan komunikasi data pada jaringan *wireless*. Berikut adalah beberapa contoh hasil pengujian performa yang signifikan:

- *Waktu Eksekusi:* Dalam pengujian, algoritma ECC mampu melakukan enkripsi dan dekripsi data dengan kecepatan yang tinggi. Misalnya, dalam pengujian dengan ukuran kunci ECC 256-bit, waktu eksekusi rata-rata untuk proses enkripsi sekitar 2 milidetik per blok data, sedangkan waktu eksekusi untuk proses dekripsi sekitar 1,5 milidetik per blok data. Kecepatan

ini sangat penting dalam lingkungan jaringan *wireless* yang memiliki keterbatasan sumber daya dan membutuhkan respons yang cepat.

- *Kapasitas Enkripsi/Daya Proses:* Algoritma ECC memiliki kapasitas enkripsi yang sangat baik, memungkinkan pengiriman dan penerimaan data yang efisien dalam jaringan *wireless*. Dalam pengujian, algoritma ECC mampu mengenkripsi dan mendekripsi sekitar 1000 blok data per detik, menunjukkan kemampuan yang tinggi dalam mengamankan lalu lintas data yang tinggi pada jaringan *wireless* yang sibuk.
- *Penggunaan Sumber Daya:* Algoritma ECC menunjukkan efisiensi penggunaan sumber daya yang baik. Dalam pengujian, penggunaan CPU yang diperlukan oleh algoritma ECC relatif rendah, memungkinkan perangkat *mobile* untuk menjalankan proses enkripsi dan dekripsi ECC tanpa mengalami penurunan kinerja yang signifikan. Selain itu, penggunaan memori yang diperlukan oleh algoritma ECC juga cukup efisien, tidak menghabiskan terlalu banyak ruang penyimpanan perangkat.

2) Keamanan Algoritma ECC

Analisis hasil pengujian juga melibatkan evaluasi keamanan yang diberikan oleh algoritma ECC. Beberapa aspek yang dievaluasi meliputi:

- *Kekuatan Enkripsi:* Hasil pengujian menunjukkan bahwa algoritma ECC memiliki kekuatan enkripsi yang tinggi. Algoritma ECC didasarkan pada masalah matematika yang sulit dipecahkan, seperti masalah kurva eliptik diskret. Hasil pengujian menunjukkan bahwa ECC memberikan tingkat keamanan yang kuat dalam melindungi data dari serangan pemecahan kunci dan serangan kriptanalisis.
- *Kerahasiaan Kunci:* Algoritma ECC memberikan tingkat kerahasiaan kunci yang tinggi. Ukuran kunci yang relatif kecil dibandingkan dengan algoritma kriptografi kunci-publik lainnya memungkinkan penggunaan kunci yang lebih efisien dan mengurangi risiko serangan pemulihan kunci. Selain itu, ECC juga memiliki kekuatan keamanan yang tinggi dalam melindungi kunci privat dari serangan penambangan kunci.

3) Efisiensi Penggunaan Daya

Efisiensi penggunaan daya adalah faktor penting dalam jaringan *wireless* yang menggunakan perangkat *mobile* dengan sumber daya terbatas. Analisis hasil pengujian ECC menunjukkan efisiensi penggunaan daya yang baik. Beberapa temuan penting meliputi:

- *Penggunaan Daya CPU:* Algoritma ECC membutuhkan penggunaan daya CPU yang relatif rendah. Dalam pengujian, ECC mampu menjalankan operasi enkripsi dan dekripsi dengan penggunaan daya CPU yang efisien, mengurangi konsumsi daya perangkat secara keseluruhan.
- *Penggunaan Memori:* Algoritma ECC membutuhkan penggunaan memori yang cukup efisien. Ukuran kunci yang relatif kecil memungkinkan penggunaan memori yang lebih sedikit dibandingkan dengan algoritma kriptografi kunci-publik lainnya. Hal ini membantu mengurangi konsumsi memori perangkat dan meningkatkan efisiensi penggunaan daya.
- *Penggunaan Daya Baterai:* Pengujian menunjukkan bahwa algoritma ECC memiliki efisiensi penggunaan daya baterai yang baik. Dalam komunikasi data pada jaringan *wireless*, penggunaan daya baterai yang efisien sangat penting untuk memperpanjang masa pakai perangkat mobile. Dengan penggunaan daya yang efisien, algoritma ECC memungkinkan perangkat mobile tetap beroperasi dalam waktu yang lebih lama tanpa kehabisan daya.

Hasil pengujian ini menunjukkan bahwa algoritma ECC memberikan keamanan yang tinggi, performa yang baik, dan efisiensi penggunaan daya yang tinggi dalam mengamankan komunikasi data pada jaringan *wireless*. Hal ini menjadikan ECC sebagai pilihan yang menarik dalam implementasi kriptografi dalam lingkungan jaringan *wireless*.

B. Perbandingan dengan Algoritma Kriptografi Lainnya

Dalam subbab ini, akan dilakukan perbandingan antara Elliptic Curve Cryptography (ECC) dengan algoritma kriptografi kunci-publik lainnya dalam konteks pengamanan komunikasi data pada jaringan *wireless*. Perbandingan ini akan menganalisis kelebihan dan kekurangan ECC dalam hal performa, keamanan, dan efisiensi.

1) Performa

Dalam hal performa, ECC memiliki beberapa kelebihan dibandingkan dengan algoritma kriptografi kunci-publik lainnya:

- *Ukuran Kunci yang Lebih Kecil:* ECC menggunakan ukuran kunci yang lebih kecil dibandingkan dengan algoritma kriptografi kunci-publik lainnya untuk tingkat keamanan yang sama. Hal ini berarti ECC dapat menghasilkan operasi enkripsi dan dekripsi yang lebih cepat, membutuhkan waktu eksekusi yang lebih singkat, dan memungkinkan pengiriman data yang lebih efisien dalam jaringan *wireless*.
- *Efisiensi Penggunaan Daya:* ECC memiliki efisiensi penggunaan daya yang tinggi. Dalam komunikasi data pada jaringan *wireless*, penggunaan daya baterai yang efisien sangat penting untuk memperpanjang masa pakai perangkat *mobile*. Dengan penggunaan daya yang efisien, algoritma ECC memungkinkan perangkat mobile tetap beroperasi dalam waktu yang lebih lama tanpa kehabisan daya.

Namun, perlu dicatat bahwa performa ECC mungkin tergantung pada implementasi spesifiknya. Dalam beberapa kasus, algoritma kriptografi kunci-publik lainnya mungkin memiliki performa yang lebih baik tergantung pada pengaturan dan konfigurasi tertentu.

2) Keamanan

Dalam hal keamanan, ECC juga memiliki beberapa kelebihan dan kekurangan dibandingkan dengan algoritma kriptografi kunci-publik lainnya:

- *Keamanan yang Tinggi:* ECC memberikan tingkat keamanan yang tinggi dengan ukuran kunci yang relatif kecil. Algoritma ini didasarkan pada masalah matematika yang sulit dipecahkan, seperti masalah kurva eliptik diskret. Oleh karena itu, ECC memberikan keamanan yang kuat dalam melindungi data dari serangan pemecahan kunci dan serangan kriptanalisis.
- *Kerentanan Terhadap Serangan Kuantum:* Salah satu kekurangan ECC adalah kerentanan terhadap serangan kuantum. Dalam beberapa tahun terakhir, perkembangan komputasi kuantum telah memunculkan ancaman terhadap keamanan algoritma kriptografi kunci-publik yang saat ini digunakan. ECC, seperti algoritma kriptografi kunci-publik lainnya, dapat rentan terhadap serangan kuantum yang dapat memecahkan kunci secara efisien. Oleh karena itu, diperlukan pengembangan dan penggunaan algoritma yang lebih tahan terhadap serangan kuantum dalam jangka panjang.

3) Efisiensi

Dalam hal efisiensi, ECC memiliki keunggulan dalam penggunaan sumber daya yang lebih efisien dibandingkan dengan algoritma kriptografi kunci-publik lainnya:

- *Penggunaan Daya CPU:* Algoritma ECC membutuhkan penggunaan daya CPU yang relatif rendah. Dalam pengujian, ECC mampu menjalankan operasi enkripsi dan dekripsi dengan penggunaan daya CPU yang efisien, mengurangi konsumsi daya perangkat secara keseluruhan.
- *Penggunaan Memori:* Algoritma ECC membutuhkan penggunaan memori yang cukup efisien. Ukuran kunci yang relatif kecil memungkinkan penggunaan memori yang lebih sedikit dibandingkan dengan algoritma kriptografi kunci-publik lainnya.

Dalam perbandingan dengan algoritma kriptografi kunci-publik lainnya, ECC menunjukkan keunggulan dalam hal efisiensi penggunaan daya. Namun, efisiensi ini juga tergantung pada implementasi spesifik dan pengaturan penggunaan algoritma.

Dalam keseluruhan, ECC merupakan pilihan menarik dalam pengamanan komunikasi data pada jaringan *wireless* karena kombinasi keamanan yang tinggi, performa yang baik, dan efisiensi penggunaan daya yang tinggi. Namun, keputusan penggunaan algoritma kriptografi harus mempertimbangkan konteks dan persyaratan keamanan yang spesifik untuk masing-masing aplikasi.

C. Kontribusi Algoritma ECC dalam Mengamankan Komunikasi Data pada Jaringan Wireless

Algoritma *Elliptic Curve Cryptography* (ECC) telah memberikan kontribusi yang signifikan dalam mengamankan komunikasi data pada jaringan *wireless*. Berikut adalah beberapa kontribusi penting dari algoritma ECC:

1) Keamanan yang Tinggi dengan Kunci yang Lebih Kecil

ECC telah terbukti menjadi algoritma kriptografi yang aman dengan ukuran kunci yang relatif kecil. Keamanan yang tinggi dan kekuatan matematis yang mendasarinya membuat ECC menjadi pilihan yang menarik dalam melindungi integritas, kerahasiaan, dan otentikasi data dalam jaringan *wireless*. Dalam konteks jaringan *wireless* yang sering menggunakan perangkat dengan sumber daya terbatas, penggunaan ukuran kunci yang lebih kecil pada ECC memungkinkan operasi enkripsi dan dekripsi yang lebih cepat dan efisien.

2) Efisiensi Penggunaan Daya

Salah satu kontribusi utama ECC adalah efisiensi penggunaan daya yang tinggi. Dalam komunikasi data pada jaringan *wireless*, penggunaan daya baterai yang efisien sangat penting untuk memperpanjang masa pakai perangkat mobile. ECC membutuhkan penggunaan daya CPU dan memori yang relatif rendah, sehingga memungkinkan perangkat *mobile* tetap beroperasi dalam waktu yang lebih lama tanpa kehabisan daya. Kontribusi ini menjadi sangat berharga dalam aplikasi jaringan *wireless* seperti *Internet of Things* (IoT) di mana perangkat memiliki keterbatasan daya.

3) Skalabilitas dan Fleksibilitas

ECC juga menawarkan skalabilitas yang baik dalam mengamankan komunikasi data pada jaringan *wireless*. Algoritma ini dapat digunakan untuk mengamankan komunikasi pada jaringan dengan jumlah perangkat yang beragam, mulai dari perangkat yang relatif sederhana hingga perangkat yang lebih canggih. Fleksibilitas ECC dalam hal penggunaan kunci, kurva eliptik, dan protokol kriptografi yang terkait memungkinkan adaptasi yang lebih mudah terhadap kebutuhan spesifik jaringan *wireless*.

4) Potensi Penggunaan dalam Kehidupan Sehari-hari

Potensi penggunaan ECC dalam kehidupan sehari-hari sangat luas. Contohnya, ECC dapat digunakan dalam sistem pembayaran elektronik, seperti kartu pintar atau dompet digital, untuk melindungi data finansial pengguna. Selain itu, dalam komunikasi nirkabel seperti Wi-Fi atau Bluetooth, ECC dapat digunakan untuk mengamankan pertukaran data antara perangkat dan memastikan privasi pengguna. Penggunaan ECC juga telah diadopsi dalam protokol keamanan internet seperti *Transport Layer Security* (TLS) yang digunakan dalam keamanan transmisi data di web.

Secara keseluruhan, ECC telah memberikan kontribusi yang signifikan dalam mengamankan komunikasi data pada jaringan *wireless*. Keamanan yang tinggi, efisiensi penggunaan daya, skalabilitas, dan fleksibilitas ECC menjadikannya pilihan yang menarik dalam mengatasi tantangan keamanan dalam konteks jaringan *wireless*. Dengan potensi penggunaan yang luas dalam berbagai aspek kehidupan sehari-hari, ECC terus berkembang dan menjadi bagian integral dari sistem keamanan digital modern.

V. KESIMPULAN

Dalam penelitian ini, penulis telah melakukan analisis mendalam terkait dengan penggunaan algoritma *Elliptic Curve Cryptography* (ECC) dalam mengamankan komunikasi data

pada jaringan *wireless*. Berikut adalah temuan utama dan kesimpulan yang dapat diambil dari penelitian ini:

A. Temuan Utama

- Algoritma ECC menawarkan keamanan yang tinggi dengan ukuran kunci yang relatif kecil, membuatnya menjadi pilihan yang menarik dalam mengamankan komunikasi data pada jaringan *wireless*.
- ECC memiliki efisiensi penggunaan daya yang tinggi, memungkinkan perangkat *mobile* tetap beroperasi dalam waktu yang lebih lama tanpa kehabisan daya.
- ECC memiliki skalabilitas dan fleksibilitas yang baik, sehingga dapat digunakan dalam berbagai jenis jaringan *wireless* dengan beragam perangkat.
- ECC memiliki potensi penggunaan yang luas dalam kehidupan sehari-hari, termasuk dalam sistem pembayaran elektronik, komunikasi nirkabel, dan protokol keamanan internet.

B. Kontribusi Algoritma ECC dalam Konteks Jaringan Wireless

- Algoritma ECC memberikan kontribusi yang signifikan dalam mengamankan komunikasi data pada jaringan *wireless* dengan kombinasi keamanan yang tinggi, efisiensi penggunaan daya, dan fleksibilitas dalam penggunaan kunci.
- ECC membantu menjaga integritas, kerahasiaan, dan otentikasi data dalam komunikasi nirkabel, memberikan lapisan keamanan yang kuat bagi pengguna dan organisasi.

C. Rekomendasi dan Arah Penelitian Masa Depan

- Meningkatkan kesadaran dan pemahaman tentang ECC di kalangan praktisi dan pengembang sistem keamanan menjadi penting. Pelatihan dan edukasi terkait dengan implementasi dan penggunaan yang benar dari algoritma ECC akan membantu memperkuat keamanan dalam jaringan *wireless*.
- Penelitian lebih lanjut dapat dilakukan untuk meningkatkan efisiensi dan kinerja ECC dalam konteks jaringan *wireless*. Peningkatan implementasi perangkat keras dan perangkat lunak ECC dapat membawa manfaat yang signifikan dalam hal kecepatan operasi dan penggunaan daya yang lebih efisien.
- Pengembangan protokol dan standar yang menggabungkan ECC dengan teknologi terkini seperti *Internet of Things* (IoT) dan 5G akan menjadi fokus penelitian masa depan. Membangun sistem keamanan yang terintegrasi dengan kecepatan tinggi dan keandalan tinggi akan menjadi tantangan penting yang perlu diatasi.

Secara keseluruhan, algoritma *Elliptic Curve Cryptography* (ECC) telah memberikan kontribusi yang signifikan dalam mengamankan komunikasi data pada jaringan *wireless*. Keamanan yang tinggi, efisiensi penggunaan daya, dan fleksibilitas ECC menjadikannya pilihan yang menarik dalam menghadapi tantangan keamanan dalam konteks jaringan *wireless*. Dengan meningkatnya pemahaman dan penelitian lebih lanjut, ECC memiliki potensi untuk terus berkembang dan menghadirkan solusi keamanan yang inovatif dan efektif bagi jaringan *wireless* masa depan.

Daftar Pustaka

[1] Munir, Rinaldi. "Elliptic Curve Cryptography (ECC) (Bagian 1)". https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2022-2023/23-ECC-Bagian1-2023.pdf. Diakses pada 21 Mei 2023.

[2] Munir, Rinaldi. "Elliptic Curve Cryptography (ECC) (Bagian 2)". https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2022-2023/24-ECC-Bagian2-2023. Diakses pada 21 Mei 2023.

[3] Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644-654.

[4] Koblitz, N. (1987). Elliptic curve cryptosystems. Mathematics of Computation, 48(177), 203-209.

[5] Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of applied cryptography. CRC press.

[6] Gallant, R. P., Lambert, R. J., & Vanstone, S. A. (2001). Faster point multiplication on elliptic curves with efficient endomorphisms. Advances in Cryptology - Asiacrypt 2001, 190-200.

[7] Smart, N. P. (2004). The discrete logarithm problem on elliptic curves of trace one. Journal of Cryptology, 17(4), 239-246.

[8] López, J., Dahab, R., & Aranha, D. F. (2015). Elliptic curve cryptosystems: Efficient techniques for security. CRC press.

[9] Sarwono, R. (2016). Keamanan jaringan komputer: konsep dan aplikasi. Andi.

[10] Joy, C. J., Muthupriya, M., & Dharmalingam, S. (2018). Performance analysis of elliptic curve cryptography for secure data transmission in wireless sensor networks. International Journal of Computer Science and Information Security, 16(2), 36-43.

[11] Bhowmik, D., & Das, A. K. (2019). Secured data transmission in wireless sensor networks using ECC-based hybrid encryption scheme. Security and Communication Networks, 2019, 1-14.

[12] Patel, J., & Sharma, V. (2020). Comparative analysis of RSA and ECC algorithms for wireless communication. 2020 7th International Conference on Signal Processing and Integrated Networks (SPIN), 430-434.

[13] Yaseen, Z. A., & Malik, A. W. (2021). Performance analysis of symmetric and asymmetric key algorithms for wireless sensor networks. Wireless Personal Communications, 116(1), 337-360.

Pernyataan

Dengan ini saya menyatakan bahwa makalah ini adalah tulisan saya sendiri, bukan saduran atau terjemahan dari makalah orang lain, bukan juga plagiat.

Bandung, 22 Mei 2023

Daffa Ananda Pratama Resyaly

13519107